RTF

Automatic Voltage Regulator





Instructions Manual for **RTF** Models
M0RTFA1902Iv33

REV. 33 - March, 2026 © ZIV APLICACIONES Y TECNOLOGÍA, S.L.U. 2019

Table of Contents

1.1 Introduction 1.1-1
1.1.1 Relay Overview and Applications 1.1-2
1.1.2 Symbols 1.1-2
1.1.3 Relay Family Features 1.1-3
1.1.3.a Hardware Design 1.1-4
1.1.3.b Measurement Processing 1.1-5
1.1.3.c Memory and Internal Clock 1.1-6
1.1.4 Functional Diagram 1.1-6

1.2 Model Selection 1.2-1
1.2.1 Hardware Model Selection 1.2-2
1.2.1.a 1/3 19" Rack Models 1.2-2
1.2.1.b 1/2 19" Rack Models 1.2-3
1.2.1.c 19" Rack Models 1.2-5
1.2.1.d Definition of Slots 1.2-7
1.2.1.e Accessories 1.2-8
1.2.2 Firmware Model Selection 1.2-9
1.2.3 Protection Functions according to Model 1.2-10

1.3 Technical Data 1.3-1
1.3.1 Power Supply Voltage 1.3-2
1.3.2 Power Supply Burden 1.3-2
1.3.3 Current Analog Inputs 1.3-2
1.3.4 Voltage Analog Inputs 1.3-2
1.3.5 Frequency 1.3-3
1.3.6 Measurement Accuracy at Environment Temperature (25ºC) 1.3-3
1.3.7 Effect of Temperature in Measurement Accuracy 1.3-5
1.3.8 Repeatability 1.3-5
1.3.9 Accuracy of the AVR Operation Times (T1 and T2) 1.3-5
1.3.10 Accuracy of the Pickup and Reset of the Voltage Elements 1.3-6
1.3.11 Accuracy of the Pickup and Reset of the Frequency Elements 1.3-6
1.3.12 Digital Inputs 1.3-7
1.3.13 Auxiliary Outputs 1.3-7
1.3.14 Input Transducers 1.3-8
1.3.15 Communications Link 1.3-8

1.4 Current Transformers Dimensioning 1.4-1
1.4.1 Introduction 1.4-2
1.4.2 CT Dimensioning According to Different Standards 1.4-2
1.4.2.a Class P of IEC 61869-2 Standard 1.4-2
1.4.2.b Class C of IEEE C57.13 Standard 1.4-4
1.4.2.c Class X of BS3938 Standard or Class PX of IEC61869-2 ..... 1.4-5
1.4.3 CT Dimensioning for Different Protection Functions 1.4-6
1.4.3.a Remanence Factor 1.4-7
1.4.3.b Ktf Factor 1.4-8

1.5 Physical Description 1.5-1
1.5.1 General 1.5-2
1.5.2 Dimensions 1.5-5
1.5.3 Connection Elements 1.5-6

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table of Contents

1.5.3.a Terminal Blocks 1.5-6
1.5.3.b Removing Printed Circuit Boards (Non Self-shorting) 1.5-7
1.5.3.c Internal Wiring 1.5-7
1.5.4 Local Interface 1.5-8
1.5.4.a Display and Keypad 1.5-8
1.5.4.b Keypad associated to the Alphanumeric Display 1.5-11
1.5.4.c Command Buttons 1.5-12
1.5.4.d Keys, Functions and Operation Modes 1.5-12
1.5.4.e Access to Options 1.5-16
1.5.5 Symbols associated to the Graphic Display 1.5-18
1.5.6 LEDs 1.5-19
1.5.7 Inputs and Outputs 1.5-20
1.5.7.a Digital Inputs 1.5-20
1.5.7.b Auxiliary Outputs 1.5-26
1.5.7.c Digital Inputs, Auxiliary Outputs and LEDs Test 1.5-27
1.5.8 Communications 1.5-28
1.5.8.a Communications Ports 1.5-28
1.5.8.b LEDs associated to the Communications Ports 1.5-29
1.5.8.c Communication with the Configuration Tool 1.5-29
1.5.8.d Communication Protocols 1.5-30
1.5.8.e Control Change Recording 1.5-30
1.5.8.f Ethernet Redundancy 1.5-31
1.5.8.g Communications Settings 1.5-36
1.5.8.h Output Signals of the Communications Module 1.5-48
1.5.9 Time Synchronization 1.5-50
1.5.9.a Manual Time Synchronization 1.5-50
1.5.9.b Time Synchronization by Protocol 1.5-50
1.5.9.c Synchronization by SNTP 1.5-50
1.5.9.d Synchronization by IRIG-B 123 and 003 ..... 1.5-50
1.5.9.e PTP Synchronization 1.5-51
1.5.9.f Synchronization Settings 1.5-51
1.5.9.g Output Signals of the Synchronization Module 1.5-53

1.6 Installation and Commissioning 1.6-1
1.6.1 General 1.6-2
1.6.2 Accuracy 1.6-2
1.6.3 Installation 1.6-3
1.6.4 Preliminary Inspection 1.6-4
1.6.5 Tests 1.6-5
1.6.5.a Isolation Test 1.6-5
1.6.5.b Power Supply Test 1.6-6
1.6.5.c Metering Tests 1.6-6

1.7 Onload Test 1.7-1
1.7.1 Introduction 1.7-2
1.7.2 Voltage Connections 1.7-2
1.7.3 Current Connections 1.7-2

1.8 Standards and Type Tests 1.8-1
1.8.1 Insulation 1.8-2
1.8.2 Electromagnetic Compatibility 1.8-3
1.8.3 Environmental Test 1.8-4
1.8.4 Power Supply 1.8-5
1.8.5 Mechanical Test 1.8-5

1.9 Schemes and Drawings 1.9-1

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table of Contents

1.10 Alarm Codes 1.10-1
1.10.1 Introduction 1.10-2
1.10.2 Activation of Signal and Alarm Generation Event 1.10-2
1.10.3 Update of the Alarm Status Magnitude 1.10-2
1.10.4 Indication on the HMI Stand-By Screen 1.10-3
1.10.5 LED Indication and Operating States of the Equipment 1.10-4
1.10.6 General Alarm Counter 1.10-4

1.11 Troubleshooting 1.11-1
1.11.1 Introduction 1.11-2
1.11.2 Software with Self-Checking 1.11-2
1.11.3 Power Up 1.11-2
1.11.4 In Service / Alarm Contact 1.11-3
1.11.5 Error Messages during Power Up 1.11-3
1.11.6 Error Messages when the Relay is in Normal Operation 1.11-4
1.11.7 Errors while Communicating 1.11-5
1.11.8 Error in Digital Inputs 1.11-7
1.11.9 Error in Digital Outputs 1.11-7
1.11.10 Error in Transducer Inputs 1.11-8
1.11.11 Error in Measurements 1.11-8
1.11.12 Fatal Errors 1.11-8

2.1 Voltage Regulator 2.1-1
2.1.1 Identification 2.1-3
2.1.2 General Block 2.1-3
2.1.3 Regulator Configuration 2.1-3
2.1.3.a Magnitude Display on Default Screen 2.1-3
2.1.3.b Type of Voltage and Current Wired 2.1-3
2.1.3.c Operation Output Types 2.1-4
2.1.3.d Tap Control and Tap Change Operation Monitoring 2.1-4
2.1.3.e Voltage Set-point and Insensitivity Degree 2.1-4
2.1.4 Regulation Variable 2.1-7
2.1.5 Delay Times 2.1-8
2.1.5.a Delay Time for the First Control Operation: T1 ..... 2.1-8
2.1.5.b Delay Time for Following Control Operations: T2 ..... 2.1-9
2.1.5.c Cancel Timer T_1 ..... 2.1-9
2.1.6 Line Drop Compensation (LDC) 2.1-10
2.1.6.a Line Drop Compensation: LDC-Z 2.1-11
2.1.6.b Line Drop Compensation: LDC-R&X 2.1-12
2.1.7 Voltage Regulation of Parallel Transformers 2.1-13
2.1.7.a Reactive Compensation 2.1-14
2.1.7.b Calculation of the Reactive Current Flowing through two Transformers in Parallel with Current Wiring 2.1-15
2.1.7.c Calculation of Circulating Reactive Current by Communications (Maximum of 5 Transformers in Parallel) 2.1-16
2.1.7.d Calculation of the Reactive Compensation Setting 2.1-16
2.1.7.e Calculation of the Compensation by Circulating Current 2.1-17
2.1.7.f Example 2.1-17
2.1.8 Combined Compensation and Maximum Compensation 2.1-18
2.1.9 Automatic / Manual Regulation Mode 2.1-19
2.1.10 Manual Commands 2.1-19
2.1.11 Tap Control 2.1-20
2.1.11.a Tap Coding 2.1-20
2.1.11.b Number of Taps, Minimum Tap, Upper Limit and Lower Limit 2.1-21

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table of Contents

2.1.11.c Tap Indication 2.1-21
2.1.11.d Tap Monitoring 2.1-22
2.1.11.e Tap Change Operation Monitoring 2.1-23
2.1.11.f Tap Change Operation Counters 2.1-23
2.1.12 Blockings 2.1-24
2.1.13 Power Flow Reversal 2.1-28
2.1.14 Voltage Band Recording 2.1-29
2.1.15 Display Information 2.1-30
2.1.16 Settings Recommendation 2.1-31
2.1.17 Settings Calculation Example 2.1-33
2.1.18 Setting Ranges 2.1-36
2.1.19 Analog Inputs to the Unit 2.1-39
2.1.20 Digital Inputs of the Voltage Regulator 2.1-39
2.1.21 Auxiliary Outputs and Events of the Voltage Regulator 2.1-41
2.1.22 IEC 61850 Logical Node 2.1-42
2.1.23 ATCC IEC 61850 Control Commands 2.1-45
2.1.24 Voltage Regulator Test 2.1-46

3.1 Voltage Elements 3.1-1
3.1.1 Common Principles 3.1-2
3.1.1.a Operation and Reset 3.1-2
3.1.1.b Trip Blocking 3.1-2
3.1.1.c Enabling and Disabling the Unit 3.1-2
3.1.1.d Restoration Settings 3.1-2
3.1.1.e Logical Node: Common Characteristics (Voltage Elements Reset Settings) 3.1-2
3.1.2 Phase Overvoltage Elements 3.1-3
3.1.2.a Identification 3.1-3
3.1.2.b General Block 3.1-3
3.1.2.c Operation Principles and Block Diagram 3.1-3
3.1.2.d Application 3.1-5
3.1.2.e Setting Ranges 3.1-5
3.1.2.f Analog Inputs to the Unit 3.1-5
3.1.2.g Digital Inputs to the Phase Overvoltage Unit 3.1-6
3.1.2.h Auxiliary Outputs and Events of the Phase Overvoltage Modules 3.1-7
3.1.2.i IEC 61850 Logical Node 3.1-8
3.1.2.j Protection Element Test 3.1-8

3.2 Frequency Elements 3.2-1
3.2.1 Common Principles 3.2-2
3.2.1.a Frequency Measurement 3.2-2
3.2.1.b Adaptation of the Sampling Frequency to the Network Frequency 3.2-3
3.2.1.c Operation and Reset 3.2-3
3.2.1.d Elements Blocking Logic 3.2-4
3.2.1.e Enabling and Disabling the Element 3.2-4
3.2.1.f Undervoltage Element for Blocking 3.2-4
3.2.1.g Common Settings 3.2-5
3.2.1.h Setting Ranges 3.2-6
3.2.1.i IEC 61850 Logical Node 3.2-6
3.2.1.j Protection Element Test 3.2-7
3.2.1.k Application 3.2-8
3.2.2 Underfrequency Elements 3.2-10
3.2.2.a Identification 3.2-10
3.2.2.b General Block 3.2-10
3.2.2.c Operation Principles 3.2-10

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.2.d Setting Ranges 3.2-10
3.2.2.e Analog Inputs to the Unit 3.2-11
3.2.2.f Digital Inputs to the Underfrequency Modules 3.2-11
3.2.2.g Auxiliary Outputs and Events of the Underfrequency Modules 3.2-12
3.2.2.h IEC 61850 Logical Node 3.2-13
3.2.2.i Protection Element Test 3.2-13

4.1 Voltage Measurement Circuit Supervision 4.1-1
4.1.1 Identification 4.1-2
4.1.2 General Block 4.1-2
4.1.3 Operation Principles and Block Diagram 4.1-2
4.1.4 Aplication of the Unit 4.1-3
4.1.5 Setting Ranges 4.1-3
4.1.6 Analogue Inputs to Voltage Measurement Circuit Supervision Module 4.1-3
4.1.7 Digital Inputs to the Voltage Measurement Circuit Supervision Module 4.1-4
4.1.8 Auxiliary Outputs and Events of the Voltage Measurement Circuit Supervision Module 4.1-4
4.1.9 IEC 61850 Logical Node 4.1-5
4.1.10 Voltage Measurement Circuit Supervision Test 4.1-6

4.2 Trip and Close Coil Circuit Supervision 4.2-1
4.2.1 Identification 4.2-2
4.2.2 General Block 4.2-2
4.2.3 Operation Principles and Block Diagram 4.2-2
4.2.3.a Circuit 1 Supervision in One State 4.2-5
4.2.3.b Supervision of Coil Circuit 2 ..... 4.2-5
4.2.4 Setting Ranges 4.2-6
4.2.5 Auxiliary Outputs and Events of the Coil Circuit Supervision Module 4.2-7
4.2.6 IEC 61850 Logical Node 4.2-7
4.2.7 Coil Circuit Supervision Test 4.2-8

4.3 General Settings 4.3-1
4.3.1 Description 4.3-2
4.3.1.a Unit In Service 4.3-2
4.3.1.b Transformer Ratios 4.3-2
4.3.1.c Angle Reference 4.3-3
4.3.1.d Digital PLL 4.3-3
4.3.1.e Simultaneous Commands 4.3-3
4.3.1.f Description Settings 4.3-4
4.3.2 Setting Ranges 4.3-4

4.4 Configuration Settings 4.4-1
4.4.1 Description 4.4-2
4.4.1.a Nominal Values 4.4-2
4.4.1.b Access Passwords 4.4-2
4.4.1.c Communications 4.4-2
4.4.1.d Date and Time 4.4-3
4.4.1.e Contrast Adjustment 4.4-3
4.4.1.f Autodimming Function 4.4-3
4.4.1.g Return Time 4.4-4
4.4.2 Setting Ranges 4.4-4

4.5 Change Settings Groups 4.5-1
4.5.1 Description 4.5-2
4.5.2 Digital Inputs to Change Settings Groups 4.5-3

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table of Contents

4.5.3 Auxiliary Outputs and Events to Change Settings Groups 4.5-4
4.6 Time Zone Calendar 4.6-1
4.6.1 Identification 4.6-2
4.6.2 General Block 4.6-2
4.6.3 Description 4.6-2
4.6.4 Setting Ranges 4.6-2
4.6.5 Auxiliary Outputs of the Time Zone Calendar 4.6-3
4.6.6 IEC 61850 Logical Node 4.6-3

4.7 Programmable Logic 4.7-1
4.7.1 Description 4.7-2
4.7.2 Functional Characteristics 4.7-2
4.7.3 Control Commands 4.7-4
4.7.3.a Command or Source Hierarchy 4.7-4
4.7.3.b Successful and Failed Command Signals 4.7-5
4.7.3.c Running simultaneous Commands 4.7-5
4.7.3.d Command Treatment 4.7-5
4.7.3.e Command Blocking as a Function of the Hierarchy 4.7-6
4.7.4 Description of Logic Operations 4.7-7
4.7.4.a Boolean Operations (Booleans) 4.7-7
4.7.4.b Move Instructions 4.7-8
4.7.4.c Pulse Activation Operations (Triggers) 4.7-10
4.7.4.d Counters 4.7-13
4.7.4.e Arithmetic Operations 4.7-14
4.7.4.f Special Operations 4.7-17

4.8 Open Pole Detector 4.8-1
4.8.1 Identification 4.8-2
4.8.2 General Block 4.8-2
4.8.3 Operation Principles and Block Diagram 4.8-2
4.8.4 Setting Ranges 4.8-4
4.8.5 Analog Inputs to the Unit 4.8-4
4.8.6 Digital Inputs to the Open Pole Module 4.8-4
4.8.7 Auxiliary Outputs and Events of the Open Pole Module 4.8-5
4.8.8 IEC 61850 Logical Node 4.8-5

4.9 Pole Discordance Detector 4.9-1
4.9.1 Identification 4.9-2
4.9.2 General Block 4.9-2
4.9.3 Operating Principles and Block Diagram 4.9-2
4.9.4 Setting Ranges 4.9-3
4.9.5 Digital Inputs to the Pole Discordance Detector Module 4.9-3
4.9.6 Auxiliary Outputs and Events of the Pole Discordance Detector Module 4.9-4
4.9.7 IEC 61850 Logical Node 4.9-4
4.9.8 Protection Element Test 4.9-5

5.1 Oscillographic Recording 5.1-1
5.1.1 Operation Principles 5.1-2
5.1.2 Capture Function 5.1-2
5.1.3 Stored Data 5.1-2
5.1.4 Number of Channels and Digital Signals 5.1-2
5.1.5 Start Function 5.1-3
5.1.6 Oscillograph Deletion Function 5.1-3
5.1.7 Pre-Fault Time 5.1-3
5.1.8 Length of the Oscillograph 5.1-4

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.1.9 Setting Ranges 5.1-4
5.1.10 Digital Inputs of the Oscillographic Recording 5.1-5
5.1.11 Auxiliary Outputs and Events of the Oscillographic Recording 5.1-6
5.1.12 IEC 61850 Logical Node 5.1-6

5.2 Event Record 5.2-1
5.2.1 Introduction 5.2-2
5.2.2 Protection Event Record 5.2-2
5.2.2.a Operation Principles 5.2-2
5.2.2.b Organization of the Event Record 5.2-3
5.2.2.c Event Mask 5.2-4
5.2.2.d Consulting the Record 5.2-4
5.2.2.e Event Record Settings (Only via Communications) 5.2-4
5.2.2.f SYSLOGSOE Event Record 5.2-5
5.2.3 IEC 61850 Based SYSLOGSOE Event Record 5.2-8
5.2.3.a SYSLOG Event Format 5.2-11
5.2.3.b SYSLOGSOE File Format 5.2-12

5.3 Metering History Log 5.3-1
5.3.1 Operation Principles 5.3-2
5.3.2 Setting Ranges 5.3-3
5.3.3 IEC61850 Logical Node 5.3-5

A. PROCOME 3.0 Communications Protocol A-1
A.1 Control Application Layer A-2
A.2 Control Data A-3

B. DNP V3.00 Device Profiles Document B-1
Dnp3 Basic Profile B-3
Dnp3 Basic Extended Profile B-23
Dnp3 Profile II B-43
Dnp3 Profile II Ethernet B-65

C. MODBUS RTU Documentation. Address Map C-1
C.1 Preliminary Information C-2
C.2 Function 01: Read Coil Status C-2
C.2.1 Modbus Address Map for RTF C-2
C.3 Function 02: Read Input Status C-3
C.3.1 Modbus Address Map for RTF C-3
C.4 Function 03: Read Holding Registers C-3
C.4.1 Modbus Address Map for RTF C-3
C.5 Function 04: Read Input Registers C-4
C.5.1 Modbus Address Map for RTF C-4
C.6 Function 05: Force Single Coil C-5
C.6.1 Modbus Address Map for RTF C-5

D. IEC 61850 Ed.2 ..... D-1
D.1 IEC 61850 Standard D-2
D.2 Communications Stack D-3
D.3 IEC 61850 Server and Data Model D-4
D.4 Web Server D-5
D.5 Communications Port D-7
D.6 File Transfer D-8
D.7 CID Configuration File D-9
D.8 Mod/Beh D-10

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table of Contents

D.9 Data Set D-11
D.10 Send GOOSE Messages D-12
D.11 Subscription to GOOSE Message Data D-14
D.12 Report Control Blocks (RCBs) D-21
D.13 Measurement Configuration (Data CF) D-23
D.14 Commands D-24
D.15 SNTP Synchronization D-25
D.15.1 SNTP Synchronism Status Calculation D-25
D.15.1.a *Unicast* Client D-25
D.15.1.b *Broadcast* Client D-26
PICS
PIXIT
TICS

E. IEC 61850 Ed.2 Dynamic Model E-1
E.1 IEC 61850 Standard E-2
E.2 Communications Stack E-3
E.3 IEC 61850 Server and Data Model E-4
E.3.1 AccesPoint E-5
E.3.2 Logical Device E-7
E.3.3 Logical Node E-7
E.4 Web Server E-9
E.5 Communications Port E-11
E.6 File Transfer E-12
E.7 CID Configuration File E-13
E.8 Mod/Beh E-14
E.9 Data Set E-16
E.10 GOOSE Messages Publishing E-17
E.11 Subscription to GOOSE Message Data E-19
E.12 Report Control Blocks (RCBs) E-22
E.13 Measurement Configuration (Data CF) E-24
E.14 Commands E-26
E.15 SNTP Synchronization E-28
E.15.1 SNTP Synchronism Status Calculation E-28
E.15.1.a *Unicast* Client E-28
E.15.1.b *Broadcast* Client E-29
PICS
PIXIT
TICS

F. Cybersecurity F-1
F.1 Introduction F-3
F.2 Ports and Communications Services F-4
F.3 Role Based Access Control (RBAC) F-6
F.3.1 Users, Roles and Permissions F-7
F.3.2 User and Role Management F-12
F.3.2.a User and Role Management from the Web F-12
F.3.2.b User and Role Management from CLI F-16
F.3.2.c User and Role Management from *ZIV e-NET Tool®* F-18
F.3.3 Session Concurrency F-23
F.3.4 Local Access F-24
F.3.4.a Password Authentication F-27
F.3.4.b User and Password Authentication F-29
F.3.5 Automatic Logout F-31
F.4 Remote User Authentication F-32
F.4.1 RADIUS (Remote Authentication Dial In User Service) F-33
F.4.2 LDAP (Lightweight Directory Access Protocol) F-35

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.4.3 Remote User Authentication Configuration F-39
F.4.3.a Remote User Authentication Configuration from the Web F-39
F.4.3.b Remote User Authentication Configuration from CLI F-41
F.4.3.c Remote User Authentication Configuration from *ZIV e-NET Tool*® F-42
F.5 Communication with Configuration Tool using PROCOME F-51
F.6 Secure Sockets F-52
F.6.1 SSH (Secure Shell) F-52
F.6.2 SFTP (SSH File Transfer Protocol) F-53
F.6.3 TLS / SSL (Transport Layer Security / Secure Socket Layer) F-53
F.6.4 HTTPS (Secure Web Server) F-54
F.6.5 Mutual Authentication F-54
F.7 Credential Management F-56
F.7.1 Devices with Basic Cybersecurity F-56
F.7.2 Devices with Enhanced Cybersecurity F-58
F.8 Digital Firmware Securization F-63
F.8.1 Devices with Basic Cybersecurity F-64
F.8.2 Devices with Enhanced Cybersecurity F-64
F.8.3 Firmware Upload Methods F-66
F.9 Registration of Activities F-68
F.9.1 Syslog Format F-68
F.9.2 Events F-68
F.9.3 Storage File F-73
F.9.4 Viewing and Downloading the File F-74

G. Syslog Protocol G-1
G.1 General G-2
G.2 Syslog Format for Cybersecurity Events G-3
G.2.1 HEADER Format G-3
G.2.2 STRUCTURED-DATA Format G-4
G.2.3 Examples G-5
G.3 Syslog Format for Cybersecurity Events (version 2) G-6
G.3.1 HEADER Format G-6
G.3.2 STRUCTURED-DATA Format G-7
G.3.3 Examples G-8
G.4 Syslog Format for Protection Events (SOE) G-9
G.4.1 HEADER Format G-9
G.4.2 STRUCTURED-DATA Format G-10
G.4.3 MSG Format G-11
G.4.4 Examples G-11
G.5 Syslog Format for Based on IEC 61850 Events (SOE) G-12
G.5.1 HEADER Format G-12
G.5.2 STRUCTURED-DATA Format G-13
G.5.3 MSG Format G-13
G.5.4 Examples G-14
G.6 Syslog Transmission G-14

H. List of Illustrations and Tables H-1
H.1 List of Figures H-2
H.2 List of Tables H-4

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Chapter 1.

Description and Start-Up

1.1 Introduction

1.1.1 Relay Overview and Applications 1.1-2
1.1.2 Symbols 1.1-2
1.1.3 Relay Family Features 1.1-3
1.1.3.a Hardware Design 1.1-4
1.1.3.b Measurement Processing 1.1-5
1.1.3.c Memory and Internal Clock 1.1-6
1.1.4 Functional Diagram 1.1-6

This instruction manual provides a technical and functional description of the relay **rtf**. The manual may be used as technical reference in engineering, installation, commissioning, and normal operation of the relay since the manual contains operating and handling instructions apart from descriptions relative to technical data, function lists, logic diagrams, input and output signals, parameter settings and detail explanation of every function.

ZIV has attempted to make this manual as accurate and easy to understand as possible. However, **ZIV** cannot guarantee that it is free of errors in the manuals and it could also be subject to possible upgrades. Therefore, **ZIV** would be very grateful to receive customer comments on possible errors or recommendations. Suggestions may be sent to **ZIV** through the following link.

1.1.1 Relay Overview and Applications

The IED generally called **RTF** integrates protection, control and metering functions to cover all transformer voltage regulation applications.

These IEDs use the most advanced digital technology based on a powerful microprocessor and DSPs that incorporate the voltage regulation automatism together with their own compensation, supervision and blocking systems as well as voltage (59), frequency (81m) or voltage supervision.

The communications interface has secure access systems (SSH, SFTP, HTTPS), and supports several protocols including communications standard IEC61850 Ed.1 & Ed.2, as well as redundancy protocols RSTP, PRP, and HSR; and synchronization protocols SNTP, PTP (1588).

1.1.2 Symbols

The following symbols can be found in the manual as well as in the back of the relay.



WARNING:
Hazards that may derived into personal injuries or damage to the equipment. Refer to the Instructions Manual.



WARNING:
Electrical risk hazard



Grounding



Protection Ground Terminal

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.1.3 Relay Family Features

Multifunction protection and control of **RTF** relays are provided with the state-of-the-art digital technology based on powerful microprocessors so that all measurements acquisition tasks and breaker supervision tasks are digitally processed within a modular design.

Relay analog inputs capture currents and voltages transmitted by instrument and protection transformers adapting them to internal processing level of the relay. **RTF** relays has 3 analog inputs: 2 current inputs and 1 voltage input. Analog measurements are processed by an analog digital converter included in the analog input board which sends the digital samples to the microcontroller.

The microcontroller carries out all the management tasks and functions of the relay, which include, for example, the filtering and re-sampling of the measurements, protection algorithms, control functions, data storage, distribution of data to the communications ports, etc.

Relay configurable inputs may be used to receive data from switchgear or other equipment through hardwiring. All relay outputs are configurable and may be used for protection or control.

The relay has two display options (as per model). Alphanumeric display and alphanumeric and graphical display.

The front alphanumeric screen has a resolution of 128x64 and can display 6 lines and 20 characters per line. The graphic screen has a resolution of 272x480, allowing the visualization of the screens configured in the user logic of the relay (single-line diagrams, alarm screens, etc.). Furthermore, both screens can display the status of all digital inputs and outputs and additional data via 16 configurable LEDs, whose activation will be shown by a red light. The status of the relay will be shown through a non-configurable tricolor LED (green/red/orange).

Models with *Standard Display* (model digit 5 = 1 or 2) feature 6 configurable bicolor LEDs (green/red) associated with the command buttons P1-P6.

Models with *Extended Buttons Display* (model digit 5 = 4) feature 12 configurable bicolor LEDs (green/red) associated with the command buttons P1-P12, plus other 2 configurable LEDs (fixed red) associated with the Local/Remote (L/R) button. For this model, only the graphic display option is available.

RTF relays include two front USB ports (1 type and 1 type B) to be able to carry out maintenance tasks and two rear remote communications ports, one series and the other Ethernet, which will allow relay communications under various protocols.

Relay electronics will carry out its tasks thanks to an internal power supply whose features could be decided at the time of selecting the required model and the details will appear in Technical Data chapter.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.1.3.a Hardware Design

The main components are:

- Main microcontroller module and memory that manage relay functions.
- Secondary microcontroller in the CPU board to gather data from the different modules or slots.
- Secondary microcontroller in the boards located in each Slot.
- Power supply board with inputs and outputs and coil supervision.
- Input and output expansion boards with coil supervision.
- Analogue boards
- Communications buses to link the various modules and to transmit the different types of data separately.

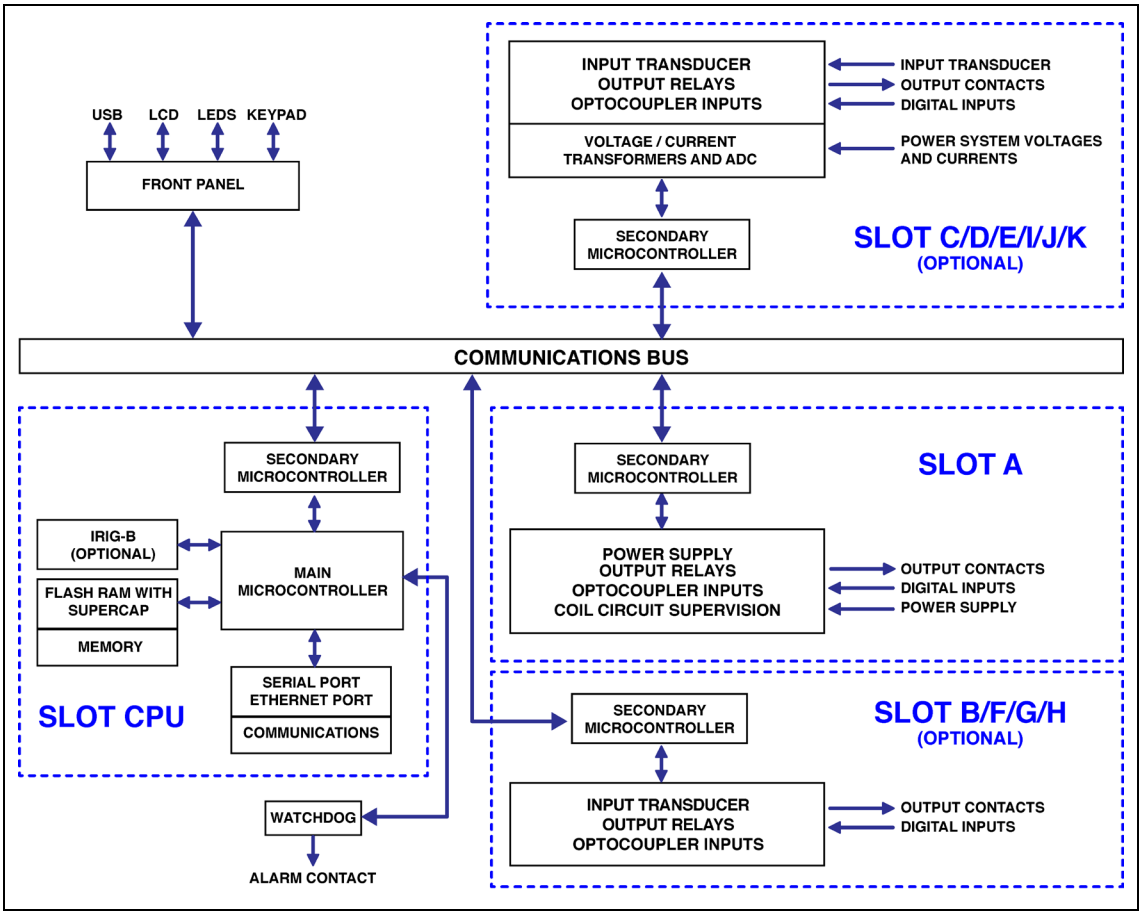


Figure 1.1.1: General HW Design.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.1.3.b Measurement Processing

RTF relays provide accurate measurement with high resolution in a broad dynamic range thanks to the high sampling frequency and the powerful measurement function they operate with.

Figure 1.1.2 (Measurement Processing) basically outlines the measurement processing from its capture point at the relay terminals, passing through the 24 bit analog digital converter and other elements up to having finally the measurement available.

After the measurement transformers, the relay is provided with a signal adapting stage together with analog low pass filter (antialiasing filter+ filter to strengthen the relay electromagnetic disturbance response). The A / D converter has an initial sampling frequency of 1 MHz. After applying a digital antialiasing filter, the A / D converter will generate, with a 24 bit resolution, an output frequency of 4800 Hz, in accordance with IEC 61869-9. The microcontroller included in each analog board performs two consecutive resamplings: the first, at 4800 Hz, to correct the magnitude and angle error introduced by the measurement chain (measurement transformers, analog filters, etc). The second, at 80 samples / cycle, to adapt the sampling frequency to the network frequency (Frequency Tracking), ensuring, in this way, a correct RMS measurement in the 15 to 80 Hz frequency range. The adaptation to the network frequency will be carried out provided the PLL element enable setting (refer to section 3.2) is set to **YES**.

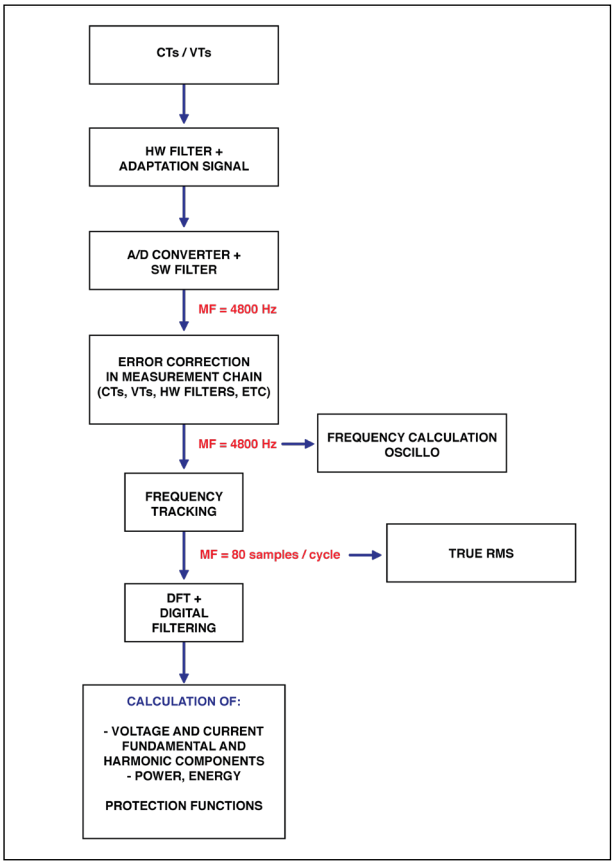


Figure 1.1.2: Measurement Processing.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.1.3.c Memory and Internal Clock

RTF relays include two different types of storage memory. All the relevant data will remain in non-volatile flash memory:

- Protection settings.
- Control logic.
- Events.
- Fault reports.
- Oscillography.
- Memorized LEDs.

In order to perform an adequate Flash memory management, the transference of data contained in circular records (Events and Fault Reports) will be made through a RAM powered by capacitors to be able to manage properly the task related to writing in Flash memory. In this way, data is stored firstly in the RAM memory to be later transferred periodically to the Flash memory. Memorized control logic signals will always be stored into this RAM.

The relay RAM memory and the internal clock are powered by capacitors. This system keeps both the data stored and the internal clock around two weeks.

1.1.4 Functional Diagram

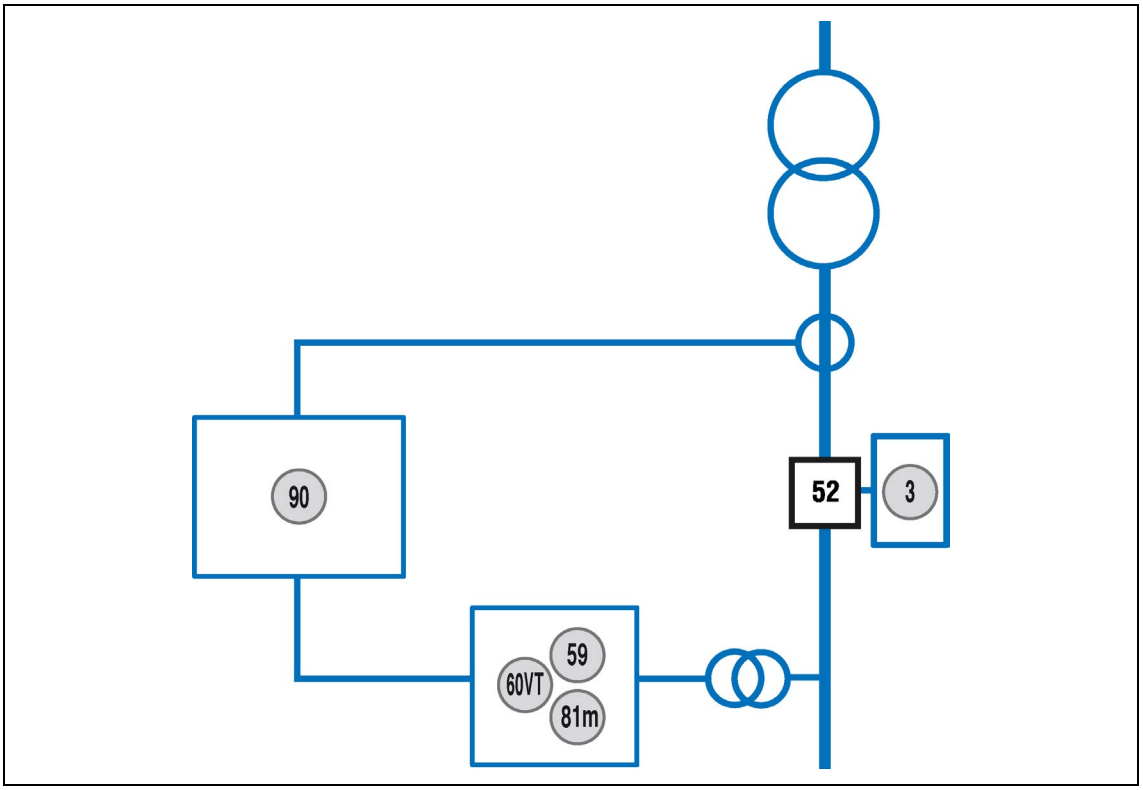


Figure 1.1.3: Functional Diagram.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2 Model Selection

1.2.1 Hardware Model Selection 1.2-2
1.2.1.a 1/3 19" Rack Models 1.2-2
1.2.1.b 1/2 19" Rack Models 1.2-3
1.2.1.c 19" Rack Models 1.2-5
1.2.1.d Definition of Slots 1.2-7
1.2.1.e Accessories 1.2-8
1.2.2 Firmware Model Selection 1.2-9
1.2.3 Protection Functions according to Model 1.2-10

1.2.1 Hardware Model Selection

The options available for configuring the model vary depending on the type of enclosure / chassis. According to the specific equipment, there will be 1/3, 1/2 or 1 x 19" rack models.

1.2.1.a 1/3 19" Rack Models

RTF		-							0	0	0	0	0	0
1-2-3	4		5	6	7	8	9	10	11	12	13	14	15	16

4	**Functionality**			
	A	Automatic voltage regulator with compensations, tap changer monitoring and parallel transformers operation.		
5	**User Interface**			
	1	Standard with alphanumeric display.	**4**	Extended buttons with graphic display.
	2	Standard with graphic display.		
6	**DI Auxiliary Supply Voltage**			
	A	Selectable by Software.	**D**	125 VDC
	B	24 VDC	**E**	250 VDC
	C	48 VDC		
7	**Enclosure/Chassis and Conformal Coat**			
	1	6U x 19" 1/3 Rack. Conformal Coated Circuit Boards. Blade Terminal.	**4**	6U x 19" 1/3 Rack. Conformal Coated Circuit Boards. Ring Lug Terminal.
8	**Slot A**			
	1	24 - 60 VDC (±20%) 16DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO.	**4**	90 - 250 VDC (±20%) and 100 - 240 VAC (-15%/+10%) 16DI (DIs distributed in 4 groups) (2 coil supervision each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO
9	**Slot B**			
	0	None.	**5**	20 DI (all independent).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**6**	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
10	**Slot C**			
	I	1V + 2I		

0	0		0			-
17	18	19	20	21	22	

19	**Communication Interface 1-2 for Remote Communication (PROCOME, MODBUS, DNP3)**			
	A	RS232 Full Modem - RS232/RS485.	**C**	GFO ST - RS232/RS485.
	B	RS232 Full Modem - GFO ST.	**D**	GFO ST - GFO ST.
21	**ETHERNET Interfaces 1 and 2**			
	1	10/100/1000BASE-T Connectors (RJ45).	**3**	100BASE-FX Connectors (Multimode GFO ST).
	2	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).		
22	**ETHERNET Interfaces 3 and 4**			
	0	None.	**3**	100BASE-FX Connectors (Multimode GFO ST).
	1	10/100/1000BASE-T Connectors (RJ45).		
	2	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).		

(*) SFP interfaces are considered as accessories and they must be additionally ordered. See Accessories.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.1.b 1/2 19" Rack Models

RTF		-									0	0	0	0
1-2-3	4		5	6	7	8	9	10	11	12	13	14	15	16

4	**Functionality**			
	A	Automatic voltage regulator with compensations, tap changer monitoring and parallel transformers operation.		
5	**User Interface**			
	1	Standard with alphanumeric display.	**4**	Extended buttons with graphic display.
	2	Standard with graphic display.		
6	**DI Auxiliary Supply Voltage**			
	A	Selectable by Software.	**D**	125 VDC
	B	24 VDC	**E**	250 VDC
	C	48 VDC		
7	**Enclosure/Chassis and Conformal Coat**			
	2	6U x 19" 1/2 Rack. Conformal Coated Circuit Boards. Blade Terminal.	**5**	6U x 19" 1/2 Rack. Conformal Coated Circuit Boards. Ring Lug Terminal.
	A	6U x 19" 1/2 Rack. Conformal Coated Circuit Boards. Blade Terminal with Short-Circuitable (SC) connectors.	**C**	6U x 19" 1/2 Rack. Conformal Coated Circuit Boards. Ring Lug Terminal with Short-Circuitable (SC) connectors.
8	**Slot A**			
	1	24 - 60 VDC (±20%) 16DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO.	**4**	90 - 250 VDC (±20%) and 100 - 240 VAC (-15%/+10%) 16DI (DIs distributed in 4 groups) (2 coil supervision each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO
9	**Slot B**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
10	**Slot C**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
11	**Slot D**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
			I	1V + 2I (Only for models with SC connectors).
12	**Slot E**			
	I	1V + 2I (Only for models without SC connectors).		

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

0	0		0			-
17	18	19	20	21	22	

19	**Communication Interface 1-2 for Remote Communication (PROCOME, MODBUS, DNP3)**			
	A	RS232 Full Modem - RS232/RS485.	**C**	GFO ST - RS232/RS485.
	B	RS232 Full Modem - GFO ST.	**D**	GFO ST - GFO ST.
21	**ETHERNET Interfaces 1 and 2**			
	1	10/100/1000BASE-T Connectors (RJ45).	**3**	100BASE-FX Connectors (Multimode GFO ST).
	2	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).		
22	**ETHERNET Interfaces 3 and 4**			
	0	None.	**2**	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).
	1	10/100/1000BASE-T Connectors (RJ45).	**3**	100BASE-FX Connectors (Multimode GFO ST).

(*) SFP interfaces are considered as accessories and they must be additionally ordered. See Accessories.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.1.c 19" Rack Models

RTF		-									0	0	0	0
1-2-3	4		5	6	7	8	9	10	11	12	13	14	15	16

4	**Functionality**			
	A	Automatic voltage regulator with compensations, tap changer monitoring and parallel transformers operation.		
5	**User Interface**			
	1	Standard with alphanumeric display.	**4**	Extended buttons with graphic display.
	2	Standard with graphic display.		
6	**DI Auxiliary Supply Voltage**			
	A	Selectable by Software	**D**	125 VDC
	B	24 VDC	**E**	250 VDC
	C	48 VDC		
7	**Enclosure/Chassis, Conformal Coat and I/Os terminal blocks**			
	3	6U x 19" Rack. Conformal Coated Circuit Boards. Blade Terminal.	**6**	6U x 19" Rack. Conformal Coated Circuit Boards. Ring Lug Terminal.
	B	6U x 19" Rack. Conformal Coated Circuit Boards. Blade Terminal with Short-Circuitable (SC) connectors.	**D**	6U x 19" Rack. Conformal Coated Circuit Boards. Ring Lug Terminal with Short-Circuitable (SC) connectors.
8	**Slot A**			
	1	24 - 60 VDC (±20%) 16DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO.	**4**	90 - 250 VDC (±20%) and 100 – 240 VAC (-15%/+10%) 16DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO+ 1 Alm. DO.
9	**Slot B**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC)
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
10	**Slot C**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
11	**Slot D**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).	**7**	6 DI (Dis distributed in 2 groups) (2 coil supervision, each one will use one group of 3 DIs) + 6 HSHD DO + 6 DO (2DO NO/NC).
12	**Slot E**			
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**3**	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).
			5	20 DI (all independent).
			6	17 DO (6DO NO/NC).
13	**Slot F**			
	0	None.	**3**	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

RTF		-									0	0	0	0
1-2-3	4		5	6	7	8	9	10	11	12	13	14	15	16

14	**Slot G**			
	0	None.	**3**	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
15	**Slot H**			
	0	None.	**3**	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).
16	**Slot I**			
	0	None.	**3**	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**5**	20 DI (all independent).
			6	17 DO (6DO NO/NC).

			0			-
17	18	19	20	21	22	

17	**Slot J**			
	0	None.	**5**	20 DI (all independent).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA).	**6**	17 DO (6DO NO/NC).
			I	1V + 2I (Only for models with SC connectors)
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC).		
18	**Slot K**			
	0	None (Only for General alarms BCU).	**5**	20 DI (all independent) (Only for General alarms BCU).
	2	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 2 IT (-5 to 20mA) (Only for General alarms BCU).	**6**	17 DO (6DO NO/NC) (Only for General alarms BCU).
			I	1V + 2I (Only for models without SC connectors)
	3	16 DI (DIs distributed in 4 groups) (2 coil supervision, each one will use one group of 3 DIs) + 7 DO (2DO NO/NC) + 1 IT (-5 to 20mA) + 1 IT (0-300VDC) (Only for General alarms BCU).		
19	**Communication Interface 1-2 for Remote Communication (PROCOME, MODBUS, DNP3)**			
	A	RS232 Full Modem - RS232/RS485	**C**	GFO ST - RS232/RS485
	B	RS232 Full Modem - GFO ST	**D**	GFO ST - GFO ST
21	**ETHERNET Interfaces 1 and 2**			
	1	10/100/1000BASE-T Connectors (RJ45).	**3**	100BASE-FX Connectors (Multimode GFO ST).
	2	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).		
22	**ETHERNET Interfaces 3 and 4**			
	0	None.	**3**	100BASE-FX Connectors (Multimode GFO ST).
	1	10/100/1000BASE-T Connectors (RJ45).		
	2	Slot (socket) for SFP* (1000BASE-SX/LX & 100BASE-FX Connectors Multimode GFO LC).		

(*) SFP interfaces are considered as accessories, and they must be additionally ordered. See Accessories.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.1.d Definition of Slots

Slot: each of the vertical layouts of the protection relay. See Chapter 1.5, Physical Description and Chapter 1.9, Schemes and Drawings. 4 slots for 1/3 rack IED and 6 slots for 1/2 rack IED. Possible provisions of the different Slots:

Rack	1/2 19" Rack Models					
Slots	A	B	C	D	E	CPU
Power Supply	**X**					
Inputs / Outputs	**X**	**X**	**X**	**X**		**X**
V / I Analog Channels					**X**	

Rack	1/3 19" Rack Models			
Slots	A	B	C	CPU
Power Supply	**X**			
Inputs / Outputs	**X**	**X**		**X**
V / I Analog Channels			**X**	

The mounting assembling of DI / DO cards from Slot A to Slot K is as follows: Card digit 7 ≥ Card digit 3 ≥ Card digit 2 ≥ Card digit 6.

There are only available models which electronic card arrangement is according to the assembling priority. For example:

Model **F***24326********** available.
Model **F***24236********** not available.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.1.e Accessories

Accessory devices should be ordered if needed. The necessary SFP interfaces must be provided by **ZIV**. All SFP interfaces sold by **ZIV** have been tested and homologated to ensure compatibility of both the application and external standard devices, the operation in temperature range and the optical reach of the same. Therefore, the correct operation of the relays is only guaranteed if SFP interfaces are provided by **ZIV**.

ACCESORIES	REFERENCE
SFP ETHERNET Interfaces	
100BASE-FX Connectors Multimode GFO LC (2 units)	**2 x 4CZ07980007**
Installation	
Iron Angles (right & left) for 1 Rack mounting	**2 x 4PF02090080**
Angles (left and right) for 1 Rack mounting (for 1 equipment of 1/3 rack)	**2 x 4PF02090094**
Angles (left and right) for 1 Rack mounting (for 1 equipment of 1/2 rack)	**2 x 4PF02090095**
Angles (left and right) for 1 Rack mounting (for 2 equipments of 1/3 rack)	**2 x 4PF02090096**
Angles (left and right) for 1 Rack mounting (for 1 equipment of 1/3 rack and 1 equipment of 1/2 rack)	**2 x 4PF02090097**
Iron Sheet for assembling of 2 devices together	**2 x 4PF02090081**
Iron Angles (upper-right & upper-left & lower-right & lower-left) for flush mounting	**4GL01950851**
Kit for IP54	**2 x 4PV01180026 +** **2 x 4PV01180029**

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.2 Firmware Model Selection

			*	*	*	*	*
23	24	25	26	27	28	29	30

23	**Remote Communication Protocols** **2** PROCOME, MODBUS, DNP3.0, IEC 61850 Ed. II
24	**Protection** **0** Initial version.
25	**Customer Code** **Z** Last firmware.
26	**Cybersecurity** **1** Basic Cybersecurity. **3** 1 + Remote authentication (LDAP + RADIUS) + Enhanced firmware securitization + Mutual authentication + HMI authentication + Public Key Infrastructure.
27/28	**Version** **04** Profile 04. **05** Profile 05. **07** Profile 07. **20** Added Syslog Protocol. **28** Unchanged. **29** Unchanged.
29/30	**Ethernet and Serial Ports Communication Version** **40** Communication protocols Ethernet ports: 1 PROCOME instance + 4 configurable instances (PROCOME, DNP3 or MODBUS RTU). IEC61850 Data model 4. Communication protocols (remote port): PROCOME, DNP3 or MODBUS Communication Redundancy: Bonding, RSTP, PRP, HSR. PTP Power Utility Profile IEC61850-9-3. **50** Communication protocols Ethernet ports: 1 PROCOME instance + 4 configurable instances (PROCOME, DNP3 or MODBUS RTU). IEC61850 Data model 5. Communication protocols (remote port): PROCOME, DNP3 or MODBUS. Communication Redundancy: Bonding, RSTP, PRP, HSR. PTP power utility profile IEC61850-9-3. **70** 50 + IEC 61850 Dynamic Data Model + Substitution Service. **72** 70 + Access points management. **73** 72 + New based on IEC 61850 SyslogSoE Event Record (replaces the former SyslogSoE Event Record) + New based on IEC 61850 Fault Report. **74** 73 + selectable Syslog protocol UDP or TCP.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.2.3 Protection Functions according to Model

ANSI	Functions	Units RTF-A 1V+2I
90	Voltage Regulator	1
	LDC (LDC-Z, LDC R-X)	1
	Under Voltage Block with Temporization	1
	Maximum Switching Current Block	1
	Voltage Out of Range Block with Temporization and Reset	1
	Power Reversal Detection	1
	Tap Changer Monitoring	1
59	Phase Overvoltage	1
81m	Underfrequency	1
60VT	VT Supervision	1

- **Analog Channels**

Model	Analog Channels
RTF-A	VCTRL, ILOC; IPAR

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3 Technical Data

1.3.1 Power Supply Voltage 1.3-2
1.3.2 Power Supply Burden 1.3-2
1.3.3 Current Analog Inputs 1.3-2
1.3.4 Voltage Analog Inputs 1.3-2
1.3.5 Frequency 1.3-3
1.3.6 Measurement Accuracy at Environment Temperature (25ºC) 1.3-3
1.3.7 Effect of Temperature in Measurement Accuracy 1.3-5
1.3.8 Repeatability 1.3-5
1.3.9 Accuracy of the AVR Operation Times (T1 and T2) 1.3-5
1.3.10 Accuracy of the Pickup and Reset of the Voltage Elements 1.3-6
1.3.11 Accuracy of the Pickup and Reset of the Frequency Elements 1.3-6
1.3.12 Digital Inputs 1.3-7
1.3.13 Auxiliary Outputs 1.3-7
1.3.14 Input Transducers 1.3-8
1.3.15 Communications Link 1.3-8

1.3.1 Power Supply Voltage

IEDs have two types of auxiliary power supplies. Depending on the model, their values are selectable:

24 - 60 VDC (±20%)
90 - 250 VDC (±20%) & 100 - 240 VAC (-15%+10%)

Note: In case of power supply failure, a maximum interruption of 100 ms is allowed for 110 VDC input.

1.3.2 Power Supply Burden

Quiescent	**15W** DOs activated
Maximum Inrush Current	**<1A** (at **125 VDC**)

1.3.3 Current Analog Inputs

Phase, Neutral and Polarization Currents	
Frequency Range	**50 Hz**, **60 Hz**
Nominal Value	**In** = **5 A** or **1 A** (selectable in the IED)
Measurement Range	**0 - 40 A** x **In**
Thermal Withstand Capability	**4 A** x **In** (continuously)
	30 A x **In** (for 10 s.)
	100 A x **In** (for 1 s.)
Current Circuits Burden	**<0.2 VA** (**In** = **5 A** or **1 A**)

1.3.4 Voltage Analog Inputs

Frequency Range	**50Hz**, **60Hz**
Nominal Value	**Un** = **110 VAC**
Measurement Range	**0 - 300 V**
Thermal Withstand Capability	**300 VAC** (continuously)
	400 VAC (for 10 s.)
Voltage Circuits Burden	**<0.1 VA** (110/120 VAC)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3.5 Frequency

Operating range	**15 - 80 Hz**

1.3.6 Measurement Accuracy at Environment Temperature (25ºC)

Measured currents Phase	**±0.25%** or **±2 mA** (the greater) for 0.1*Inom≤I<1*Inom **±0.2%** for 1*Inom≤I≤5*Inom
Calculated currents Circulating Current	**±0.3%** or **±8 mA** (the greater) for 0.1*Inom<I≤5*Inom
2^{nd}, 3^{rd}, 4^{th} and 5^{th} Harmonic currents	**±1%** or **±20 mA** (the greater) For In = 1A and 5A
Measured voltages Phase-Ground	**±0.2%** or **±50 mV** (the greater) for 0.2 V≤V<130 V **±0.25%** for 130 V≤V≤250 V
Calculated voltages Compensating Setpoint Voltage	**±0.3%** or **±75 mV** (the greater) **±0.3%** or **±100 mV** (the greater) for 0.2 V≤V≤250 V
Active and reactive powers (In = 1A and 5A e I_{phases}>1A calculated as 3 times the single-phase power) Minimum current required to calculate the Power	**±0.33% W/Var** (0º or ±90º or 180º) **±1.6% W/Var** (±45º or ±135º) **±5% / 0.65% W** (±75º / ±115º) **10mA**
Angles Phase Current Sequence Currents (I1 and I2) Voltage	 **±0.5º** for **0.1 A> I <25 A** **±1º** for **60 mA> I <100 mA** **±0.5º** for **0.1 A> I <25 A** **±1º** for **20 mA> I <100 mA** **±0.5º** for **0.2 V> V <250 V** **±1º** for **50 mV> I <200 mV**
Power Factor	**±0.013**
Frequency	**±0.005 Hz** for **41<Fq<69Hz**

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Signal Processing

Sampling function adjustment of analog input signals is made by means of zero pass count of one of the measured signals (Cosine filter of Clark alpha component voltage, difference between channels or direct magnitude of the channel), and works detecting the change in said signal period. The value of the calculated frequency is used to modify the sampling frequency used by the metering device attaining a constant sampling frequency of 80 samples per cycle. The frequency value is saved for later use in Protection and Control tasks.

Zero passage detection is carried out depending on the number of channels the IED has:

***IEDs with three channels**: the Vclark cosine signal ((2VA - VB – VC)/3) is used, and when the value of the combination of Vclark and Vcosine drops below the disable voltage setting, the frequency measurement becomes impossible.*

***IEDs with two channels**: the magnitude calculated as the difference between both channels is used.*

***IEDs with one channel**: the magnitude of the channel itself with no additional calculations is used.*

Upon losing this voltage, the following will be carried out:

The last valid frequency is kept for two seconds.

After two seconds, the frequency measurement goes to zero.

When Protection and Control tasks are readjusted in accordance with the sampling function, phasor real and imaginary components of analog signals are calculated by means of the Fourier transform. Fourier components are calculated by means of said Discrete Fourier Transform (DFT) using 80 sample/cycle. Using DFT this way the magnitude and phase angle of the fundamental component at power system frequency of every analog input signal is obtained. The rest of measurements and calculations of Protection functions is obtained based on the fundamental components calculated by the Fourier method. DFT gives a precise measurement of the fundamental frequency component and it is an efficient filter for harmonics and noise.

For frequencies other than the rated frequency, harmonics are not fully attenuated. For small deviations of ±1Hz this is not a problem but, in order to admit higher operating frequency deviations, the setting automatic conversion to the sampling frequency, PLL, is included. In the absence of an adequate signal to carry out the conversion of the sampling frequency or with the setting PLL disabled, the frequency will be converted to the rated frequency at which the relay is operating (50/60Hz).

Angle reference for relay measurements is the channel VA or IA as per the setting.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3.7 Effect of Temperature in Measurement Accuracy

Temperature Range	**-25ºC** to **70ºC** (operating range)
Measured Currents Any current channels	for 0.1*Inom≤I<1*Inom **±0.35%** for -25ºC ≤x≤20ºC for 1*Inom≤I≤5*Inom **±0.15%** for -25ºC ≤x≤5ºC
Measured Voltages Any voltage channel	for 0.2 V≤V<1 V **±0.35%** for 40ºC ≤x≤70ºC for 1 V≤V≤250 V **±0.1%** for -25ºC ≤x≤-5ºC

Note: These error margins will be added to the measurement accuracy at environment temperature ones. In the temperature range which is not defined, the measurement accuracy is not affected.

1.3.8 Repeatability

Operating Time	**2 %** or **25 ms** (the greater)

1.3.9 Accuracy of the AVR Operation Times (T1 and T2)

Mode	Measuring Times
Inverse Curve (T1) Fixed Time (T1 and T2)	±2% of setting or ±25 ms (the greater)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3.10 Accuracy of the Pickup and Reset of the Voltage Elements

Overvoltage Elements

Pickup (static test)	**±2%** or **±250 mV** of the theoretical value (the greater)
Reset	**1.5 cycles** for 50 and 60Hz (*)

(*) If the reset time is measured using electromechanical DOs there will be an extra increment of up to ½ cycle.

Measuring Times

Mode	Time Setting	Measuring Times	
		50Hz	60Hz
Fixed Time	0 s	14.5 ms	16 ms
Fixed Time	> 0 s	±1% of the setting or ±25 ms (the greater)	

1.3.11 Accuracy of the Pickup and Reset of the Frequency Elements

Underfrequency Elements	
Pickup and reset	**±0.005 Hz** of the theoretical value for **41<Fq<69 Hz**
	±0.01 Hz of the theoretical value for **Fq<41** and **Fq>69 Hz**
Measuring Times	
Fixed Time	**±1%** of the setting or **±25 ms** (the greater)

The total trip time is equal to the adjusted fixed time plus the time defined in "Activation Half-time" (see 3.2, Frequency Units).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3.12 Digital Inputs

Configurable inputs (depending on the setting) with polarity (all the Inputs are DC are isolated by octocoupler).

Nominal Voltage	Maximum Voltage	Burden	V ON / OFF
24 VDC (*)	48 VDC	38 mW	Configurable (See 1.5.6.a)
48 VDC (*)	90 VDC	75 mW	Configurable (See 1.5.6.a)
125 VDC (*)	300 VDC	195 mW	Configurable (See 1.5.6.a)
250 VDC (*)	300 VDC	390 mW	Configurable (See 1.5.6.a)

The use of any of the SLOTS (A and/or B) digital inputs for coil supervision is as follows:

Trip Circuit supervision: use inputs **ED11**, **ED12** and **ED13** of the corresponding SLOT.
2 Circuit supervision: use inputs **ED14**, **ED15** and **ED16** of the corresponding SLOT.

1.3.13 Auxiliary Outputs

All relay contacts have the same physical features and all are configurable with the exception of the relay in service /failed.

I DC maximum limit (with resistive load)	**60 A** 1s
I DC continuous service (with resistive load)	**16 A**
Close	**5000 W**
Breaking capability (with resistive load)	**72 W** (**1.5 A - 48 VDC**)
	60 W (**0.5 A - 125 VDC**)
	75 W (**0.3 A - 250 VDC**)
Break (L/R = 0.04 s)	**120 W** at **125VDC**
Switching voltage	**250 VDC**
Momentary close time trip contacts remain closed	**100 ms**
Break delay	**<150 ms**

Contact Performance Test according to ***IEC60255-1 6.11***.

Mechanical endurance unloaded	**10000 cycles**.
Making capacity	**125 VDC** / **8.05 A** / **1006 W** / **R/L 0.04** / **1000 cycles**.
Breaking capacity	**125 VDC** / **0.242 A** / **30.3 W** / **R/L 0.04** / **1000 cycles**.
Continuous contact current	**5 A** / **125 VDC**.
Short time contact current	**30 A** / **125 VDC** / **Ton 200 ms** / **Toff 15 s** / **1000 cycles**.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.3.14 Input Transducers

-20mA to 20mA Input Transducers

Input impedance	**196 Ω ±5%**
Measurement accuracy	**±0.2 %** or **±10 µA** (the greater)

10V to 350V Voltage Transducer

Input impedance	**150 kΩ ±10%**
Measurement accuracy	**±0.2 %** or **±0.2 V** (the greater)

1.3.15 Communications Link

Local Communications Port

USB type B 2.0 (connection with configuration tool).
USB type A 2.0 (host for uploading and downloading IEC 61850 files).

Serial Remote Communications Port (GFO, RS232-Full Modem, or RS232/RS485)
LAN Port (RJ45/ST/LC)

Glass Fiber Optics (Remote Ports)

Type	**Multimode**
Wavelength	**820 nm**
Connector	**ST**
Transmitter minimum power	
50/125 Fiber	**- 20 dBm**
62.5/125 Fiber	**- 17 dBm**
100/140 Fiber	**- 7 dBm**
Receiver sensitivity	**- 25.4 dBm**

RS232 Port Signals (Remote Ports)

DB 9 (9 pin) connector. Used signals	**Pin 5 - GND**
	Pin 2 - RXD
	Pin 3 - TXD

RS485 Port Signals (Remote Ports)

DB 9 (9 pin) connector. Used signals	**Pin 4 - (A) TX+ / RX+**
	Pin 6 - (B) TX- / RX-

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

RS232 Full Modem Port Signals (Remote Ports)

DB 9 (9 pin) connector. Used signals

Pin 1 - DCD
Pin 2 - RXD
Pin 3 - TXD
Pin 4 - DTR
Pin 5 - GND
Pin 6 - DSR
Pin 7 - RTS
Pin 8 - CTS
Pin 9 - RI

Transmission via RJ45, 10/100/1000BASE-T (Ethernet Port)

Transmission with SFP modules (Ethernet Port)

Transmission via GFO with ST 100BASE FX Connector (Ethernet Port)

IRIG-;

B00X	**B12X**
B: 100pps	B: 100pps
0: By pulse width	1: Amplitude modulated wave
0: Without carrier	2: 1kHz/1ms
X: 0,.., 7	X: 0,.., 7

X: 0 (BCD, CF, SBS); 1 (BCD, CF); 2 (BCD); 3 (BCD, SBS); 4 (BCD, BCD, CF, SBS); 5 (BCD, BCD, CF); 6 (BCD, BCD); 7 (BCD, BCD, SBS).

BNC Type Connector

Input impedance	**211 Ω**
Maximum input voltage	**10 V**
Synchronization accuracy	**± 1ms**

When the IED is receiving an IRIG-B signal for synchronization both Date and Time settings will not be available through the HMI. Synchronization by IRIG-B has priority over any other synchronization method.

It is possible to configure one of the auxiliary outputs to check the IRIG-B signal status. This output will remain active as long as the IRIG-B signal reception is correct.

All the devices are also designed to give an indication for both the loss and recovery of such IRIG-B signal by generating the particular event.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.4 Current Transformers Dimensioning

1.4.1	Introduction	1.4-2
1.4.2	CT Dimensioning According to Different Standards	1.4-2
1.4.2.a	Class P of IEC 61869-2 Standard	1.4-2
1.4.2.b	Class C of IEEE C57.13 Standard	1.4-4
1.4.2.c	Class X of BS3938 Standard or Class PX of IEC61869-2	1.4-5
1.4.3	CT Dimensioning for Different Protection Functions	1.4-6
1.4.3.a	Remanence Factor	1.4-7
1.4.3.b	Ktf Factor	1.4-8

1.4.1 Introduction

When dimensioning the Current Transformers (CTs), several factors are taken into account that influence the level of flux generated in the CT itself and, therefore, the tendency of the same to saturate. These include: load, internal resistance, incidence angle of the fault, primary and secondary time constants, remanence, etc.

The following points describe the data provided by different CT standards and the factors that must be calculated for the CT dimensioning

1.4.2 CT Dimensioning According to Different Standards

1.4.2.a Class P of IEC 61869-2 Standard

The CT is specified with the following data:

- Rated transformation ratio: the ratio of the rated primary current to the rated secondary current, e.g 600/5.
- Rated power: power provided by the CT at rated current and rated burden, e.g 10 VA.
- Accuracy class: 5P and 10P defines a maximum composite error of 5% or 10% at the accuracy limit current (accuracy limit factor (ALF) multiplied by the rated current).
- Accuracy limit factor: times the rated current, without DC offset, at which the accuracy class is fulfilled.
- Secondary internal resistance.

The CT will be adequate if K_total=Kssc*Kb*Ktf*Krem<ALF, where

Kssc: symmetrical short-circuit current factor.
Kb: burden factor.
Ktf: overdimensioning factor for DC offset.
Krem: remanence overdimensioning factor.

- **Symmetrical Short-Circuit Current Factor (Kssc)**

It is the ratio between the maximum short circuit current and the rated current.

- **Burden Factor (Kb)**

It is the ratio (Rct+Rburden)/(Rct+Rn), where:

Rn is the rated burden. Rn can be calculated from the CT rated power:

$$Rn = \frac{Pn}{I2n^2}$$

Rct: is the internal secondary resistance of the CT.
Rburden: is the burden resistance.
I2n: is the rated secondary current.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The accuracy limit factor is defined for the rated burden. For a different burden the maximum symmetrical current that assures the fulfillment of the accuracy class will be different than the accuracy limit current (it will be higher than the accuracy limit current if the burden is lower than the rated one and it will be lower if the burden is higher than the rated one). This condition is taken into account by the burden factor.

- **Transient Overdimensioning Factor (Ktf)**

The flux created by a current with DC offset (asymmetrical current) is much higher than the flux generated by a current without any DC component (symmetrical current). As the ALF factor is defined for a symmetrical current, an overdimensioning factor for asymmetrical currents must be considered. This factor will be given by $\frac{\phi_{\text{MAX AC+DC}}}{\phi_{\text{MAX AC}}}$,which represents the ratio between the maximum total flux (sum of DC and AC fluxes) and the maximum AC flux. Ktf is calculated with the following formula:

$$Ktf = \frac{w \cdot T1 \cdot T2}{T1 - T2} \cdot \cos\theta \cdot (e^{\frac{-t}{T1}} - e^{\frac{-t}{T2}}) + \sin\theta \cdot e^{\frac{-t}{T2}} - \sin(wt + \theta) \qquad \text{(1.4.1), where}$$

T1 is the primary time constant.
T2 is the secondary time constant.
t is the saturation free time or time to saturation.
θ is the fault inception angle.

For saturation free times higher than 15 ms, the maximum flux will be obtained with $\theta = 0$, however, for saturation free times lower than 15 ms, the maximum flux will be obtained for other fault inception angles.

For each saturation free time tolerated by the protection function the worst inception angle should be determined.

- **Remanence Overdimensioning Factor (Krem)**

The remanent flux may worsen the CT transient response if it has the same sign of the flux generated by the current magnitude, burden value and DC offset. This is considered by the remanence overdimensioning factor $Krem = \frac{1}{(1 - Kr)}$, where Kr is the remanent factor (maximum remanent flux / saturation flux).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.4.2.b Class C of IEEE C57.13 Standard

The most common accuracy class in the IEEEC57.13 standard is the C class. The letter C is followed by a number that indicates the secondary voltage rating, which is defined as the CT secondary voltage that the CT will deliver when it is connected to a standard secondary burden at 20 times the rated secondary current, without exceeding a 10% ratio error. The common standard burdens for protection CTs are 1, 2, 4 and 8 ohms, which correspond, at 5 A rated current, to 100, 200, 400 and 800 V secondary rating voltages (for a C100 CT the voltage at the 1 ohm burden will be 20*5*1=100 V).

With the secondary voltage rating (burden voltage - Vb) we can obtain the internal magnetizing voltage by adding the voltage drop in the secondary resistance (Rct):

$$Emrated=Vb+Rct*20*I2n$$

The dimensioning of an IEEE CT can be done by calculating Em as:

$$Emcalc=Ktotal'*I2n*(Rct+Rb),$$

where Ktotal'=Kssc*Ktf*Krem.

If Emcalc<Emrated= Vb+Rct*20*I2n the CT will be valid

An easier deduction can be made considering that the ALF factor of a C class CT is always 20 (the 10% ratio error cannot be exceeded for a secondary current 20 times the rated current with the rated burden). If Ktotal<ALF the CT will be valid.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.4.2.c Class X of BS3938 Standard or Class PX of IEC61869-2

Class X CT is defined with:

- Primary and secondary rated currents.
- Transformation ratio.
- Rated knee-point voltage.
- Magnetizing current at rated knee-point voltage.
- Resistance of secondary winding.

The rated knee-point voltage is defined as the minimum voltage, at rated frequency, applied to the CT secondary terminals which increased by a 10% causes an increase in the magnetizing current of 50% (see Figure 1.4.1).

The relationship between the rated knee-point voltage (Vknee) and the magnetizing voltage at the accuracy limit current with rated burden (Emrated) is done by approximation, because the definition of the two voltages has no direct relation (Vknee has to do with the slope of the magnetizing characteristic and Emrated with the current composite error). It is normally considered that Emrated=(1.25 – 1.3)*Vknee.

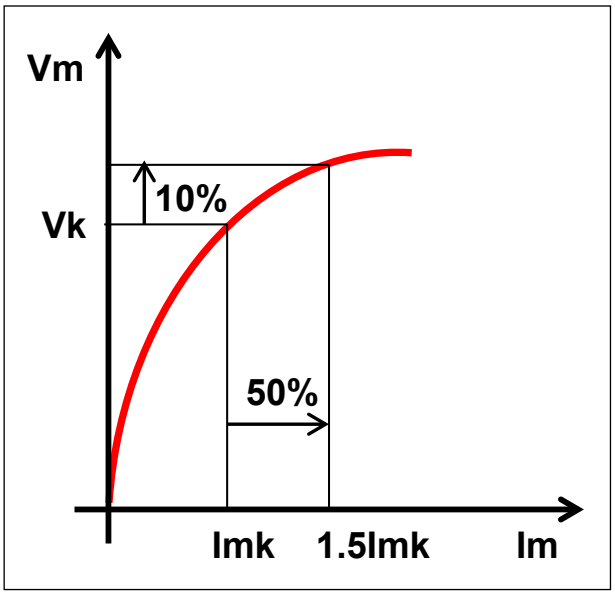


Figure 1.4.1 Knee Point Voltage Definition.

Once Emrated is calculated it can be compared with Emcalc= Ktotal'*I2n*(Rct+Rb). The CT will be valid if Emcalc<Emrated.

where Ktotal'=Kssc*Ktf*Krem

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.4.3 CT Dimensioning for Different Protection Functions

Table 1.4-1 includes general parameters to be considered for the calculation of CT dimensioning factors.

Table 1.4-2 includes the saturation free times (for Ktf calculation) and current values (for Kssc calculation) that must be used for CT dimensioning.

Table 1.4-1: General Parameters

Data	Description	Units
f	Frequency (50 or 60 Hz)	(Hz)
IF	Maximum primary fault current (single phase fault current or three phase fault current, the highest one). It depends on the protection function – see Table 1.4-2	(A)
CT ratio	I1n/I2n	
I1n	Primary nominal current	(A)
I2n	Secondary nominal current	(A)
T1	Primary time constant = L/R (taking into account the total impedance from the source to the fault location).	(s)
T2	Secondary time constant (CT time constant) (Usual value = 3 s)	(s)
Rn	CT nominal resistance	(ohms)
Rct	CT internal resistance For CTs of 5 A nominal current, the Rct is around 0.2 ohms to 0.4 ohms. For the CTs of 1 A nominal current, the Rct is higher (10 ohms for example).	(ohms)
Rb	CT burden resistance = Relay burden + Cable resistance	(ohms)
	Cable resistance = 2·RL (if the maximum primary fault current belongs to a single phase fault). Cable resistance = RL (when the maximum primary fault current belongs to a 3 phase fault). RL = ρ · (L/S) ρ = resistivity (mm^2*Ω/m) S = cable section (m^2) L = cable length (m)	(ohms)
	Relay burden = (0.2 VA) / ($I2n^2$)	(ohms)
t	Required saturation free time (depends of the protection function – see Table 1.4-2)	(s)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.4-2: Saturation Free Time and Fault Current Values				
Protection Function	**Fault Scenarios to be considered**	**t (s) = the time (seconds) from the fault start until the CT becomes saturated.**		**IF (fault current to calculate Kssc)**
		f = 50 Hz	f = 60 Hz	
87	External fault in the busbar (giving maximum fault current)	$3x10^{-3}$ (s)	$2.5x10^{-3}$ (s)	$IF = IF_{max_external}$ Maximum fault current for external fault
87N	External fault in the busbar (giving maximum fault current)	$4x10^{-3}$ (s)	$3.5x10^{-3}$ (s)	$IF = IF_{max_external}$ Maximum fault current for external fault
50	Internal fault giving a fault current equal to the pick-up value	It depends on the primary constant, however, it is always lower than $10x10^{-3}$ (s)	It depends on the primary constant, however, it is always lower than $8.3x10^{-3}$ (s)	$IF = IF_{pickup50}$ (instantaneous overcurrent unit pickup in primary value). $\mathbf{IF_{pickup50} \approx 0.7 \cdot (IF_2)}$ $\mathbf{IF_2}$=the fault current to be detected by 50 overcurrent protection. It is normally the fault current at 50%-80% of the feeder. **Note 1**: The 0.7 factor is introduced to compensate CT errors, relay errors and short circuit calculation errors. **Note 2**: If the current IF_2 is not known, a first approximation could be done taking $\mathbf{IF_1}$ **instead of** $\mathbf{IF_2}$; Being $\mathbf{IF_1}$= 80% of the fault current at 0% of the feeder (maximum short circuit current) = 80% ($\mathbf{IF_{0\%}}$)
	Internal fault at 0% of the line	It depends on the primary constant, however, it is always lower than $7.4x10^{-3}$ (s)	It depends on the primary constant, however, it is always lower than $6 x10^{-3}$ (s)	$IF = IF_{0\%}$
21	Internal fault at 0% of the line	$8.4x10^{-3}$ (s)	$7 x10^{-3}$ (s)	$IF = IF_{0\%}$
	Internal fault at 100% of the line	$15x10^{-3}$ (s)	$12.5x10^{-3}$ (s)	$IF = IF_{100\%}$
	Internal fault at the limit of zone 1 reach (normally 80% of the line).	$25x10^{-3}$ (s)	$21x10^{-3}$ (s)	$IF = IF_{80\%}$

1.4.3.a Remanence Factor

Remanence factor is not considered for overcurrent and distance protection. For the mentioned functions Krem=1.

For the rest of the functions Kr=75%-->Krem=4.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.4.3.b Ktf Factor

The following tables include different ktf values calculated according to the formula (1.4.1). The saturation free times included in table 2 are considered together with the worst inception angles (θ). T2 is considered equal to 3 s.

Function	T1 (s)	K_{tf}
87T	0.01-0.3	0.43

Function	T1 (s)	K_{tf}
87N	0.01-0.3	0.58

Function	T1 (s)	K_{tf_pickup} 60 Hz	K_{tf_pickup} 50 Hz	$K_{tf_0\%}$ 60 Hz	$K_{tf_0\%}$ 50 Hz
50	0.01	1	1	1	1
	≤ 0.02	1	1	1	1
	≤ 0.03	1.15	1.15	1	1
	≤ 0.04	1.48	1.48	1	1
	≤ 0.05	1.6	1.6	1	1
	≤ 0.08	1.9	1.9	1	1
	≤ 0.1	2.1	2.1	1	1
	≤ 0.2	2.4	2.4	1	1
	≤ 0.3	2.5	2.5	1	1

Function	T1 (s)	$K_{tf\ zone1}$ 60 Hz	$K_{tf\ zone1}$ 50 Hz	$K_{tf\ 100\%}$ 60 Hz	$K_{tf\ 100\%}$ 50 Hz	$K_{tf\ 0\%}$ 60 Hz	$K_{tf\ 0\%}$ 50 Hz
21	0.01	4.3	3.9	3.8	3.6	2.3	2.3
	≤ 0.02	5.9	5.5	4.6	4.4	2.6	2.5
	≤ 0.03	6.6	6.3	4.9	4.8	2.7	2.6
	≤ 0.04	7.15	6.8	5.1	5	2.7	2.7
	≤ 0.05	7.46	7.2	5.3	5.2	2.7	2.7
	≤ 0.1	8.14	7.9	5.5	5.5	2.8	2.8
	≤ 0.2	8.5	8.4	5.6	5.6	2.8	2.8
	≤ 0.3	8.6	8.5	5.7	5.7	2.8	2.8

NOTE: For overcurrent and distance functions, Ktotal must be calculated for each of the cases considered (fault at 0% and fault with Ifault=Ipick-up for overcurrent; fault at 0%, 80% and 100% of the line for distance). The maximum value of Ktotal must be used to compare against ALF.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Overcurrent

$$Ktotal_{0\%}=Kssc_{0\%}*Kburden*Ktf_{0\%}*Krem$$

$$Ktotal_{pick\text{-}up}=Kssc_{pick\text{-}up}*Kburden*Ktf_{pick\text{-}up}*Krem$$

$$Ktotal=max(Ktotal_{0\%}, Ktotal_{pick\text{-}up})$$

Distance

$$Ktotal_{0\%}=Kssc_{0\%}*Kburden*Ktf_{0\%}*Krem$$

$$Ktotal_{80\%}=Kssc_{80\%}*Kburden*Ktf_{80\%}*Krem$$

$$Ktotal_{100\%}=Kssc_{100\%}*Kburden*Ktf_{100\%}*Krem$$

$$Ktotal=max(Ktotal_{0\%}, Ktotal_{80\%}, Ktotal_{100\%})$$

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5 Physical Description

1.5.1 General 1.5-2
1.5.2 Dimensions 1.5-5
1.5.3 Connection Elements 1.5-6
1.5.3.a Terminal Blocks 1.5-6
1.5.3.b Removing Printed Circuit Boards (Non Self-shorting) 1.5-7
1.5.3.c Internal Wiring 1.5-7
1.5.4 Local Interface 1.5-8
1.5.4.a Display and Keypad 1.5-8
1.5.4.b Keypad associated to the Alphanumeric Display 1.5-11
1.5.4.c Command Buttons 1.5-12
1.5.4.d Keys, Functions and Operation Modes 1.5-12
1.5.4.e Access to Options 1.5-16
1.5.5 Symbols associated to the Graphic Display 1.5-18
1.5.6 LEDs 1.5-19
1.5.7 Inputs and Outputs 1.5-20
1.5.7.a Digital Inputs 1.5-20
1.5.7.b Auxiliary Outputs 1.5-26
1.5.7.c Digital Inputs, Auxiliary Outputs and LEDs Test 1.5-27
1.5.8 Communications 1.5-28
1.5.8.a Communications Ports 1.5-28
1.5.8.b LEDs associated to the Communications Ports 1.5-29
1.5.8.c Communication with the Configuration Tool 1.5-29
1.5.8.d Communication Protocols 1.5-30
1.5.8.e Control Change Recording 1.5-30
1.5.8.f Ethernet Redundancy 1.5-31
1.5.8.g Communications Settings 1.5-36
1.5.8.h Output Signals of the Communications Module 1.5-48
1.5.9 Time Synchronization 1.5-50
1.5.9.a Manual Time Synchronization 1.5-50
1.5.9.b Time Synchronization by Protocol 1.5-50
1.5.9.c Synchronization by SNTP 1.5-50
1.5.9.d Synchronization by IRIG-B 123 and 003 ..... 1.5-50
1.5.9.e PTP Synchronization 1.5-51
1.5.9.f Synchronization Settings 1.5-51
1.5.9.g Output Signals of the Synchronization Module 1.5-53

1.5.1 General

The equipments are made up of the following modules:

- Processor module and HMI.
- Analog inputs module.
- Power Supply.
- Digital inputs, outputs and transducers inputs module.
- Communications module.

The modules are mounted vertically, constituting removable modules that do not require disassembling the front of the equipment. External connection is carried out by means of plug-in terminal blocks (supported on the bearing strip located at the back of each module) for ring lug connectors in case of analogical inputs, and pointed hubs for digital inputs and outputs and for transducer inputs.

Depending on the terminal configuration, all the inputs / outputs contacts may be used or some may remain as spare signals.

Next figures represent the external appearance of the IEDs for 1/3 rack of 19" and 6U standard height. The alphanumeric / graphic keypad and display, the local communication port (USB-B, USB-A), the local control buttons and the LED targets are mounted on the front part of the equipment.

Models with Standard Display (model digit 5 = 1 or 2) feature 6 configurable bicolor LEDs (green/red) associated with the command buttons P1-P6.

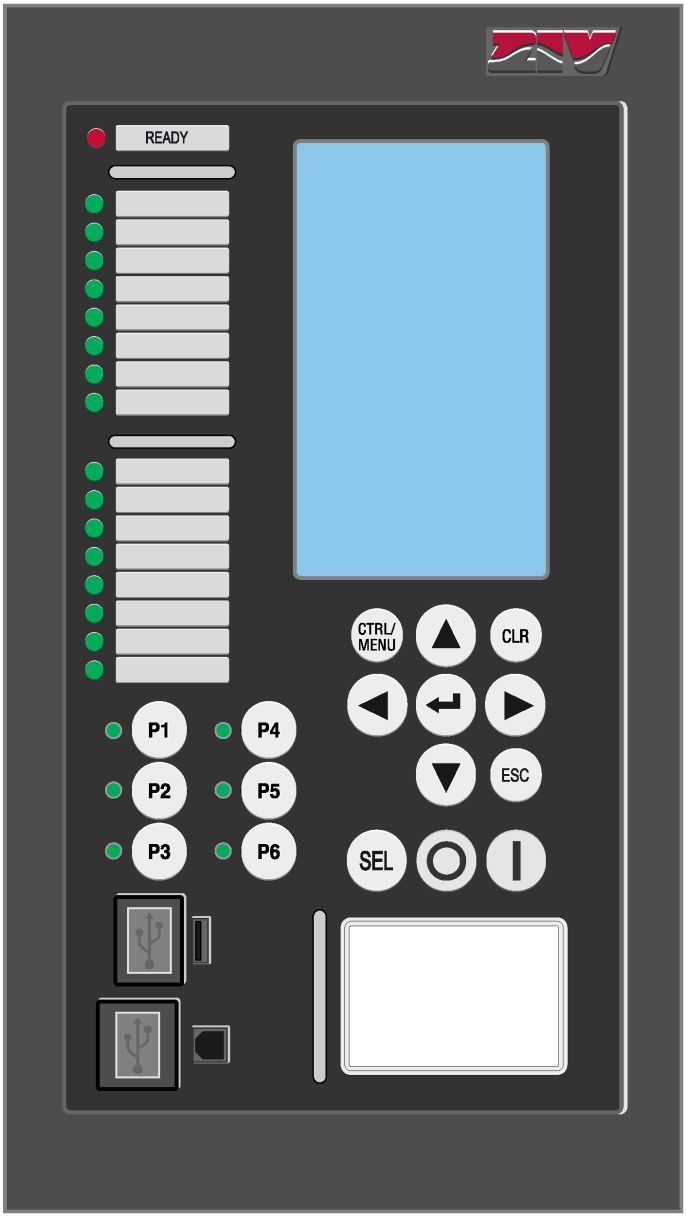


Figure 1.5.1 Front of a 6U x 19" 1/3 Rack Model.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Models with Extended Buttons Display (model digit 5 = 4) feature 12 configurable bicolor LEDs (green/red) associated with the command buttons P1-P12, plus other 2 configurable LEDs (fixed red) associated with the Local/Remote (L/R) button. For this model, only the alphanumeric display option is available.

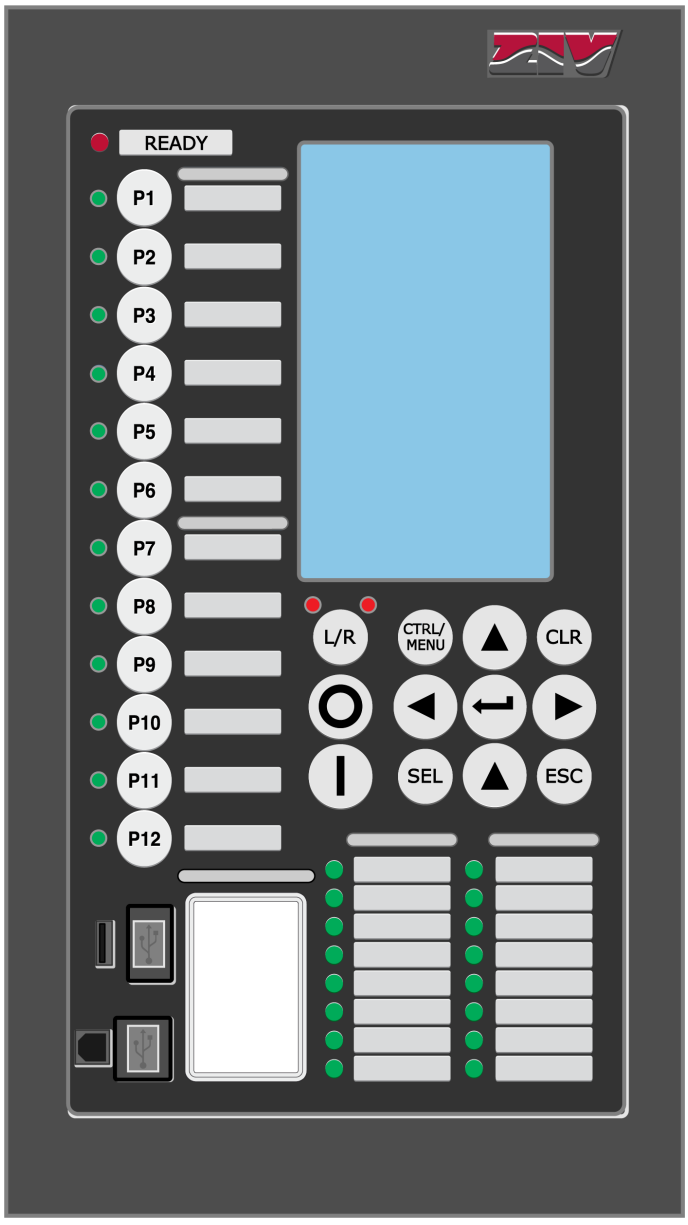


Figure 1.5.2 Front of a 6U x 19" 1/3 Rack Model with Extended Buttons Display.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

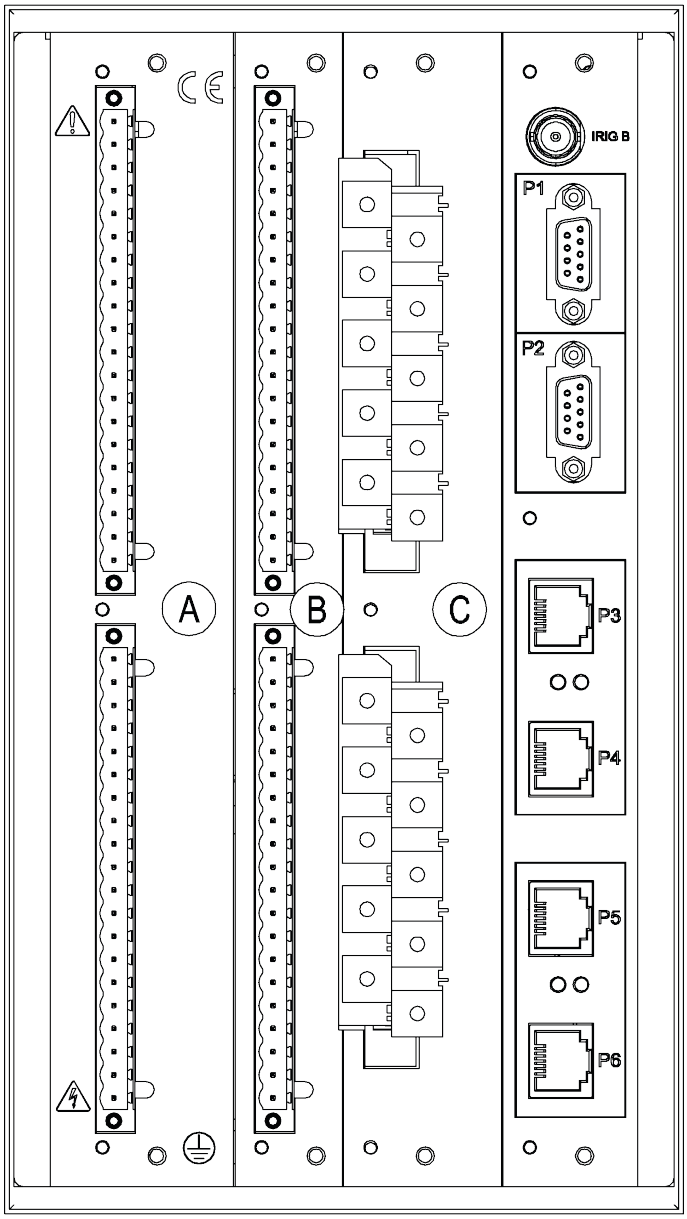


Figure 1.5.3 Rear of a 6U x 19" 1/3 Rack Model.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.2 Dimensions

Depending on the model, the IEDs are mounted as follows:

- Models in enclosures of 1/3 19"-, 6 standard units high.
- Models in enclosures of 1/2 19"-, 6 standard units high.

Relays are designed for panel flush mounting or in cabinet racks. The box is graphite grey. Below are shown several combinations for mounting the equipments.



Figure 1.5.4 Three 6U x 19" 1/3 RTF Rack Mounted.

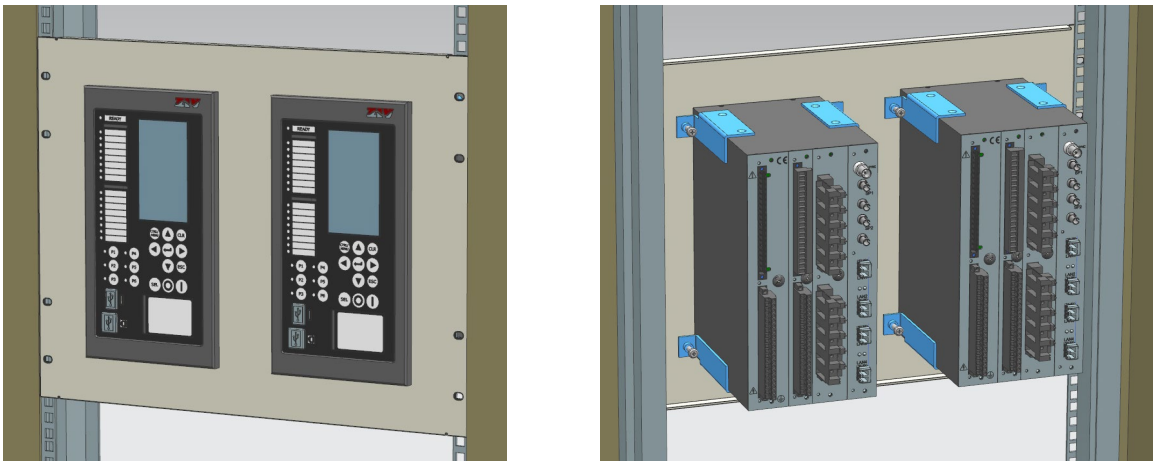


Figure 1.5.5 Mounting two RTF to Steel Plate (built-in into the cell).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.3 Connection Elements

1.5.3.a Terminal Blocks

The number of connectors of the relay depends on the number of analogical inputs and the digital inputs / outputs of the specific model. Relays without connector will have a cover in its place.

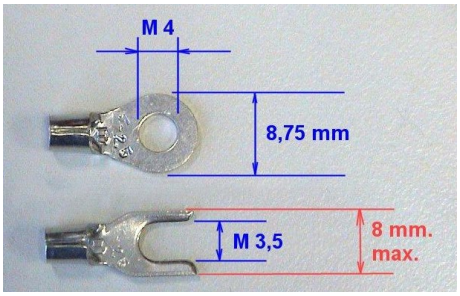
Strips are arranged vertically as shown in figure. Terminal arrangement by columns is as follows:

- **SLOT A**: 2 terminal blocks of 20 terminals for relay auxiliary power supply, digital inputs and outputs, including the internal relay in anomaly output.
- **SLOT B**: 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT C** (1/3 rack and 1/2 rack equipment):
  - 1/3 Rack equipment: 1 terminal block with up to 10 analog channels or 1 terminal block of 20 terminals to connect digital inputs and outputs.
  - 1/2 rack and 1 rack equipment: 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT D** (1/2 rack and 1 rack equipment):
  - 1/2 rack equipment: 1 terminal block with up to 10 analog channels or 1 terminal block of 20 terminals to connect digital inputs and outputs.
  - 1 rack equipment: 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT E** (1/2 rack and 1 rack equipment):
  - 1/2 rack equipment: 1 terminal block with up to 10 analog channels or 1 terminal block of 20 terminals to connect digital inputs and outputs.
  - 1 rack equipment: 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT F** (only 1 rack equipments): 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT G** (only 1 rack equipments): 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT H** (only 1 rack equipments): 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT I** (only 1 rack equipments): 1 terminal block with up to 10 analog channels or 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT J** (only 1 rack equipments): 1 terminal block with up to 10 analog channels or 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT K** (only 1 rack equipments): 1 terminal block with up to 10 analog channels or 2 terminal blocks of 20 terminals to connect digital inputs and outputs.
- **SLOT CPU**: communications ports and synchronization (IRIG-B, 2 Serial Ports, up to 4 LAN Ports).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The ring lug terminals corresponding to the current analog inputs take wires up to #10 AWG (6 mm^2). We recommend ring lug terminals for these connections.

The connectors are plug-in and not self-shorting. They can be assigned to the current circuits supporting a current of 20 A continuously.



The terminals of the 20 terminals block admit a #13 AWG (2.5 mm^2) cable in the case of pin terminals and cables between 2.5 and 4 mm^2 in the case of the ring lug terminals. Use of pin terminals is recommended to connect to connectors.

1.5.3.b Removing Printed Circuit Boards (Non Self-shorting)



The IED's printed circuit board can be taken out. **WARNING: the current connector is non self-shorting. Consequently, the CT secondaries must be short-circuited externally before board removal.**

The back plate and the printed circuit board are attached to the case with self-tapping screws. These screws must be removed before the board is withdrawn. This operation always requires the protection to be **not in service**.

1.5.3.c Internal Wiring

The equipment uses traditional printed circuit board connections and internal buses to minimize internal wiring.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.4 Local Interface

1.5.4.a Display and Keypad

There are two display options (as per model selection): Alphanumeric display and alphanumeric and graphical display.

Alphanumeric Display has a screen resolution of 128x64 with capacity for 6 lines and 20 characters per line.

You can visualize alarms, settings, measurements, status, etc. from the display.

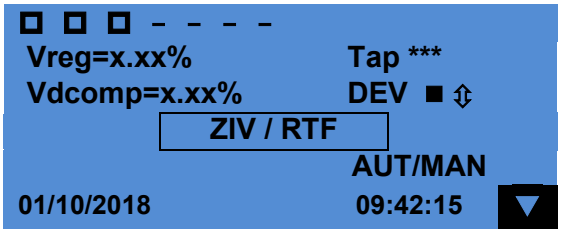


Figure 1.5.6 Alphanumeric Display.

The graphic display has a resolution of 272x480 to show the screens that have been configured in the relay user logic (single line, alarm screens, etc.), as well as the status of all digital inputs and outputs.

In the following chapters it will be explained how, by means of the CTRL/MENU button, the user can switch from the graphical display to the protection menu where it can be visualized all the information given by the alphanumeric display.

- **Default Display**

Default Alphanumeric Display: presents the model, the date and time and the status of the front communications port, serial remote port, LAN port and protocol instances through the LAN port.

Default Graphic Display: shows the single line diagram programmed in the user logic. If no single line diagram is available, the home screen will show the relay model, the date and time.

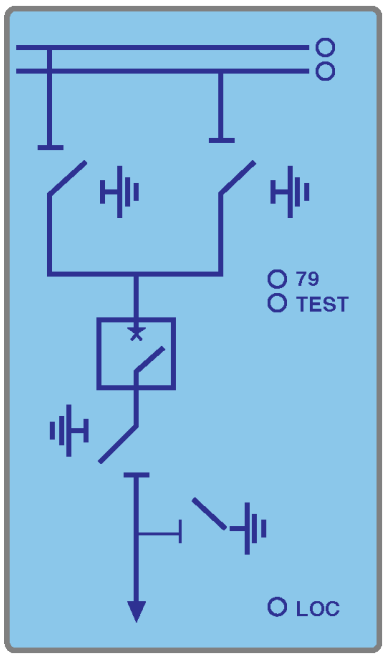


Figure 1.5.7 Graphic Display.

If no activity is detected by the relay during the time set in ***Display Time***, it will automatically return to the home screen.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Below the display the scroll keys shown in Figure 1.5.8 are located. They explained in the following sections.

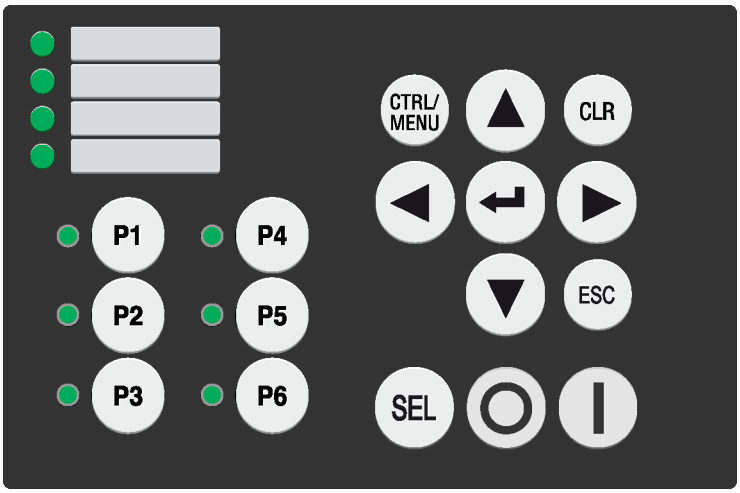


Figure 1.5.8 Keypad.

- **Command Panel Screen (associated with the alphanumeric display)**

The equipments are provided with a graphic screen for HMI commands, which can be accessed pressing **SEL** button, and where the status of different elements can be displayed and commands can be configured by ***ZIV e-NET tool***®. Once on the screen, the user can press again the **SEL** key to switch between different commands and controls that have been configured. In order to operate the command, it must be selected (blinking) and at that moment the close (I) or open (O) key will be pressed depending on ~~of~~ the action the user wants to operate over the selected command.

As commented before, access to the command panel is gained through the **SEL** key. The different commands can be scrolled using also the **SEL** key. The selected command blinks and the text configured for activation and deactivation of the command is displayed on the bottom part. In this blinking state, press the open or close keys to carry out the desired action.

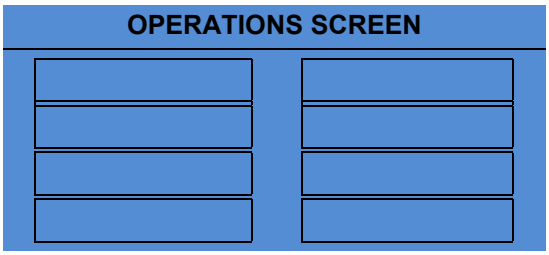


Figure 1.5.9 Command Panel Default Screen.

The command panel is configured from the ***ZIV e-NET tool***®, within the relay settings. The controls are distributed from 1 to 4, and there are two controls per number, A and B. The number indicates the row and the letter the corresponding column where the configured command will be placed on the relay screen.

Each command will have eight settings:

- **Command panel status signal**: signal linked to the command. When this signal is active, the corresponding square will be shown black whereas if the signal is deactivated, the square background will remain white.
- **Status Text Commands Panel**: Text that will appear inside the corresponding square.
- **Action Text Commands Panel**: texts that will appear in the bottom line of the screen when the command is selected. It is just a graphic presentation. The user can select the texts to be shown within a list available at the relay. Default texts are Activate / Deactivate.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Sig Block Commands Panel**: signal the user can link to the command to block it. It can be any digital protection signal or signal generated in the control logic. When this blocking signal is active, the relay will prevent the command from being selected.
- **Action Button O Commands Panel**: O button signal activation mode. It can be a pulse, or step to 1 level (Activate) or 0 level (Deactivate). Default setting is to Disabled, which indicates that pressing the button will not effect any change to the associated signal.
- **Signal Button O Commands Panel**: command panel signal that will activate when the command is selected and the O button is pressed.
- **Action Button I Commands Panel**: I button signal activation mode It can be a pulse, or step to 1 level (Activate) or 0 level (Deactivate). Default setting is to Disabled, which indicates that pressing the button will not effect any change to the associated signal
- **Signal Button I Commands Panel**: command panel signal that will activate when the command is selected and the **I** button is pressed.

Button signals could be protection signals so that their activation or deactivation would trigger directly the desired action (enable or disable protection elements, element blocking, editing settings tables, etc.), or command signals so that their activation and deactivation can be taken into account in the relay logic.

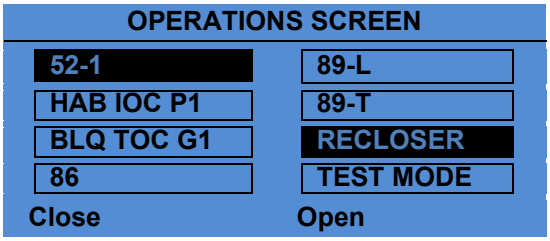


Figure 1.5.10 Example of configured command panel screen.

- **Autodimming**

Relays screen can be configured to keep the backlight permanently active or to switch the backlight off after a given time. The user can modify the ***Autodimming*** settings from the relay HMI by gaining access to the **Configuration** menu or else from the ***ZIV e-NET tool***®. By default, autodimming will be enabled for 2 minutes, so that the screen will turn off by itself 2 minutes after the last interaction with the relay or after booting. The *backlight* will never be permanently switched off through setting. The screen will always be lit up when the autodimming is disabled.

At the time a fault occurs, the relay backlight will automatically light up and will remain lit until the trip is reset.

The ***Display Time*** will also be used to return to the default screen.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.4.b Keypad associated to the Alphanumeric Display

The keypad has 11 keys, as follows.

CTRL / MENU: switches between graphic and alphanumerical screen. It has functionality just in models with graphical display.

▲	From the default screen, events and fault reports are displayed (only if they exist).
▶	From the default screen, measurements are visualized. Pressing again moves from one measurement screen to the next one.
▼	From the default screen you can see the status of the digital inputs and outputs.
◀	From the default screen it is accessed the screen where is displayed the information related to the last fault.

The keypad also provides an **Enter** key ↵ (in the center) **Escape** (**ESC**) and Clear (**CLR**):

Enter	Button used to Select or Accept.
ESC	Button whose purpose is to return to the previous screen. When being in the default screen, when pressed, the IED will show a screen with information regarding the configuration of the programmable buttons (P1 to P12). This screen will display the configured texts of each programmable button so that the user will now which function has been configured in each button.
CLR	Button to gain access to the memorized LED reset menu, last trip screen reset, event reset and fault reports reset. Both events and fault reports that can be reset are the ones showed in the HMI, all events and fault reports that can be downloaded by communications ports through ***ZIV e-NET tool***®) will be kept in the relay memory. Press the **CLR** button to switch between reset menus, and the relay will show them only if there are data subject to be erased. To proceed with the reset, from the corresponding menu, press **Enter** ↵ around two seconds until the prompt reset done is displayed on the screen. In case of resetting memorized LEDs, the relay will activate all LEDs and will reset the ones memorized without showing any message on the screen. If after the reset command and the activation of the 8 LEDs, any LED remains lit, it is because the signal associated to this LED is active.
ENT	When being in the protection default screen, when pressed, the IED will show during the time defined in ***Display Time*** a screen with information regarding the configuration of the programmable buttons (P1 to P12). This screen will display the configured texts of each programmable button so that the user will now which function has been configured in each button. In relays with alphanumeric display, the panel command screen can be accessed pressing again SEL button or pressing ENT button. For more information check the programmable buttons section.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.4.c Command Buttons

Pressing the **SEL** button once will open the command buttons screen, referring to the configuration of the programmable buttons, which can vary according to the IED model, P1 to P6 or P1 to P12. In models with alphanumeric display, pressing the button **ENT** or **SEL** again will open the Operation Screen, after user authentication.

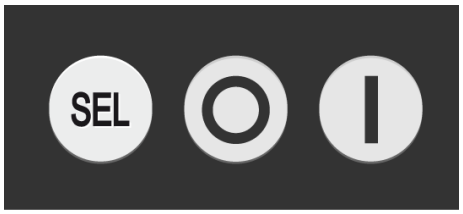


Figure 1.5.11 Command Buttons.

This **SEL** key is also used to scroll the command panel and to go to the required place. The controls configured in the protection settings are run through buttons (**I**) and (**O**).

In models with Graphic Display, the **SEL** key allows selecting, one by one, each single line diagram element until the no element selected situation is reached again. The selected element is represented graphically by a blinking symbol. Once the element has been selected, it is operated using the keys **O** – **I**. Being in the protection menu it will show the informative screen of the programmable buttons:

Open (O)	Open command after selecting the configured command on the Operation Screen or pressing buttons **P1** to **P6** or **P1** to **P12**, depending on the model. In graphic displays, the open command is issued through this key after selecting the configured component in the single-line diagram.
Close (I)	Close command after selecting the configured command on the Operation Screen or pressing buttons **P1** to **P6** or **P1** to **P12**, depending on the model. In graphic displays, the close command is issued through this key after selecting the configured component in the single-line diagram.

1.5.4.d Keys, Functions and Operation Modes

Below are the functions of the available keys, both the functions associated with the alphanumeric display and those of the keyboard.

- **Keypad**



Confirmation key
The confirmation key is used for confirming an action: after making a selection, or after editing a setting, or else to go on to visualize the totality of the registered data. After an operation is carried out (selection, change of settings, information, etc.), press ← again and return to the immediately previous level.



Escape key
The **ESC** key is used to exit the display if you do not wish to make any modification in the setting, or if you simply wish to exit the information display. In any case, when you press this key the system returns to the immediately previous level.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019



Reset key
Press the **CLR** key to gain access to the memorized LED reset menu, last trip screen reset, event reset and reset of fault reports shown in the HMI. To proceed with the reset, from the corresponding menu, press **Enter** around two seconds until the prompt reset done is displayed on the screen. In case of resetting memorized LEDs, the relay will activate all LEDs and will reset the memories without showing any message on the screen. If after the reset command and the activation of the 8 LEDs, any LED remains lit, it is because the signal associated to this LED is active.



Selection keys on the display
You can go forward or backward in correlative order, using the selection keys, to any of the options available in a menu or submenu. When more than eight options are available in a menu, an arrow (⇓) will be visualized on the right-hand side of the display, indicating the existence of the same. These options will be accessed with key ▼ and the options that appear in the first place will cease to be visualized.

Then, a bar with an arrow (⇑) will appear on the right-hand side of the display, which will indicate, at the same time, the existence of these first options.

The key ◄ is also used for erasing digits within a setting when modifications are being carried out on the same. It only has this function when the setting is being introduced.

- **Auxiliary Function Keys**



When this key is pressed from the default display, it gives access to the information provided by the registration of control changes (events) and fault reports.



The key ► is used for consulting the unit as regards the data pertaining to current, voltage, power, etc.

The function key ► is used for rejecting the changes undertaken on the settings (when the unit requests the confirmation of these changes) and to reject the activation of a table of reserve settings (also when this confirmation is requested).



By pressing ▼ you can visualize the status of digital inputs and outputs from the unit.

Once the status of digital inputs is on screen, click the function key ► to visualize the status of digital outputs.



By pressing ◄ you confirm the changes of settings undertaken (when the unit requests that changes need to be confirmed) or the activation of a table of settings is confirmed (when the unit requests that changes need to be confirmed).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Programmable Buttons**

The configurable buttons, **P1** to **P6** or **P1** to **P12** depending on the model, allow the operation of elements/units that can be selected by the user through the configuration program.

Models with Extended Buttons Display (model digit 5 = 3 or 4) feature a configurable **L/R** button, which can be used to change between Local/Remote hierarchical levels. This button has the same characteristics as the other user-configurable buttons (**P1**-**P12**), with the difference that the **L/R** Button has 2 associated LEDs (fixed color red). This button provides flexibility to implement the Local/Remote function.

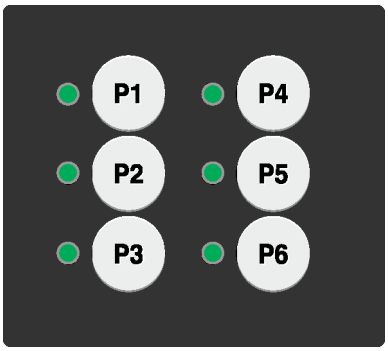


Figure 1.5.12 Programmable Command Buttons.

The programmable buttons are configured from the ***ZIV e-NET tool***®, within the relay settings. Each button will have ten (10) settings (6 for the button and 4 for the associated LED):

- **Text**: Text that will appear in the screen of the IED after pressing the button or ESC. Maximum of 15 characters are allowed.
- **Block Signal**: signal the user can link to the command to block it. It can be any digital protection signal or signal generated in the control logic. When this blocking signal is active, the relay will prevent the command from being selected.
- **Action Button O Command**: It indicates the operation mode over the associated signal when selecting the **O** button. It can be a pulse or a level signal (1/Activate or 0/Deactivate). The default setting is **Disabled**, which indicates that pressing the button will have no effect over the associated signal.
- **Signal Button O Command**: signal that will receive the operation mode (pulse, activation, deactivation) when the button is selected and the **O** button is pressed. It can be any signal of the relay (protection or control signal).
- **Action Button I Command**: It indicates the operation mode over the associated signal when selecting the **I** button. It can be a pulse or a level signal (1/Activate or 0/Deactivate). The default setting is **Disabled**, which indicates that pressing the button will have no effect over the associated signal.
- **Signal Button I Command**: signal that will receive the operation mode (pulse, activation, deactivation) when the button is selected and the **I** button is pressed. It can be any signal of the relay (protection or control signal).

Each programmable button has a double colored LED (red/green) associated. In order to configure them there are 4 settings available:

- **Red Activation:** Group of 16 settings where any digital signal of the relay can be configured (protection or control signal). The relay will activate the red LED colour of the corresponding button when any of the 16 signals activates.
- **Green Activation:** Group of 16 settings where any digital signal of the relay can be configured (protection or control signal). The relay will activate the green LED colour of the corresponding button when any of the 16 signals activates.
- **Blink:** when setting to yes, the LED will start flashing taking into account an internal pulse train when any of the colours in activated.
- **Memorized:** when setting to yes, the LED will remain in active status even after the deactivation of all the signals configured in the OR logics. The LED will deactivate after receiving a LED reset command.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

In order to know which is configured in each programmable button, pressing the **SEL** key when being in the protection default screen, it will be displayed during the time set in ***Display Time,*** a screen with the configured texts of each button.

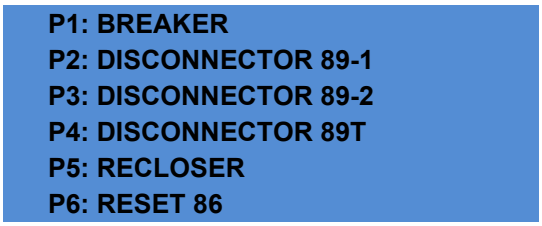


Figure 1.5.13 Example of programmable buttons screen.

When pressing any of the programmable buttons that screen will also appear. In this case, if the button can be selected (associated block signal deactivated or not configured) the text of the pressed push button will be shown blinking to indicate that it has been selected.

So, in models with graphical display, the information screen will appear just when being in the default screen of the “protection menu” (not in the graphical display), this is, after having pressed CTRL/MENU.

To show the information screen:

IEDs with **graphical display** (and being in the default screen of the protection menu):
- When pressing SEL button it will appear the screen in an informative way. This screen will be static and will be shown during the ***Display Time*** setting if the ESC button is not pressed earlier. - When pressing any of the buttons P1 to P6 or P1 to P12. In this case, and if the command is not blocked (corresponding block signal setting deactivated) the line which corresponds to the button which has been pressed will appear blinking and the corresponding LED will start also blinking in orange. When the command is executed (Button P1 to P6 + I/O button) the information screen will disappear. If the command is not executed, the screen will remain visible according to the ***Display Time*** setting. - If the information screen is being shown and any other P1 to P6 button or SEL button is pressed again, the counter will restart from zero (***Display Time***).
IEDs with **alphanumeric display** (and being in the default screen):
- When pressing SEL button it will appear the screen in an informative way. This screen will be static and will be shown during the ***Display Time***. After this time the IED will show the command panel screen. To avoid waiting that time to access the command panel screen the user can press again the SEL button or the ENT button and the IED will change the screen into the command panel one. In both screens (information and command panel) when pressing the ESC button, the IED will go to the default screen. - When pressing any of the buttons P1 to P6 or P1 to P12. In this case, and if the command is not blocked (corresponding block signal setting deactivated) the line which corresponds to the button which has been pressed will appear blinking and the corresponding LED will start also blinking in orange. When the command is executed (Button P1 to P6 + I/O button) the information screen will disappear. If the command is not executed, the screen will remain visible according to the Display Time setting. After directly pressing buttons P1 to P6 or P1 to P12 and showing the information screen it will never be access to the command panel screen, the IED will return after it to the default screen. The panel command screen can be accessed just after pressing SEL button. While one button is selected, pressing SEL button is not considered.

Both for models with graphic and alphanumeric display, buttons P1 to P6 or P1 to P12 will work normally even if the relay is not in the standard “protection menu/protection display”, but in this case the information screen will not appear.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

If the signal configured in the button block is in active status, the button cannot be selected so when it is pressed:

- The information screen will appear (if we are in the default menu/protection screen) with all the texts in a static way.
- The corresponding LED will not blink.
- If after pressing the button P1 to P6 or P1 to P12 any of the I/O button is pressed, the IED will not perform any action. It would be like pressing I/O button without having pressed before P1 to P6 or P1 to P12 buttons.

If the signal configured in the button block is in inactive status, the button can be selected so when it is pressed:

- The information screen will appear (if we are in the default menu/protection screen) and the line which corresponds to the button which has been pressed will appear blinking.
- The corresponding LED will start also blinking in orange.
- If after pressing the P1 to P6 button any of the I/O button is pressed, the IED will activate the associated signal based on the selected mode (activation level, deactivation level, pulse).

1.5.4.e Access to Options

To access options, you must scroll around the menus using the selection keys and afterwards confirm the option selected by pressing **ENT**.

- **Operation**

Range Settings

Range settings are displayed as follows: the operational value of the setting is displayed next to **ACT** (Actual). The new value is introduced in the next line, next to **NEW**, where the cursor will display an intermittent flash.

Auxiliary function keys are used for editing the new value which must correspond with the range specified in the last line of the display. If there is an error when a value is introduced, you must use key ◄ to erase the same. Once the new value has been edited, press key ↵ to confirm the same and exit to the previous menu.

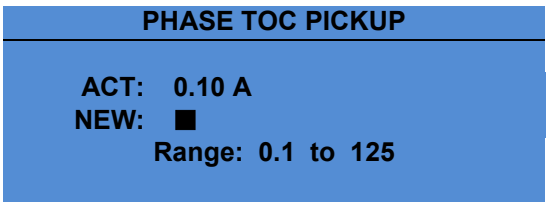


Figure 1.5.14 Range Settings.

YES / NO Type Settings

There is a type of setting whose range is limited to options **YES** and **NO**. Keys ▲ and ▼ correspond in this case to values **YES** and **NO**. After this, press key ↵ to confirm the setting and return to the previous screen. A similar case will be the numbered settings where the relay shows the various options. Scroll with the keys ▲ and ▼ to get the required option.

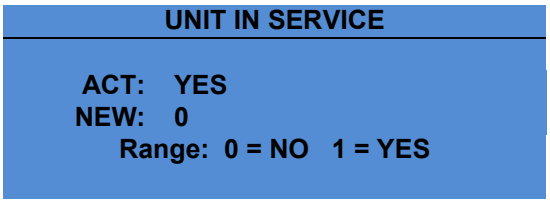


Figure 1.5.15 Numbered Settings.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings for the Selection of an Option

These settings present the layout of an options menu. Select the required option through the selection keys and confirmation using ↵. Thus, the system returns to the previous screen.

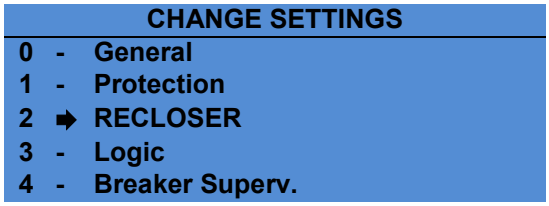


Figure 1.5.16 Selection Settings.

Masks Settings

As can be observed in the figure, the different options are presented in vertical order. Its current setting is: an empty square or a filled square which indicates enabled (■) or disabled (□) respectively.

The mask is modified (in the line indicated by brackets) using keys ◄ (1), enable, and ► (0), disabled.

In the event that there are more options than those that can represented in one screen alone, an arrow (↓) will appear at the end of the last line, which will indicate the existence of that second screen. This second screen appears as soon as the last option on the first screen has been set.

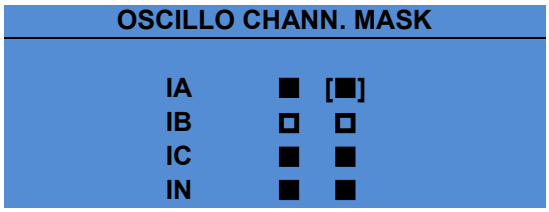


Figure 1.5.17 Mask Settings.

Exit Menus and Settings

In order to exit a menu or setting that you do not wish to modify, press **ESC** key. To exit a data display, you can either press the confirmation key ↵ or **ESC**. In all cases, you will return to the previous menu.

- **Last Trip Indication**

If any trip takes place, the terminal would present, on the default screen, the data related to it in a menu titled **TRIP**.

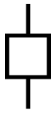
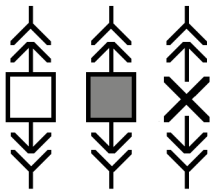
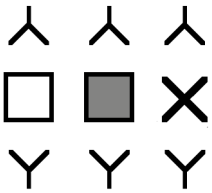
Additional screens will be created depending on the last types of units that trip. The format is always similar: a heading line that indicates the type of unit that has tripped (for example, Phase Undervoltage), and below this, all the elements and phases that have been involved (UV A1, UV B1,...). If various functions had tripped, and thus all of them do not fit into one screen, you can access all the functions involved through the selection keys.

The last trip screen will appear only if after a reset a trip has taken place.

This last trip screen will remain as default screen until it is removed through the reset menu accessed by the **CLR** key or until the device is switched off and booted again.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.5 Symbols associated to the Graphic Display

Element	State 1	State 2
Breaker	 Open	 Closed
Breaker	 Unknown (0-0)*	 Unknown (1-1)*
Switch	 Open	 Closed
Position of the Breaker mechanism	 Plugged	 Unplugged
Position of the Breaker mechanism	 Pulled out closed	 Pulled out open
Recloser	 In Service	 Out of Service
Capacitor Bank Control	 Automatic	 Manual
Voltage Regulator	 Automatic	 Manual

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.6 LEDs

Depending on the model, the IED may have 31 or 23 LEDs on the front, one with fixed function and the others configured.

- **Fixed function LED**

The LED on the upper right part of the relay with the greatest separation from the other LEDs is used to show the device status.

It is a tricolor LED that will indicate the following conditions:

- Relay in operation: steady green.
- Relay booting up: blinking green.
- Writing to flash memory: blinking orange.
- Relay in test mode: orange (future functionality).
- Relay in critical error (red).

- **Configurable LEDs**

The relay has 16 configurable monochrome LEDs. They can be configured to be activated in a fixed or blinking state and will always show the activation in red color.

These LEDs are configured through protection settings being able to assign up to 16 input signals to an OR gate so that when any of these 16 variables is activated, the corresponding LED is activated. Selected signals could be internal of the relay or user signals configured in the control logic configuration. Also, each LED will have two settings, ***Blinking*** and ***Memorizing*** so that they can be set separately for each LED in order that:

- ***Blink***: when the setting is set to **YES** and any of the OR logic signals is activated, the LED starts blinking, being activated and deactivated as a function of a pulse train of fixed duration.
- ***Memorized***: when the setting is set to **YES** and the signals assigned to the OR logic are deactivated after one activation, the LED remains lit or blinking until a LEDs reset command is received.The reset command may be carried out through the **CLR** key or through a digital input, command from the command panel or command through communications if so the relay has been configured by means of the control logic for that purpose.

The relay also has 6 to 12 bicolor LEDs (red/green), linked to 6 or 12 function buttons configured in the relay control logic through the ***ZIV e-NET tool***® configuration program. The number of buttons 1-6 or 1-12 is the defined according to the model.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.7 Inputs and Outputs

Inputs and outputs are grouped by SLOTs, being part of the power supply module or own digital input, output modules and transducer inputs.

The power supply module (**SLOT A** of the relay) will always be present while the rest of the modules (SLOTs) are optional and will depend on the selected model. This is why inputs and outputs are identified for each **SLOT** and not in a global way:

Both inputs and outputs will be configured through protection settings being able to assign up to 16 input signals to an OR gate for each input and output, so that when any of these 16 variables is activated, the corresponding physical input or physical output will be activated. Selected signals could be internal of the relay or user signals configured in the control logic configuration.

1.5.7.a Digital Inputs

The filtering and operation of the digital inputs is configurable according to the following options:

- ***Enable Digital Inputs***: When this setting is set to **NO** (inputs disabled), the inputs switch to disable or invalid status regardless the status of the signals assigned for activation in settings.
- ***Number of Changes to Disable*** (2-60): in order to prevent problems of a digital input under external or internal malfunction, a settable time window is established, in which the number of times the status of this digital input changes is monitored. If this number of changes exceeds a settable value, the digital input is disabled and the last status is frozen.
- ***Disable Window*** (1-30s): settable time window to disable a digital input for excessive number of changes.
- ***Number of Changes to Enable*** (2-60): once an input is disabled, it will be enabled again when complying with the enable conditions, this is, when the number of changes within the time window is less than the setting value, or through an enable command.
- ***Enable Window*** (1-30s): settable time window to enable a digital input that has previously been disabled for excessive number of changes.
- ***Digital Inputs Power Supply Supervision*** (NO / Digital Input / TRS1V_SB). Allows enabling Digital Input validity control as a function of a given digital input supply voltage (according to the ***Activation Level*** setting). When the setting is set to **Digital Input**, the relay will supervise the voltage value of this input and if it is below the activation value, the validity of all digital inputs will be disabled and deactivated, which will remain in their last state. When the voltage exceeds the supervision input threshold, all inputs will be enabled showing their present state and active validity. When the setting is set to **TRS1V_SB**, the relay will supervise the voltage value of this transducer and if it is below the Activation Level of digital inputs setting, the validity of all digital inputs will be disabled. When the voltage exceeds the ***Activation Level*** threshold, all inputs will be enabled showing their present state and active validity.
- ***Digital Inputs Voltage Supervisory Input*** (ED 1 to 6 of Slot B). Allows selecting the digital input that will be used as supply voltage reference. If the selected Digital Input is energized, the ***Digital Input Validity*** will remain active, otherwise, the ***Digital Input Validity*** will be deactivated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The relay includes 4 filters. Each filter is set through the settings below:

- ***Time between Samples*** (1-10 ms). To set up the sampling frequency of a digital input status.
- ***Number of Samples to Validate Changes*** (1-10): number of samples with the same value to validate an input. The number of samples to logic “0” or logic “1” consecutively to be detected in order to assume that the input is deactivated or activated respectively.

The filter for each input can be allocated through a setting:

- ***Filter Assignation*** (Filter 1 - Filter 2 – Filter 3 – Filter 4). Through this setting, “filter 1”, “filter 2”, “filter 3” or “filter 4” can be allocated to each configurable digital input. Filters 1, 2, 3, and 4 are made through the settings above allowing the creation of fast detection inputs or slow detection inputs.

A setting is also provided for each input to allow its automatic disabling:

- ***Automatic Disabling*** (YES / NO): There is a separate setting for each Digital Input. If set to YES, it allows the automatic disabling of the DI due to excessive number of changes.

The ***Activation Level*** of digital inputs can be allocated through a setting for each SLOT. Below is the input activation and deactivation value as a function of the according to the supply voltage used:

DI ON	Vdc ≥ Setting
DI ON/OFF	Setting - X < Vdc <Setting
DI OFF	≤ Setting - X

Where the hysteresis **X = 10 V** if the ***Activation Level*** setting is in the range of 15 V to 60 Vdc and where **X = 20 V** if the ***Activation Level*** setting is in the range of 60 V to 200 Vdc.

Vdc= Digital input supply voltage.
Setting= Activation threshold, range 15 - 200Vdc.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The IED's metering elements and logic functions use **Logic Input Signals** in their operation. They are listed in the tables along with the description of each of them and can be assigned to the **Physical Digital Inputs** or to logic output signals of opcodes configured in the programmable logic. It must be taken into account that several logic inputs can be assigned to one physical input, but the same logic input signal cannot be assigned to more than one physical input.

The tables mentioned above only list the inputs available with the default configuration. The list of inputs can be expanded with those that are configured in the programmable logic (any logic input signal created in the programmable logic can be used with the description that the user generates).

Each protection element module of the relay has a special **Logic Input** signal to put it “into service” or “out of service” from the HMI (buttons on the front), with a digital input by level and with the communications protocol configured in each port (control command).

It is normal to do it either from the control logic through control functions or through a digital input. This logic input signal is called **Enable Input…**. It combines with the **In Service** setting in this algorithm.

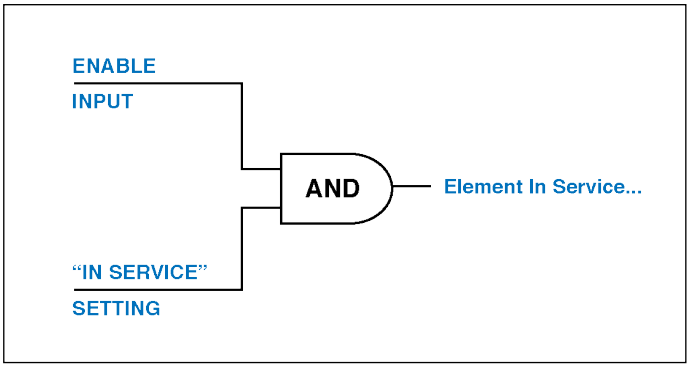


Figure 1.5.18 Element Enable Logic.

The default value of the logic input signal **Element Enable Input**... is a “1.” Therefore, when you do not configure the programmable logic at all, putting the protection elements into service depends only on the value of the **In Service** setting of each of them. The logic configuration to activate or switch off the enabling logic input signal will be as complicated or simple as you wish, from assigning it to a status contact input to building logical schemas with the various logic gates available (flip-flop’s) or allocate them to controls from the command panel or by communications.

Those protection functions that are put “out of service” by any of these methods will not generate or activate any of their associated logic signals, not even those that may be configured in the programmable logic and are directly related to these functions.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Digital input related settings may only be configured from the communications program:

Table 1.5-1: Digital Inputs of the Inputs Module

Name	Group	IEC 61850	Description	Vis.	Function
SLOTX_DI01DISORD	Unit Enablement Control	-	Slot X Command to Disable Digital Input 1		Inputs to the module of digital inputs that activate and deactivate each of the digital inputs
SLOTX_DI02DISORD		-	Slot X Command to Disable Digital Input 2		
SLOTX_DI03DISORD		-	Slot X Command to Disable Digital Input 3		
SLOTX_DI04DISORD		-	Slot X Command to Disable Digital Input 4		
SLOTX_DI05DISORD		-	Slot B Command to Disable Digital Input 5		
SLOTX_DI06DISORD		-	Slot X Command to Disable Digital Input 6		
SLOTX_DI07DISORD		-	Slot X Command to Disable Digital Input 7		
SLOTX_DI08DISORD		-	Slot X Command to Disable Digital Input 8		
SLOTX_DI09DISORD		-	Slot X Command to Disable Digital Input 9		
SLOTX_DI010DISORD		-	Slot X Command to Disable Digital Input 10		
SLOTX_DI011DISORD		-	Slot B Command to Disable Digital Input 11		
SLOTX_DI012DISORD		-	Slot X Command to Disable Digital Input 12		
SLOTX_DI013DISORD		-	Slot X Command to Disable Digital Input 13		
SLOTX_DI014DISORD		-	Slot X Command to Disable Digital Input 14		
SLOTX_DI015DISORD		-	Slot B Command to Disable Digital Input 15		
SLOTX_DI016DISORD		-	Slot X Command to Disable Digital Input 16		
SLOTX_DI01ENAORD		-	Slot X Command to Enable Digital Input 1		
SLOTX_DI02ENAORD		-	Slot X Command to Enable Digital Input 2		
SLOTX_DI03ENAORD		-	Slot X Command to Enable Digital Input 3		

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.5-1: Digital Inputs of the Inputs Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
SLOTX_DI04ENAORD	Unit Enablement Control	-	Slot X Command to Enable Digital Input 4		Inputs to the module of digital inputs that activate and deactivate each of the digital inputs.
SLOTX_DI05ENAORD		-	Slot X Command to Enable Digital Input 5		
SLOTX_DI06ENAORD		-	Slot X Command to Enable Digital Input 6		
SLOTX_DI07ENAORD		-	Slot X Command to Enable Digital Input 7		
SLOTX_DI08ENAORD		-	Slot X Command to Enable Digital Input 8		
SLOTX_DI09ENAORD		-	Slot X Command to Enable Digital Input 9		
SLOTX_DI10ENAORD		-	Slot X Command to Enable Digital Input 10		
SLOTX_DI11ENAORD		-	Slot X Command to Enable Digital Input 11		
SLOTX_DI12ENAORD		-	Slot X Command to Enable Digital Input 12		
SLOTX_DI13ENAORD		-	Slot X Command to Enable Digital Input 13		
SLOTX_DI14ENAORD		-	Slot X Command to Enable Digital Input 14		
SLOTX_DI15ENAORD		-	Slot X Command to Enable Digital Input 15		
SLOTX_DI16ENAORD		-	Slot X Command to Enable Digital Input 16		

Table 1.5-2: Digital Outputs of the Inputs Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
SLOTX_DI01VALUE	Physical Digital Inputs	INSXGGIO1.Ind1	Slot X Digital Input 1		They indicate that the corresponding input has been activated.
SLOTX_DI02VALUE		INSXGGIO1.Ind2	Slot X Digital Input 2		
SLOTX_DI03VALUE		INSXGGIO1.Ind3	Slot X Digital Input 3		
SLOTX_DI04VALUE		INSXGGIO1.Ind4	Slot X Digital Input 4		
SLOTX_DI05VALUE		INSXGGIO1.Ind5	Slot X Digital Input 5		
SLOTX_DI06VALUE		INSXGGIO1.Ind6	Slot X Digital Input 6		
SLOTX_DI07VALUE		INSXGGIO1.Ind7	Slot X Digital Input 7		
SLOTX_DI08VALUE		INSXGGIO1.Ind8	Slot X Digital Input 8		
SLOTX_DI09VALUE		INSXGGIO1.Ind9	Slot X Digital Input 9		
SLOTX_DI10VALUE		INSXGGIO1.Ind10	Slot X Digital Input 10		
SLOTX_DI11VALUE		INSXGGIO1.Ind11	Slot X Digital Input 11		
SLOTX_DI12VALUE		INSXGGIO1.Ind12	Slot X Digital Input 12		
SLOTX_DI13VALUE		INSXGGIO1.Ind13	Slot X Digital Input 13		
SLOTX_DI14VALUE		INSXGGIO1.Ind14	Slot X Digital Input 14		
SLOTX_DI15VALUE		INSXGGIO1.Ind15	Slot X Digital Input 15		
SLOTX_DI16VALUE		INSXGGIO1.Ind16	Slot X Digital Input 16		

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.5-2: Digital Outputs of the Inputs Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
SLOTX_DI01VALIDITY	Validity of Digital Inputs		Slot X Validity of Digital Input 1		They indicate the valid status of the digital input.
SLOTX_DI02VALIDITY			Slot X Validity of Digital Input 2		
SLOTX_DI03VALIDITY			Slot X Validity of Digital Input 3		
SLOTX_DI04VALIDITY			Slot X Validity of Digital Input 4		
SLOTX_DI05VALIDITY			Slot X Validity of Digital Input 5		
SLOTX_DI06VALIDITY			Slot X Validity of Digital Input 6		
SLOTX_DI07VALIDITY			Slot X Validity of Digital Input 7		
SLOTX_DI08VALIDITY			Slot X Validity of Digital Input 8		
SLOTX_DI09VALIDITY			Slot X Validity of Digital Input 9		
SLOTX_DI10VALIDITY			Slot X Validity of Digital Input 10		
SLOTX_DI11VALIDITY			Slot X Validity of Digital Input 11		
SLOTX_DI12VALIDITY			Slot X Validity of Digital Input 12		
SLOTX_DI13VALIDITY			Slot X Validity of Digital Input 13		
SLOTX_DI14VALIDITY			Slot X Validity of Digital Input 14		
SLOTX_DI15VALIDITY			Slot X Validity of Digital Input 15		
SLOTX_DI16VALIDITY			Slot X Validity of Digital Input 16		
FALLOTALIMENTACIONENTRADASDIGITALES	Alarm and Error Signals		Digital Inputs Power Failure		Indication of voltage reference loss in Dis.
ENTRADASDIGITALESHABILITADAS	Others		Digital Inputs Enabled		Indication of DIs enabled by setting.

Slot X. There may be X A or B connectors depending on model.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.7.b Auxiliary Outputs

The number of digital outputs available will depend on each particular model. They can all be configured with any input or output signal of the pre-existing protection and control modules or defined by the user in the programmable logic.

Auxiliary outputs may use normally open, normally closed relays or quick solid state outputs. For details on the arrangement of contacts for each model, see the External Connections Scheme.

In operation, metering elements and logic elements generate several logic outputs. These signals or any other signal registered in the relay can be used to configure the activation of each digital output through the OR gate available in the protection settings. For more complex logic and to be able to allocate the resultant outputs to physical auxiliary outputs, the necessary opcodes must be programmed in the programmable logic to generate a user signal to be used in the setting of the corresponding output.

There is an additional, non-programmable auxiliary output contact (**SLOT A**) that corresponds to the relay **In Service**.

Table 1.5-3: Auxiliary Outputs of the Outputs Module

Name	Group	IEC 61850	Description	Vis.	Function
SLOTX_DO01	Physical Digital Outputs	OUTSXGGIO1.Ind1	Slot B Digital Output 1		They indicate that the corresponding input has been activated.
SLOTX_DO02		OUTSXGGIO1.Ind2	Slot B Digital Output 2		
SLOTX_DO03		OUTSXGGIO1.Ind3	Slot B Digital Output 3		
SLOTX_DO04		OUTSXGGIO1.Ind4	Slot A Digital Output 4		
SLOTX_DO05		OUTSXGGIO1.Ind5	Slot A Digital Output 5		
SLOTX_DO06		OUTSXGGIO1.Ind6	Slot A Digital Output 6		
SLOTX_DO07		OUTSXGGIO1.Ind7	Slot A Digital Output 7		

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.7.c Digital Inputs, Auxiliary Outputs and LEDs Test

Apply rated voltage, appropriate for the model. At this time, the **In Service** LED should be lit.

- **Digital Inputs**

For the inputs test, exceed the rated voltage adjusted in ***Activation Level*** by SLOT between the terminals corresponding to the inputs (marked in the external connections diagram), always taking the polarity of the contacts into account and activation levels indicated in paragraph 1.5.6.a.

From the inputs screen of the menu check that the inputs are activated. Remove the voltage and check that the inputs are deactivated. The check may also be carried out through the relay events or communications program status section.

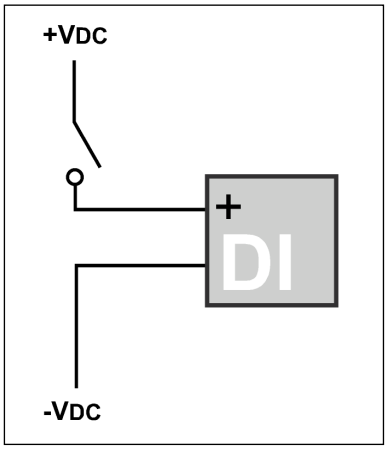


Figure 1.5.19 Digital Inputs Test.

- **Auxiliary Outputs**

To test the auxiliary contact outputs, their operation is provoked according to how they are configured. If they are not configured, they can be configured as activation of the status contact inputs or any other signal available on the equipment.

- **Selection and Command Buttons and Associated LEDs**

To test the configurable selection and command buttons on the front of the IED, they are assigned a configuration such that, once they have been selected and the command given, the corresponding auxiliary contact outputs are activated and deactivated.

Pressing the **P1** to **P6** keys after the configuration indicated above has been made, causes the LEDs corresponding to each of them to blink. Then, pressing the **I** key (which indicates closure) or the **O** key (which indicates opening), enables the contacts corresponding to the auxiliary contact outputs.

- **LED Targets**

In order to check the LED indicators, press the **CLR** key on the default screen until the LED reset screen appears. Keep **ENT** pressed until all LEDs light up and go off.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.8 Communications

1.5.8.a Communications Ports

The IEDs are provided with different types of communications ports depending on the selected model:

- **1 Front Local Port** USB-A host type for loading and downloading IEC 61850 files.
- **1 Front Local Port** USB-B type. Uses only PROCOME protocol for connection with the configuration tool.
- **2 Remote Ports** with the following characteristics:
  - Remote Port 1 (SP1): GFO (ST connector) interface or RS232 Full Modem electric interface.
  - Remote Ports 2 (SP2): GFO (ST connector) interface or RS232 / RS485 electric interface.
- **Up to 4 LAN Ports**. Two redundant interfaces with the following possible configurations (ETHERNET type communications).
  - Interface 1: LAN 1 and LAN 2:

	LAN1	**LAN2**
1st combination	RJ45	RJ45
2nd combination	GFO LC	GFO LC
3rd combination	GFO ST	GFO ST

  - Interface 2: LAN 3 and LAN 4

	LAN3	**LAN4**
1st combination	Not available	Not available
2nd combination	RJ45	RJ45
3rd combination	GFO LC	GFO LC
4th combination	GFO ST	GFO ST

The relays include one controller per communications gate, so that communications can be established through all of them at the same time. On the other hand, Ethernet ports support up to 5 instances of protocols (PROCOME, DNP3 V3.0, MODBUS) simultaneously apart from MMS and GOOSE messages (IEC 61850) if an IEC 61850 relay is selected.

Technical data for these communications links can be found in Technical Data section. Information on model ports can be found in 1.2, Model Selection section.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.8.b LEDs associated to the Communications Ports

Hereafter, it appears the colour code used in the LEDs which are associated to the communications ports that are located in the rear part of the IED:

Electrical Ethernet		**Optical Ethernet**	
Colour		**Colour**	
10 Mb	Yellow	Any speed	Green
100 Mb	Green	**Mode**	
1Gb	Red	Without activity or link	Switched of
Mode		Link	Switched on
Without activity or link	Switched off	Activity	Flash
Link	Switched on		
Activity	Flash		

1.5.8.c Communication with the Configuration Tool

Communication to set and download protection data (events, fault reports, disturbance recorder files, etc.) can be achieved through any communication ports set to PROCOME protocol. The local port is always assigned to this protocol, whereas remote ports must be assigned to protocol PROCOME for this purpose.

Communications are established through ***ZIV e-NET Tool***® program, which allows communicating whether locally (via a PC connected to front port) or remotely (via rear serial ports with PROCOME protocol), covering all needs regarding programming, settings, recording, reports, etc...

The configuration of the local communications gate may only be edited from the HMI, however, remote communications gate settings may also be edited through the communications program ***ZIV e-NET Tool***®, but only communicating with the relay through the local port.

The ***ZIV e-NET Tool***® program is protected against non-authorized users through access passwords. The ***ZIV e-NET Tool***®, which runs in WINDOWS™ environment, is easy to operate and uses buttons or keys to display the different submenus.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.8.d Communication Protocols

The following protocols are provided depending on the communications port:

- Front Local Port **USB-A** type (host). For loading and downloading IEC 61850 files using a pendrive.
- Front Local Port **USB-B** type. Uses only PROCOME protocol.
- Remote Ports **SP1** and **SP2**. Each port may be configured to be able to communicate through one protocol PROCOME, DNP V3.0 or MODBUS.
- **LAN** Ports. Two redundant interfaces. May communicate in MMS/GOOSE (IEC 61850) and simultaneously with one PROCOME instance with fixed port tcp 32001 and four configurable instances with configurable port TCP and configurable protocol (PROCOME, DNP3 V3.0 and MODBUS).

It is worth mentioning that communications through all ports can be maintained simultaneously.

PROCOME protocol complies with IEC-870-5 standards and is used, like IEC61850, for both protection and control information management. On the other hand, protocols DNP V3.0 and MODBUS can be used only for control information management.

For more details on protocols refer to the applicable protocol ANNEX.

1.5.8.e Control Change Recording

According to the signals that have been configured in the programmable logic through the ***ZIV e-NET Tool***®, the different events that occur in the system will generate the annotation of those signals that has changed their state.

Different signal lists for PROCOME 3.0, DNP V3.0 and MODBUS protocols can be configured through the programmable logic, saving the changes into different and separate relay files for each of the communications ports. This means that although the changes queue of one port is emptied after collecting said information, the same information is available at the other port for collection through the allocated protocol, whether it is the same as for the first port or not.

In the same way, from the signals configured in PROCOME, DNP 3.0 or both, user can select the ones to be displayed through the HMI. They are also saved into separate files, so that even if control changes queues of communications ports are emptied, the information is still available through HMI.

Control change register data is displayed from the relay HMI, through the menu **Data/Registers/Events** or by pressing the **Up arrow** (which shows the options to **Display Events** or **Fault Reports)**. When entering into the display events option, the last generated event is always displayed (the most recent). Data is displayed as follows:

YY/MM/DD|HH:MM:SS
ms text1 □ or ■
ms text2 □ or ■

YY/MM/DD|HH:MM:SS
ms text3 □ or ■
ms text4 □ or ■

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

This is, events are grouped by “date” and “time”. Then, in the following line, the milliseconds corresponding to each control change and the label defined through the ***ZIV e-NET Tool***® (maximum of 13 characters) are shown. And at the end of the line, a filled or blank square indicates ACTIVATION-ON (■) or DEACTIVATION-OFF (□) respectively.

Default signal text labels are defined in input and output tables; in case of new signals generated into the programmable logic, said text must be defined. In any case, in order to use the names required by each user, the creation of a logic record card allocating a personalized name to every signal to be displayed is recommended.

The date and time stamp will be generated every time a new event occurs in it.

The MODBUS allows to display the actual value of the configured digital signals but do not record their changes.

1.5.8.f Ethernet Redundancy

The equipment can have one or two redundant interfaces. Each redundant interface consists of two LAN ports. Depending on a setting, the operating mode can be defined: no redundancy, Bonding (Hot Stand By), RSTP, PRP or HSR.

- **No Redundancy**

The relay is provided with 2 separate network adapters with different MAC address and different IP address.

Both adapters are independent, it is possible to access the MMS data through both of them.

GOOSE messages will be sent and received only through one adapter, the one defined in the ***GOOSE Channel*** setting.

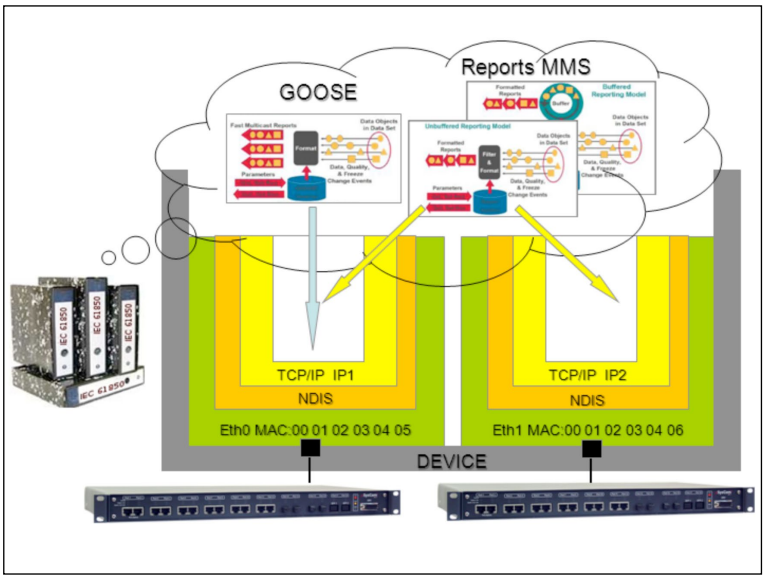


Figure 1.5.20 Configuration of Communications Ports for Relays without Ethernet Redundancy.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Bonding Type Redundancy (Hot Stand By)**

The relay is provided with 2 network adapters both operating with the same MAC address and the same IP address, only one of them being active as a function of the medium detection (a broken connection to the adapter results in switching to the other adapter that has a good connection). Both MMS data and GOOSE messages will be sent and received only by the active adapter.

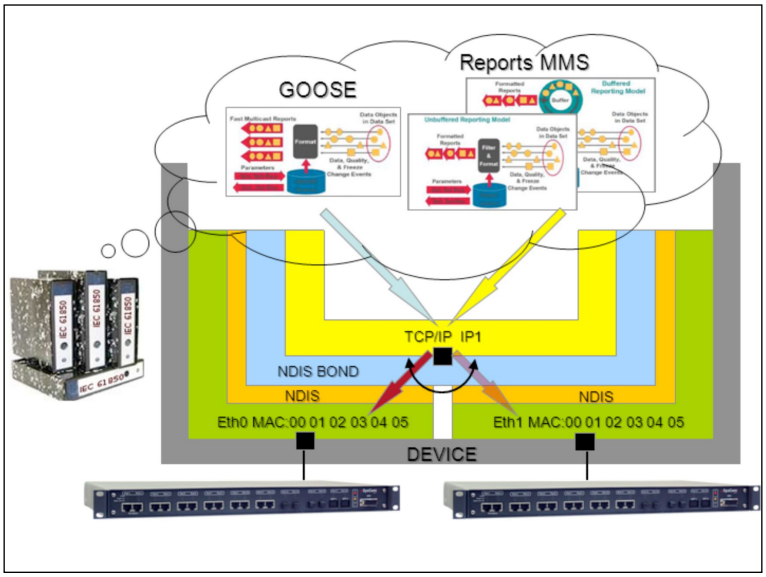


Figure 1.5.21 Configuration of Communications Ports for Relays with Bonding Type Redundancy (Hot Stand By).

- **RSTP Type Redundancy**

The relay includes 2 network adapters, both operating with the same MAC address and the same IP address, and both adapters are active always. Relays define, together, the optimal path to send messages opening the ring to prevent loop formation. Also, they reconfigure the path when some type of relay or link failure occurs.

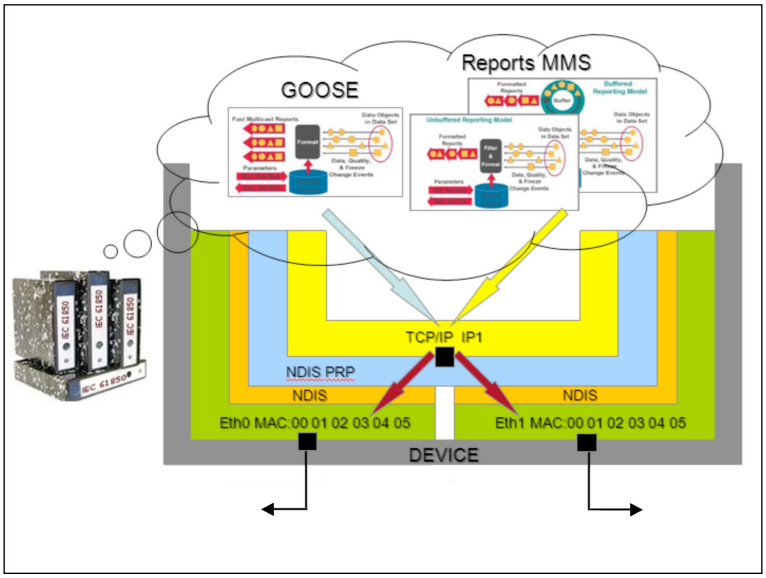


Figure 1.5.22 Configuration of Communications Ports for Relays with RSTP Type Redundancy.

RSTP type redundancy is based on connecting relays with each other with single ring, star or star-ring instead of using switches. The relays themselves are in charge of defining and opening the ring, as well as deleting messages from the same preventing their indefinite recirculation. All the equipments must support RSTP type Redundancy.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

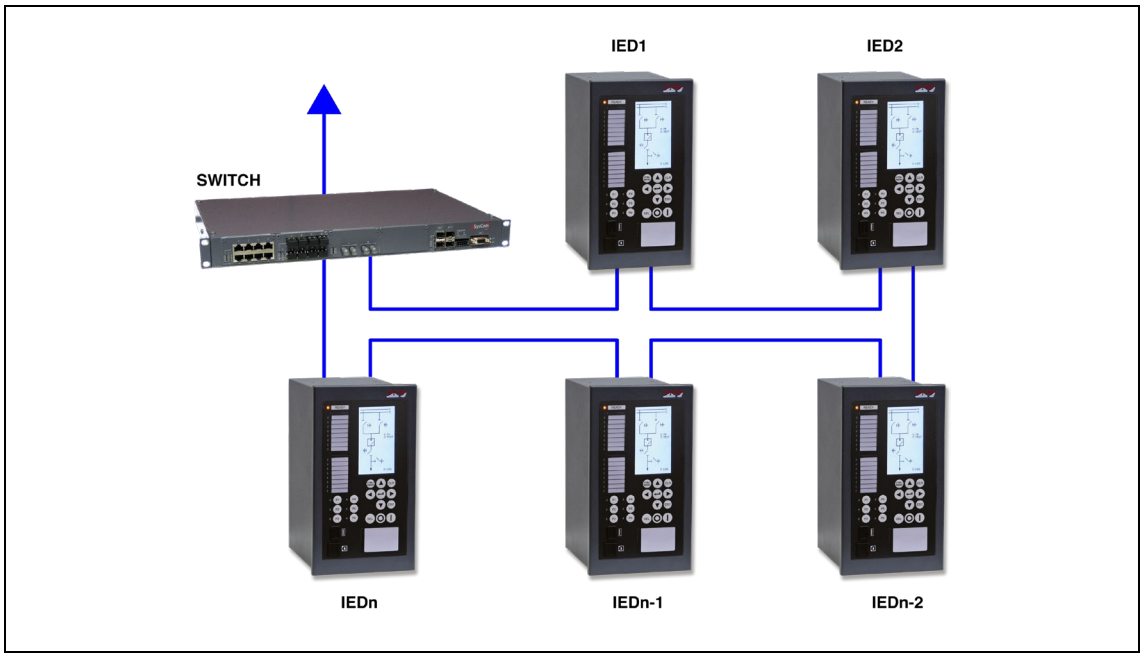


Figure 1.5.23 Example of Connecting Relays with RSTP Redundancy with Simple Ring.

- **PRP Type Redundancy**

The relay is provided with 2 network adapters both operating with the same MAC address and the same IP address.

Both adapters are in active status all the time, sending the same data through both of them according to the IEC 62439-3 Parallel Redundancy Protocol (PRP).

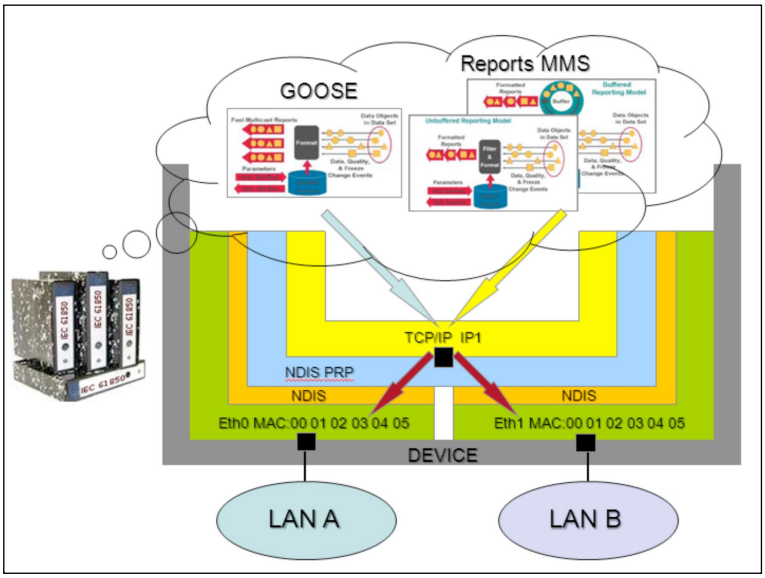


Figure 1.5.24 Configuration of Communications Ports for the Relay with PRP Type Redundancy.

This protocol is based on connecting the relays to two different Ethernet networks (LAN), not connected between them (independent LAN networks). The same data is sent through both adapters at the same time, adding 6 bytes to each Ethernet frame for the PRP protocol. These bytes enable discarding duplicate data, as the same data is received through both adapters and the idea is discarding the duplicate packet at the lowest possible level within the communications stack. Both MMS data and GOOSE messages will be sent through both adapters at the same time. In a PRP Redundancy system, both relays supporting PRP and relays not supporting RPR can operate, the latter being only connected to a single network.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

LanID is fixed: 0x0A for LAN1 and LAN3 and 0x0B for LAN2 and LAN4.

- **HSR Type Redundancy**

The relay has 2 network adapters, both operating with the same MAC address and the same IP address, both adapters being active at all times and managing the traffic according to IEC 62439-3- High-availability Seamless Redundancy (HSR) protocol.

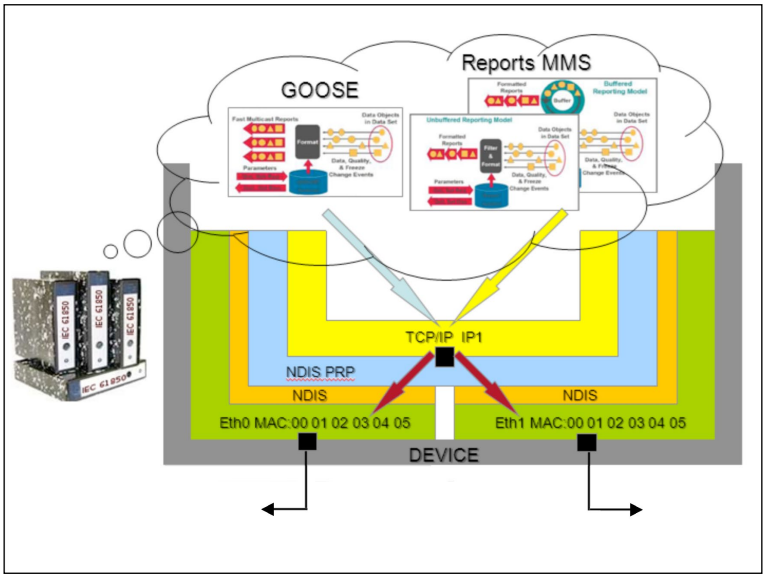


Figure 1.5.25 Configuration of Communications Ports for the Relay with HSR Type Redundancy.

The HSR Redundancy is based on connecting the relays with each other in a ring structure. All relays connected to an HSR network must support HSR and the devices themselves carry out Ethernet frame management, operating as a bridge and resending traffic in case a relay is neither source nor target, receiving and deleting frames if they are target, discarding frames in case of emitter if they are returned through the same adapter as that used for sending or different adapter, sending supervision frames, etc.

LanID is fixed: 0x0A for LAN1 and LAN3 and 0x0B for LAN2 and LAN4.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Examples of Common Redundancies**

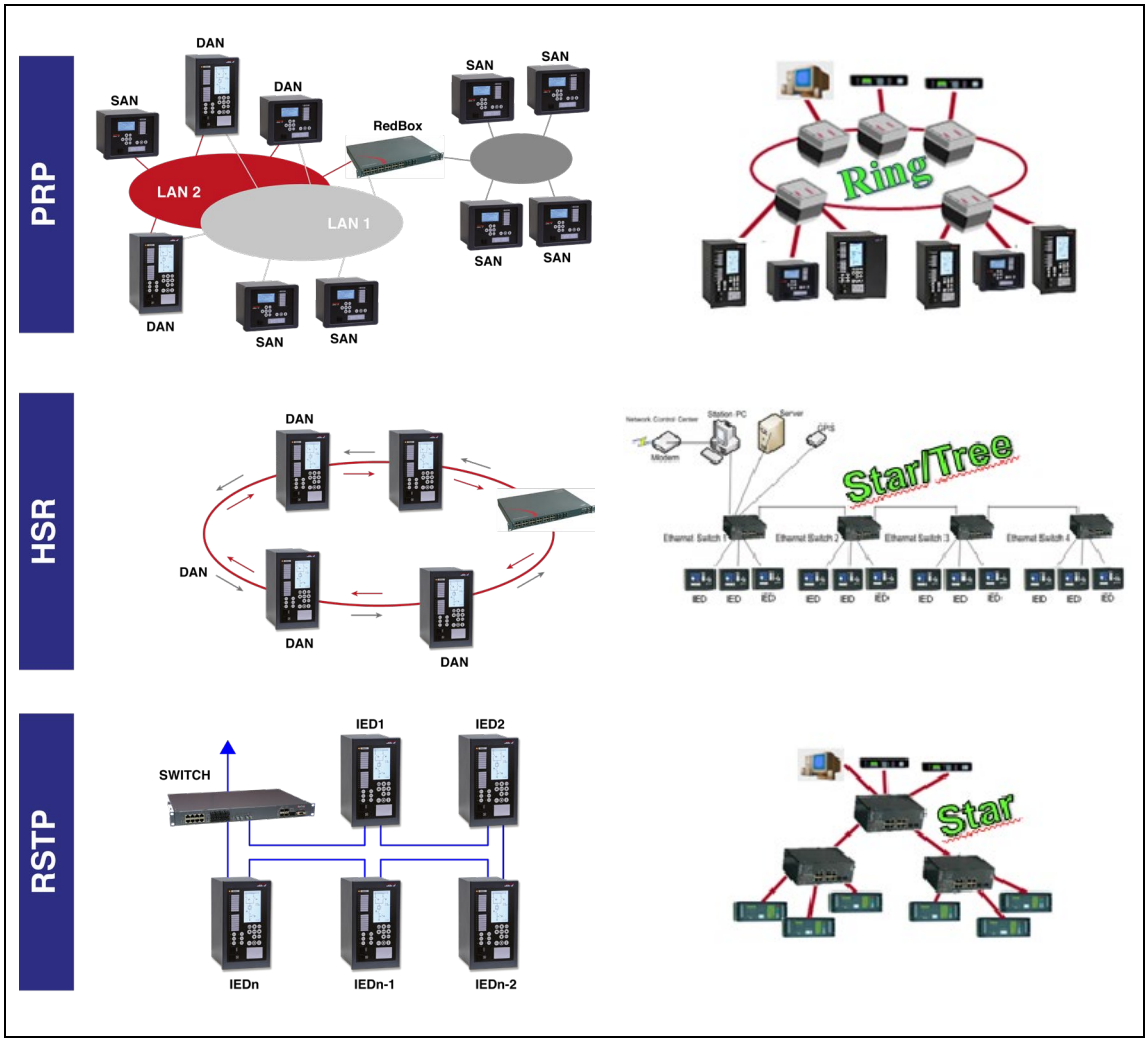


Figure 1.5.26 Examples of Common Redundancies.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.8.g Communications Settings

The settings described below are totally independent for each port and they are grouped as follows: ***Serial Port Settings (Local***, ***Remote Port 1*** **[SP1] or Remote Port 2 [SP2])**, ***LAN 1-2 Ports*** **(LAN1 or LAN2)**, ***LAN 3-4 Ports*** **(LAN3 or LAN4)**. Finally, specific settings for each protocol are described.

Every time a communications session is started through one of these ports, the relay communications port is displayed on the upper left corner of the relay alphanumeric screen (HMI). From left to right, local port, remote ports SP1 and SP2, fixed PROCOME instance to TCP 32001 port and configurable instances 1, 2, 3 and 4. On models with graphic display, this information is available in the protection menu.

That indication, in case of PROCOME 3.0 protocol, remains displayed during ***Communications Password TimeOut*** setting for the PROCOME Protocol after the last communication carried out; in case of MODBUS and DNP V3.0 protocols, the message remains displayed for one minute after the last communication.

There are different time settings for each physical communications ports (***Communications Fail Timer***), which, regardless of the protocol allocated, allow to configure the period of time with no communications activity after which the corresponding alarms (digital signals and events) of **Communications Fail Remote Port, Protocol 1, Protocol 2, Protocol 3, Protocol 4** and **Protocol PROCOME** are generated.

As stated above, the relay may include one or two redundant interfaces to make a total of 2 or 4 LAN ports. Settings are segregated by redundant interface, LAN1-2 and LAN3-4. Each interface includes the settings corresponding to each LAN port (LAN1, LAN2, LAN3 and LAN4), which will be used separately if the relay is set without redundancy, and the settings corresponding to the available interface redundancies (Bonding or Hot Stand By, RSTP, PRP and HSR).

When an interface is set with redundancy, its ports will work in pairs, LAN1 with LAN2 and LAN3 with LAN4. Each interface may be set with different type of redundancy. Regardless the selected type of redundancy, both adapters will work with the same MAC and IP address. The IP address used will be set in the LAN1 adapter for the LAN1-2 redundant interface or LAN3 in case of the LAN3-4 redundant interface.

The USB-B port allows the communication between 300 bits/s and 256000 bits/s automatically (it is not necessary to modify any setting on the port).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Configuration / Communications / Ports / Local Port (HMI)					
Setting	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Communication Failure Indication Time	Comms Fail Time		0-600 s	0.1 s	60 s
Authenticated Protocol	Authenticated Prot		YES / NO		YES

Settings / Communications / Ports / Serial Ports / Remote Port 1					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Protocol Select	Protocol Select.		Procome 3.0 DNP3.0 MODBUS		Procome
Baudrate	Baudrate		2400-115200 Bauds		38400
Stop Bits	Stop Bits		1-2	1	1
Parity	Parity		None Odd Even		None
RX Time between characters	Rx Time btw. Char		1-60000 ms	0.5 ms	10 ms
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Authenticated Prot.	Authenticated Prot		YES / NO		YES
Advanced Settings	Advanced Settings				
Flow Control	Flow Control				
CTS Flow	CTS Flow		NO / YES		NO
DSR Flow	DSR Flow		NO / YES		NO
DSR Sensitive	DSR Sensitive		NO / YES		NO
DTR Control	DTR Control		Inactive Active Enable Send		Inactive
RTS Control	RTS Control		Inactive Active Enable Send Solicit Send		
Times	Time				
Tx Time Factor	Tx Time Factor		0-100	0.5	1
Tx Timeout Const.	Tx Timeout Const.		0-60000 ms	1 ms	0 ms
Message Modification	Message Modif.				
Number of Zeros	Number of Zeros		0-200	1	0
Collisions	Collisions				
Collision Type	Collision Type		No Echo DCD		No
Max Retries	Max Retries		0-3	1	0
Min Retry Time	Min Retry Time		0-60000 ms	1 ms	0 ms
Max Retry Time	Max Retry Time		0-60000 ms	1 ms	0 ms
Max Echo Delay	Max Eco Delay		0-60000 ms	0.5 ms	10 ms

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / Ports / Serial Ports / Remote Port 2					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Protocol Select.	Protocol Select.		Procome 3.0 DNP3.0 MODBUS		Procome
Baudrate	Baudrate		2400-115200 Bauds		38400
Stop Bits	Stop Bits		1-2	1	1
Parity	Parity		None Odd Even		None
RX Time between characters	Rx Time btw. Char		1-60000 ms	0.5 ms	10 ms
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Authenticated Prot.	Authenticated Prot		YES / NO		YES
Advanced Settings	Advanced Settings				
Operating Mode	Operating Mode		RS-232 RS-485		RS-232
Times	Time				
Stop Bytes Number RS-485	Stop Bytes 485		0-4	1	0
Message Modification	Message Modif.				
Number of Zeros	Number of Zeros		0-200	1	0
Collisions	Collisions				
Collision Type	Collision Type		No Echo		No
Max Retries	Max Retries		0-3	1	0
Min Retry Time	Min Retry Time		0-60000 ms	1 ms	0 ms
Max Retry Time	Max Retry Time		0-60000 ms	1 ms	0 ms
Max Echo Delay	Max Eco Delay		0-60000 ms	0.5 ms	10 ms

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / LAN Ports / Ports 1-2					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Redundancy Mode	Redundancy Mode	LCCH1.RedTyp	None Bonding PRP HSR RSTP		None
Channel Live Time	Channel Live Time	LCCH1.ChLivTms1	1-60 s	1 s	5 s
Link Live Time	Link Live Time	LCCH1.LnkLivTmms1	0-60 s	0.1 s	0 s
Bonding	Bonding				
Link Check Interval	Link Chk Interval	LCCH1.BndChkTmms	25-1000 ms	1 ms	100 ms
PRP					
Interval for Sending Supervision Frames	Superv TX Interval		0-30 s	0.5 s	2 s
LSB of Destination MAC for Supervision Frames	Sup LSB Dest MAC		0-255	1	0
HSR	HSR				
HSR Transmission	HSR transmission	LCCH1.HSRTxTyp	Store-Forward Cut-Through		Store-Forward
Interval for Sending Supervision Frames	Superv TX Interval		0-30 s	0.5 s	2 s
LSB of Destination MAC for Supervision Frames	Sup LSB Dest MAC		0-255	1	0
RSTP	RSTP				
Brige Priority	Brige Priority	LCCH1.STPPrio	0-61440	4096	32768
Hello Time	Hello Time	LCCH1.STPHello	1-10 s	1 s	2 s
Max Age	Max Age	LCCH1.STPMaxAge	6-40 s	1 s	20 s
Forward Delay	Forward Delay	LCCH1.STPFwdDl	4-30 s	1 s	15 s
Port 1	Port 1				
Priority	Priority	LCCH1.STPPrio1	0-240	16	128
Cost	Cost	LCCH1.STPCost1	0-200000000	1	200000
Edge	Edge	LCCH1.STPEdge1	On / Off		Off
Port 2	Port 2				
Priority	Priority	LCCH1.STPPrio2	0-240	16	128
Cost	Cost	LCCH1.STPCost2	0-200000000	1	200000
Edge	Edge	LCCH1.STPEdge2	On / Off		Off

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / LAN Ports / Ports 1-2					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
LAN 1	LAN 1				
DHCP Enable	Enable DHCP		NO / YES		NO
IP Address	IP Address		ddd.ddd.ddd.ddd		192.168.1.81
Network Mask	Network Mask		ddd.ddd.ddd.ddd		255.255.255.0
Routing Tables	Routing tables				
Default Gateway	Default gateway				
Default route 1 IP address	IP default GW 1		ddd.ddd.ddd.ddd		0.0.0.0
Default route 1 metric	Metric def GW 1		0-65535	1	1
Default route 2 IP address	IP default GW 2		ddd.ddd.ddd.ddd		0.0.0.0
Default route 2 metric	Metric def GW 2		0-65535	1	1
Static routes	Static routes				
Destination address of route 1	Dest addr route 1		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 1	Netmask route 1		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 1	GW IP route 1		ddd.ddd.ddd.ddd		0.0.0.0
Destination address of route 2	Dest addr route 2		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 2	Netmask route 2		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 2	GW IP route 2		ddd.ddd.ddd.ddd		0.0.0.0
LAN 2	LAN 2				
DHCP Enable	Enable DHCP		NO / YES		NO
IP Address	IP Address		ddd.ddd.ddd.ddd		192.168.1.81
Network Mask	Network Mask		ddd.ddd.ddd.ddd		255.255.255.0
Routing Tables	Routing tables				
Default Gateway	Default gateway				
Default route 1 IP address	IP default GW 1		ddd.ddd.ddd.ddd		0.0.0.0
Default route 1 metric	Metric def GW 1		0-65535	1	1
Default route 2 IP address	IP default GW 2		ddd.ddd.ddd.ddd		0.0.0.0
Default route 2 metric	Metric def GW 2		0-65535	1	1
Static routes	Static routes				
Destination address of route 1	Dest addr route 1		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 1	Netmask route 1		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 1	GW IP route 1		ddd.ddd.ddd.ddd		0.0.0.0
Destination address of route 2	Dest addr route 2		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 2	Netmask route 2		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 2	GW IP route 2		ddd.ddd.ddd.ddd		0.0.0.0

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / LAN Ports / Ports 3-4					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Redundancy Mode	Redundancy Mode	LCCH1.RedTyp	None Bonding PRP HSR RSTP		None
Channel Live Time	Channel Live Time	LCCH1.ChLivTms1	1-60 s	1 s	5 s
Link Live Time	Link Live Time	LCCH1.LnkLivTmms1	0-60 s	0.1 s	0 s
Bonding	Bonding				
Link Check Interval	Link Chk Interval	LCCH1.BndChkTmms	25-1000 ms	1 ms	100 ms
PRP					
Interval for Sending Supervision Frames	Superv TX Interval		0-30 s	0.5 s	2 s
LSB of Destination MAC for Supervision Frames	Sup LSB Dest MAC		0-255	1	0
HSR	HSR				
HSR Transmission	HSR transmission	LCCH1.HSRTxTyp	Store-Forward Cut-Through		Store-Forward
Interval for Sending Supervision Frames	Superv TX Interval		0-30 s	0.5 s	2 s
LSB of Destination MAC for Supervision Frames	Sup LSB Dest MAC		0-255	1	0
RSTP	RSTP				
Brige Priority	Brige Priority	LCCH1.STPPrio	0-61440	4096	32768
Hello Time	Hello Time	LCCH1.STPHello	1-10 s	1 s	2 s
Max Age	Max Age	LCCH1.STPMaxAge	6-40 s	1 s	20 s
Forward Delay	Forward Delay	LCCH1.STPFwdDl	4-30 s	1 s	15 s
Port 1	Port 1				
Priority	Priority	LCCH1.STPPrio1	0-240	16	128
Cost	Cost	LCCH1.STPCost1	0-200000000	1	200000
Edge	Edge	LCCH1.STPEdge1	On / Off		Off
Port 2	Port 2				
Priority	Priority	LCCH1.STPPrio2	0-240	16	128
Cost	Cost	LCCH1.STPCost2	0-200000000	1	200000
Edge	Edge	LCCH1.STPEdge2	On / Off		Off

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / LAN Ports / Ports 3-4					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
LAN 3	LAN 3				
DHCP Enable	Enable DHCP		NO / YES		NO
IP Address	IP Address		ddd.ddd.ddd.ddd		192.168.1.81
Network Mask	Network Mask		ddd.ddd.ddd.ddd		255.255.255.0
Routing Tables	Routing tables				
Default Gateway	Default gateway				
Default route 1 IP address	IP default GW 1		ddd.ddd.ddd.ddd		0.0.0.0
Default route 1 metric	Metric def GW 1		0-65535	1	1
Default route 2 IP address	IP default GW 2		ddd.ddd.ddd.ddd		0.0.0.0
Default route 2 metric	Metric def GW 2		0-65535	1	1
Static routes	Static routes				
Destination address of route 1	Dest addr route 1		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 1	Netmask route 1		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 1	GW IP route 1		ddd.ddd.ddd.ddd		0.0.0.0
Destination address of route 2	Dest addr route 2		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 2	Netmask route 2		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 2	GW IP route 2		ddd.ddd.ddd.ddd		0.0.0.0
LAN 4	LAN 4				
DHCP Enable	Enable DHCP		NO / YES		NO
IP Address	IP Address		ddd.ddd.ddd.ddd		192.168.1.81
Network Mask	Network Mask		ddd.ddd.ddd.ddd		255.255.255.0
Routing Tables	Routing tables				
Default Gateway	Default gateway				
Default route 1 IP address	IP default GW 1		ddd.ddd.ddd.ddd		0.0.0.0
Default route 1 metric	Metric def GW 1		0-65535	1	1
Default route 2 IP address	IP default GW 2		ddd.ddd.ddd.ddd		0.0.0.0
Default route 2 metric	Metric def GW 2		0-65535	1	1
Static routes	Static routes				
Destination address of route 1	Dest addr route 1		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 1	Netmask route 1		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 1	GW IP route 1		ddd.ddd.ddd.ddd		0.0.0.0
Destination address of route 2	Dest addr route 2		ddd.ddd.ddd.ddd		0.0.0.0
Network mask of route 2	Netmask route 2		ddd.ddd.ddd.ddd		255.255.255.0
IP Gateway address of route 2	GW IP route 2		ddd.ddd.ddd.ddd		0.0.0.0

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / Ports / LAN Protocols					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Procome Protocol	PROCOME Protocol				
Port Number	Port Number		1-65535	1	32001
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Encrypted Prot.	Encrypted Prot.		NO / YES		YES
Authenticated Prot.	Authenticated Prot		NO / YES		SYES
Advanced Settings	Advanced Settings				
TCP KeepAlive Time	Tcp KeepAlive Time		0-32767	1	20
TCP KeepAlive Probes	Tcp KeepAlive Prob		1-127	1	2
TCP KeepAlive Interval	Tcp KeepAlive Int		0-32767	1	10
Protocol 1	Protocol 1				
Ethernet Protocol	Ethernet Protocol		None Procome Dnp 3.0 Modbus		None
Port Number	Port Number		1-65535	1	20000
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Encrypted Prot.	Encrypted Prot.		NO / YES		YES
Authenticated Prot.	Authenticated Prot		NO / YES		SYES
Advanced Settings	Advanced Settings				
TCP KeepAlive Time	Tcp KeepAlive Time		0-32767	1	20
TCP KeepAlive Probes	Tcp KeepAlive Prob		1-127	1	2
TCP KeepAlive Interval	Tcp KeepAlive Int		0-32767	1	10
Protocol 2	Protocol 2				
Ethernet Protocol	Ethernet Protocol		None Procome Dnp 3.0 Modbus		None
Port Number	Port Number		1-65535	1	20001
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Encrypted Prot.	Encrypted Prot.		NO / YES		YES
Authenticated Prot.	Authenticated Prot		NO / YES		SYES
Advanced Settings	Advanced Settings				
TCP KeepAlive Time	Tcp KeepAlive Time		0-32767	1	20
TCP KeepAlive Probes	Tcp KeepAlive Prob		1-127	1	2
TCP KeepAlive Interval	Tcp KeepAlive Int		0-32767	1	10

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / Ports / TCP/IP Protocols					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Protocol 3	Protocol 3				
Ethernet Protocol	Ethernet Protocol		None Procome Dnp 3.0 Modbus		None
Port Number	Port Number		1-65535	1	20002
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Encrypted Prot.	Encrypted Prot.		NO / YES		YES
Authenticated Prot.	Authenticated Prot		NO / YES		SYES
Advanced Settings	Advanced Settings				
TCP KeepAlive Time	Tcp KeepAlive Time		0-32767	1	20
TCP KeepAlive Probes	Tcp KeepAlive Prob		1-127	1	2
TCP KeepAlive Interval	Tcp KeepAlive Int		0-32767	1	10
Protocol 4	Protocol 4				
Ethernet Protocol	Ethernet Protocol		None Procome Dnp 3.0 Modbus		None
Port Number	Port Number		1-65535	1	20003
Comms Fail Timer	Comms Fail Time		0-600 s	0.1 s	60 s
Encrypted Prot.	Encrypted Prot.		NO / YES		YES
Authenticated Prot.	Authenticated Prot		NO / YES		SYES
Advanced Settings	Advanced Settings				
TCP KeepAlive Time	Tcp KeepAlive Time		0-32767	1	20
TCP KeepAlive Probes	Tcp KeepAlive Prob		1-127	1	2
TCP KeepAlive Interval	Tcp KeepAlive Int		0-32767	1	10

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / Protocols					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
PROCOME 3.0	Procome Protocol				
IED Address	Unit Number		0-254	1	0
DNP 3.0 Protocol	DNP 3.0 Protocol				
IED Address	Relay Number		0-65519	1	1
T. Confirm Timeout	T. Confirm Timeout		100-65535 ms	1	1000 ms
Max Retries	Max Retries		0-65535	1	0
Enable Unsolicited	Enab. Unsolicited		NO / YES		NO
Unsolicited Master No.	Unsol. Master No.		0-65519	1	1
Unsolicited Grouping Time	Uns. Grouping Time		100-65535 ms	1	1000 ms
Sync Interval	Syncr. Interval		0-120 min	1	0 min
Binary Changes Class	Binary Class		None Class 1 Class 2 Class 3		Class 1
Analog Changes Class	Analog Class		None Class 1 Class 2 Class 3		Class 2
Counter Changes Class	Counter Class		None Class 1 Class 2 Class 3		Class 3
Binary Status	Binary Status		NO / YES		YES
32 Bits Analog Inputs	32 Bit Analog Inp.		NO / YES		YES
Metering (16 Dead Bands)	Measures		0.0001-100	0.0001	100
Counters (20 Counter Dead Bands)	Counters		1-32767	1	1
MODBUS Protocol	MODBUS Protocol				
IED Address	Unit Number		0-247	1	1

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Communications / Protocols					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
IEC 61850					
GOOSE Channel			LAN1 LAN2 LAN3 LAN4		LAN1
Goose	Goose				
Simulation	Simulation				
Publications	Publication				
GCB 01 Simulated	GCB 01 Simulated		NO / YES		NO
GCB 02 Simulated	GCB 02 Simulated		NO / YES		NO
GCB 03 Simulated	GCB 03 Simulated		NO / YES		NO
GCB 04 Simulated	GCB 04 Simulated		NO / YES		NO
GCB 05 Simulated	GCB 05 Simulated		NO / YES		NO
GCB 06 Simulated	GCB 06 Simulated		NO / YES		NO
GCB 07 Simulated	GCB 07 Simulated		NO / YES		NO
GCB 08 Simulated	GCB 08 Simulated		NO / YES		NO
GCB 09 Simulated	GCB 09 Simulated		NO / YES		NO
GCB 10 Simulated	GCB 10 Simulated		NO / YES		NO
Subscription	Subscription		NO / YES		NO

The configuration settings of the PROCOME 3.0 protocol are:

- ***IED Address*** (0-254): it specifies the address of the relay (acting as RTU or Remote Terminal Unit) in relation to the rest of equipment that communicate with the same master station (MTU or Master Terminal Unit).

The DNP 3.0 protocol configuration settings include the definition of:

- ***Relay Number*** (0-65519): it specifies the address of the relay (acting as RTU or Remote Terminal Unit) in relation to the rest of equipment that communicate with the same master station (MTU or Master Terminal Unit). The 0xFFF0 to 0xFFFF addresses are reserved for the Broadcast addresses.
- ***T. Confirm TimeOut*** (100-65535): it specifies the time lapse (in milliseconds) from the time the IED sends a message requesting the master to confirm the Application layer (Level 7), until this confirmation is considered lost. The IED requests confirmation of the Application Layer when it sends spontaneous (Unsolicited) messages or in response to requests for Class 1 or Class 2 Data. When this time expires, the message is retransmitted the number of times specified in the N. Retries parameter.
- ***N. Retries*** (0-65535): number of retries of the Application Layer (N7). The default value is 0 (zero), indicating that no retransmission will be attempted.
- ***Enable Unsolicited*** (YES/NO): enables (YES) or disables (NO) sending spontaneous messages (Unsolicited); it is used in combination with the ***MTU Number*** parameter. For the relay to begin sending spontaneous messages the master must also enable them with the Function Code FC = 20.
- ***Master Number Unsolicited*** (0-65535): it specifies the address of the master station (MTU or Master Terminal Unit) to which the relay will send spontaneous (Unsolicited) messages. It is used in combination with Enable Unsolicited parameter. Addresses 0xFFF0 to 0xFFFF are reserved for Broadcast addresses.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- ***Time Grouping Unsolicited*** (100-65535): it specifies the time interval between the generation of a first event for an unsolicited message and the transmission of the message, with the purpose of grouping several events that may occur within this time interval in a single transmission message, in order not to saturate the communications line with multiple messages.
- ***Sync. Interval*** (0-120 minutes): it specifies the maximum time interval between two synchronizations. If no synchronization occurs within the interval, the need for synchronization is set in Internal Indication (IIN1-4 NEED TIME). This setting has no effect if the Sync. Interval is 0.

Up to 64 measurements or analog magnitudes can be set for DNP3 transmission. Among them, up to 16 measurements can be set for transmission upon a change request. To select the measurements to transmit upon a change request, enable the ***DNP3 Measurement Change*** control configuration option using ***ZIV e-NET Tool***®.

The measurement change transmission is set through two parameters for each measurement: ***Upper Limit*** (in profile I relays) or ***Maximum Value*** (in profile II relays) setting values and the ***Band*** setting value set for that measurement. Up to 16 band values may be configured through ***ZIVercomPlus***®, which will be associated to the measurements enabled for change transmission in the same sequence as they are ordered in ***ZIV e-NET Tool***®. This is: band value 000 will be assigned to the first measurement enabled for change transmission, 001 to the second, and so on up to the last measurement enabled, with the limit of 16. The band represents a percentage of the ***Maximum Value***, so that when a measurement change exceeds that band, the measurement value is annotated to be sent as change. When the relay receives a measurement change request, it will send all changes annotated.

Analog changes will not be annotated for measurements with option ***DNP3 Measurement Change*** enabled but with the band set to 100%, or measurements with option ***DNP3 Measurement Change*** not enabled, they being deemed disabled for change transmission. Additionally, these are other settings defined for the DNP3.0 Profile II and DNP 3.0 Profile II ETHERNET Protocols:

- ***Class for Binary Changes*** (CLASS 1, CLASS 2, CLASS 3, NONE). Assigns the class to the binary changes.
- ***Class for Analog Changes*** (CLASS 1, CLASS 2, CLASS 3, NONE). Assigns the class to the analog changes.
- ***Class for Counter Changes*** (CLASS 1, CLASS 2, CLASS 3, NONE). Assigns the class to the counter changes.
- ***"Status" Type Binary Inputs*** (YES-NO). Binary inputs used are according to "status" type inputs (YES) or binary inputs used are not sent according to "status" type inputs (NO).
- ***32 bits Analog Inputs*** (YES-NO). Analog inputs used are 32 bits resolution (YES) or analog inputs used are 16 bits resolution (NO).

In order for the relay to accept commands received through DNP3, the internal Remote Control signal must be active, for this, it must be activated through control logic.

The only configuration setting of the MODBUS protocol is the ***Relay Number*** (0-254), which specifies the relay address (acting as RTU or Remote Terminal Unit) with reference to the rest of relays communicating with the same master station (MTU or Master Terminal Unit).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.8.h Output Signals of the Communications Module

Table 1.5-4: Output Signals of the Communications Module

Name	Group	IEC 61850	Description	Vis.	Function
FALLO_LINK1	Errors and Alarms	LCCH1.LnkLiv	LAN1 Link Failure	I	Signal indicating link failure after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_COMS1		LCCH1.ChLiv	LAN1 Communications Failure	I	Signal indicating that no traffic exists after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_LINK2		LCCH1.RedLnkLiv	LAN2 Link Failure	I	Signal indicating link failure after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_COMS2		LCCH1.RedChLiv	LAN2 Communications Failure	I	Signal indicating that no traffic exists after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_LINK3		LCCH2.LnkLiv	LAN3 Link Failure	I	Signal indicating link failure after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_COMS3		LCCH2.ChLiv	LAN3 Communications Failure	I	Signal indicating that no traffic exists after the timer set time times out. IEC 61850 signal indicates otherwise.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.5-4: Output Signals of the Communications Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
FALLO_LINK4	Errors and Alarms	LCCH2.RedLnkLiv	LAN4 Link Failure	I	Signal indicating link failure after the timer set time times out. IEC 61850 signal indicates otherwise.
FALLO_COMS4		LCCH2.RedChLiv	LAN4 Communications Failure	I	Signal indicating that no traffic exists after the timer set time times out. IEC 61850 signal indicates otherwise.
AVALANCHAENLAN1		LCCH1.InOv	Network Congestion Detected on LAN1		The number of frames received exceeds the limit supported and the relay discards incoming traffic through this port.
AVALANCHAENLAN2		LCCH1.RedInOv	Network Congestion Detected on LAN2		The number of frames received exceeds the limit supported and the relay discards incoming traffic through this port.
AVALANCHAENLAN3		LCCH2.InOv	Network Congestion Detected on LAN3		The number of frames received exceeds the limit supported and the relay discards incoming traffic through this port.
AVALANCHAENLAN4		LCCH2.RedInOv	Network Congestion Detected on LAN4		The number of frames received exceeds the limit supported and the relay discards incoming traffic through this port.
BONDINGACT1	Others	LCCH1.BndActCh	Bonding LAN1 active		Indicates active Bonding port. In IEC 61850, FALSE stands for LAN1 port and TRUE for LAN2 port.
BONDINGACT2			Bonding LAN2 active		
BONDINGACT3		LCCH2.BndActCh	Bonding LAN3 active		Indicates active Bonding port. In IEC 61850, FALSE stands for LAN3 port and TRUE for LAN4 port.
BONDINGACT4			Bonding LAN4 active		

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.9 Time Synchronization

1.5.9.a Manual Time Synchronization

If synchronization is not detected from any source, the relay will accept manual synchronization through the HMI.

1.5.9.b Time Synchronization by Protocol

Relays may be synchronized as follows:

- **Protocol PROCOME**: the relay can receive the date and time through protocol PROCOME either from a central unit or from the communications program, which will send the PC local time. The relay will synchronize if IRIG-B or SNTP synchronization is not detected.
- **Protocol DNP3**: the relay may receive the date and time through protocol DNP3 from a server. The relay will synchronize if IRIG-B, SNTP or PROCOME synchronization is not detected.

1.5.9.c Synchronization by SNTP

IEC 61850 relays can be synchronized through protocol SNTP by means of broadcast or unicast and with one or two servers. The relay will be synchronized through SNTP if IRIG-B synchronization is not detected. For this, there is a Synchronization section within the settings menu, where the following settings can be found.

1.5.9.d Synchronization by IRIG-B 123 and 003

Relays are provided (depending on the model) with a BNC type input for IRIG-B 123 or 003 standard time synchronization signals. Said input is located at the relay rear panel. Synchronization accuracy is ±1ms.

In case the relay is receiving an IRIG-B synchronization signal, access from HMI to **Date and Time** settings is denied.

An output can be configured to show IRIG-B signal received status. This output remains active while the relay receives correctly said signal. These relays are also prepared for indication of both the loss and recovery of IRIG-B signal by generating events associated to each of these circumstances.

Discerning whether the time received through BNC connector corresponds to **UTC Time** or a given **Time Zone (Local)** is possible through ***IRIG-B Time Type*** setting.

In the first case, a correction must be introduced to adapt the UTC time to the time zone of the relay site. The ***Local Time Zone*** setting within the ***Date and Time*** settings group is used for this purpose, which allows putting UTC time forward or back as required.

In the second case, the relay receives the time signal already adapted to the local time zone and no correction is needed. In this case local ***Local Time Zone*** has no effect.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.5.9.e PTP Synchronization

The precision time protocol also known by the acronym PTP is originally defined by the IEEE 1588 standard and is used for relay synchronization through a local area network, reaching a microsecond accuracy, namely, it is a protocol far more accurate than SNTP, IRIG-B or serial protocol.

In order to reach this accuracy, the synchronization system uses protocol messages sent between PTP nodes to determine the clock phase difference and the delays inherent to the network, such that propagation and latency times are taken into account.

1.5.9.f Synchronization Settings

Settings / Synchronization					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Clock Priority	Clock Priority		IRIG-B PTP		IRIG-B
IRIG-B	IRIG-B				
Type of Synchronization Signal	Type of sync	LTIM1.SynSigTyp	Disabled PPS Signal (Pulses Per Second) IRIG-B003 IRIG-B123		Disabled
IRIG-B Time Type	IRIG-B Time Type	LTIM1.IrigBTmTyp	Local Time UTC Time		Local Time
SNTP	SNTP				
Enable SNTP	Enable SNTP	LNTP1.SNTPEna	NO / YES		NO
Enable Broadcast Synchronization	Enable Broadcast	LNTP1.BcSynEna	NO / YES		NO
Enable Unicast Synchronization	Enable Unicast	LNTP1.UcSynEna	NO / YES		NO
Main Server IP Address	Main Server	LNTP1.IPSrv1	ddd.ddd.ddd.ddd		0.0.0.0
Backup Server IP Address	Backup Server	LNTP1.IPSrv2	ddd.ddd.ddd.ddd		0.0.0.0
Unicast Valid Time	Unicast Valid Time	LNTP1.UcOkTms	10-1000000 s	1 s	30 s
Unicast Error Time	Unicast Error Time	LNTP1.UcErrTms	10-1000000 s	1 s	30 s
Number of Retry Attempts	Retry Attempts	LNTP1.ConnReNum	1 - 10	1	3
Synchronization Period	Synch Period	LNTP1.SynPerTms	10-1000000 s	1 s	10 s
Retry Period	Retry Period	LNTP1.ReSynTms	10-1000000 s	1 s	10 s
Broadcast Valid Time	Broadcast Valid T.	LNTP1.BcOkTms	0-1000000 s	1 s	0 s
Broadcast Error Time	Broadcast Error T.	LNTP1.BcErrTms	0-1000000 s	1 s	0 s
Maximum Time Gap Allowed in Synchronization	Max Time Differ.	LNTP1.SynDifTms	0-1000000 s	1 s	0 s

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Synchronization					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Ignore Leap Indicator in Synchronization	Ignore Leap Indic.	LNTP1.InhLI	NO / YES		NO
Synchronization State Calculation Method	Sync State Calcul.	LNTP1.SynClc	Time Delay Leap Indicator		Time Delay
Force Unicast Query	Force Unicast	LNTP1.ForceUc	NO / YES		YES
Retry Period	Retry Period SNTP	LNTP1.ConnReTms	1-1000000 s	1 s	3 s
PTP	PTP				
Domain Number	Domain Number	LPTP1.DomainNum	0-127&254	1	254
eth0	eth0				
Enable PTP	Enable	LPTP1.PTPEna1	NO / YES		NO
Log ch calc interv	Log ch calc interv	LPTP1.DlClcPer1	0.125s 0.25s 0.5s 1s 2s 4s 8s 16s 32s		1s
Delay	Delay	LPTP1.DlAdjTm1	0–1000000 ns	1ns	0ns
Asymmetry	Asymmetry	LPTP1.AsymAdjTm1	-10000 to 10000	1ns	0ns
eth1	eth1				
Enable PTP	Enable	LPTP1.PTPEna1	NO / YES		NO
Log ch calc interv	Log ch calc interv	LPTP1.DlClcPer1	0.125s 0.25s 0.5s 1s 2s 4s 8s 16s 32s		1s
Delay	Delay	LPTP1.DlAdjTm1	0–1000000 ns	1ns	0ns
Asymmetry	Asymmetry	LPTP1.AsymAdjTm1	-10000 to 10000	1ns	0ns

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Synchronization					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
eth2	eth2				
Enable PTP	Enable	LPTP1.PTPEna1	NO / YES		NO
Log ch calc interv	Log ch calc interv	LPTP1.DlClcPer1	0.125s 0.25s 0.5s 1s 2s 4s 8s 16s 32s		1s
Delay	Delay	LPTP1.DlAdjTm1	0–1000000 ns	1ns	0ns
Asymmetry	Asymmetry	LPTP1.AsymAdjTm1	-10000 to 10000	1ns	0ns
eth3	eth3				
Enable PTP	Enable	LPTP1.PTPEna1	NO / YES		NO
Log ch calc interv	Log ch calc interv	LPTP1.DlClcPer1	0.125s 0.25s 0.5s 1s 2s 4s 8s 16s 32s		1s
Delay	Delay	LPTP1.DlAdjTm1	0–1000000 ns	1ns	0ns
Asymmetry	Asymmetry	LPTP1.AsymAdjTm1	-10000 to 10000	1ns	0ns

1.5.9.g Output Signals of the Synchronization Module

Table 1.5-5: Output Signals of the Synchronization Module

Name	Group	IEC 61850	Description	Vis.	Function
SIGNAL_IRIGB	Others	LTIM1.SynSt	IRIGB Active	I	Signal indicating that IRIG-B signal is being received.
SNTP_SINCRONIZADO			Synchronization by SNTP	I	Signal indicating that SNTP signal is being received.
PTP_SINCRONIZADO			Synchronization by PTP	I	Signal indicating that PTP signal is being received.
SICRONIZACIONRELOJ		-	Clock Synchronization		Signal indicating that the clock has been synchronized.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.6 Installation and Commissioning

1.6.1	General	1.6-2
1.6.2	Accuracy	1.6-2
1.6.3	Installation	1.6-3
1.6.4	Preliminary Inspection	1.6-4
1.6.5	Tests	1.6-5
1.6.5.a	Isolation Test	1.6-5
1.6.5.b	Power Supply Test	1.6-6
1.6.5.c	Metering Tests	1.6-6

1.6.1 General

Improper handling of electrical equipment is extremely dangerous; therefore, only skilled and qualified personnel familiar with appropriate safety procedures and precautions should work with this equipment. Damage to equipment and injury to personnel can result when proper safety precautions are not followed.

The following general safety precautions are provided as a reminder:

- **High magnitude voltages are present in Power Supply and metering circuits even after equipment has been disconnected.**
- **Equipment should be solidly grounded before handling or operating.**
- **Under no circumstances should the operating limits of the equipment be exceeded (voltage, current, etc.).**
- **The power supply voltage should be disconnected from the equipment before extracting or inserting any module; otherwise damage may result.**

The tests defined next are those indicated for the start-up of an IED. They do not necessarily coincide with the final manufacturing tests to which each manufactured equipment is subjected. The number, the type and the specific characteristics of the acceptance tests are model dependent.

1.6.2 Accuracy

The accuracy of the measuring instruments and test source signals (auxiliary power supply voltage, AC currents and AC voltages) is key in electrical testing. Therefore, the information specified in the Technical Data section (2.1) of this manual can only be reasonably verified with test equipment under normal reference conditions and with the tolerances indicated in the UNE 21-136 and IEC 255 standards in addition to using precision instruments.

It is extremely important that there be little or no distortion (<2%) in the test source signals as harmonics can affect internal measuring of the equipment. For example, distortions will affect this IED, made up of non-linear elements, differently from an AC ammeter, because the measurement is made differently in both cases.

It must be emphasized that the accuracy of the test will depend on the instruments used for measuring as well as the source signals used. Therefore, tests performed with secondary equipment should focus on operation verification and not on measuring accuracy.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.6.3 Installation

- **Location**

The place where the equipment is installed must fulfill some minimum requirements, not only to guarantee correct operation and the maximum duration of useful life, but also to facilitate placing the unit in service and performing necessary maintenance. These minimum requirements are the following:

- Absence of dust.
- Absence of humidity.
- Absence of vibration.
- Good lighting.
- Easy access.
- Horizontal or vertical mounting.

Installation should be accomplished in accordance with the dimension diagrams.

- **Connections**

The first terminal of the terminal block corresponding to the auxiliary power supply must be connected to ground so that the filter circuits can operate. The cable used for this connection should be 14 AWG stranded wire, with a minimum cross section of 2 mm^2. The length of the connection to ground should be as short as possible, but not more than 75 inches (30 cm). In addition, the ground terminal of the case, located on the rear of the unit, should be connected to ground.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.6.4 Preliminary Inspection

The following equipment aspects should be examined:

- The unit is in good physical condition, mechanical parts are securely attached and no assembly screws are missing.
- The unit model number and specifications agree with the equipment order.

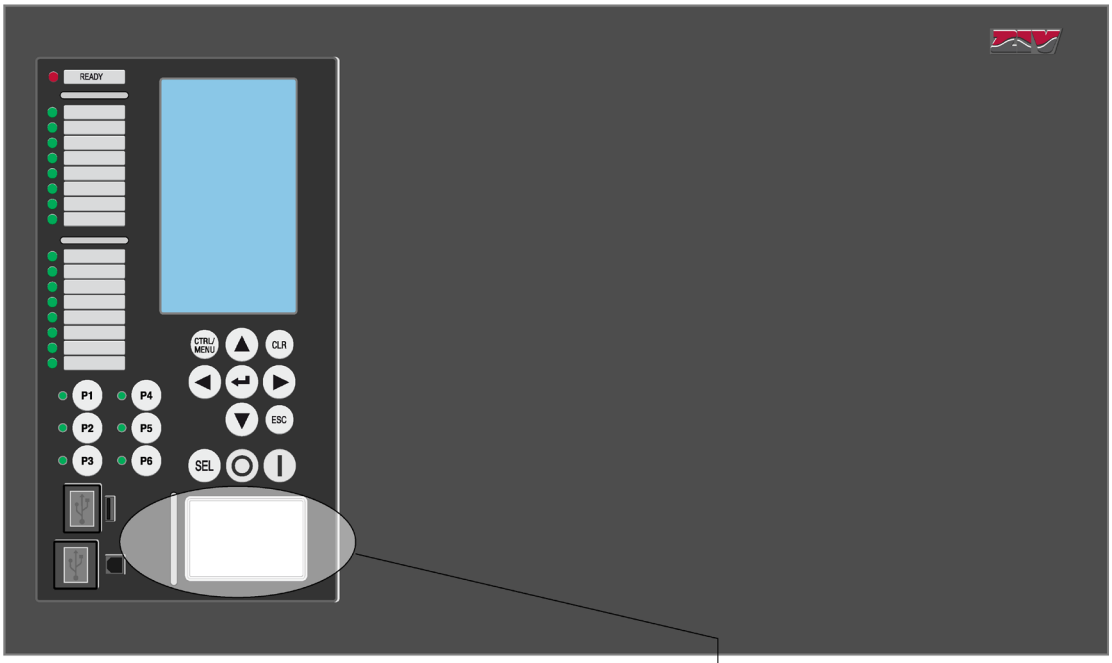


Figure 1.6.1: Name Plate (RTF).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.6.5 Tests

1.6.5.a Isolation Test

While testing for isolation of switchgear and external wiring, the IED must be disconnected to avoid damage in case the test is not performed properly or if there are shorts in the harness, since the manufacturer has performed isolation testing on 100% of the units.

- **Common Mode**

All the terminals of the IED must be short-circuited, except those that relate to the power supply. The enclosure ground terminal must also be disconnected. Then 2000 Vac are applied between the interconnected terminals and the metal case for 1 min or 2500 Vac during 1s between the terminal group and the metal enclosure. When the IED has the inputs, outputs and converters expansion card, terminals of the transducers do not need to be short-circuited (See External Connection Schemes).

- **Between groups**

The isolation groups are made up of the current and voltage inputs (independent channels), digital inputs, auxiliary outputs, trip and close contacts and power supply. Refer to the connection's schematic to identify the terminals to group for performing the test. Then 2500 VAC are applied during 1 sec. between each pair of groups. For the transducers test 1000 VAC are applied during one second between this group and all the rest.



There are internal capacitors that can generate high voltage if the test points are removed for the insulation test without reducing the test voltage.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.6.5.b Power Supply Test

Connect the power supply as indicated in following table.

VDC PROT	CON1P	CON2P
Slot A pin 3(+) - 2(-)	Slot A pin 6 - 5	Slot A pin 6 - 4

It is important to verify that, when the IED is not energized, the contacts designated CON2P in the table mentioned previously are closed, and those designated CON1P are open. Then it is fed its rated voltage and the contacts designated CON1P and CON2P must change state and the “In Service” LED must light up.

1.6.5.c Metering Tests

The currents and voltages which, as an example, are indicated in the following table, will be applied to each of the channels and the following measures will be verified:

Applied Current or Voltage	Measured Current or Voltage	Phase of I or V applied	Phase of I or V measured	Frequency Applied (V > 20 Vac)	Frequency Measured (V > 20 Vac)
X	X ±1%	Y	Y ±1º	Z	Z ±5 mHz

If high current values are to be checked, they will be applied the shortest possible time; for example, less than 8 seconds for 20A. For angle display, phase A voltage must be applied or inject current into the phase A as a function of the reference angle setting value and the injected values must exceed the setting values set for this purpose. In order to be able to measure the frequency, voltage must be injected into any phase, taking into account that the instantaneous value of the Clarke alfa voltage considers a value above the “Inhibit Voltage” disable setting.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.7 Onload Test

1.7.1 Introduction 1.7-2
1.7.2 Voltage Connections 1.7-2
1.7.3 Current Connections 1.7-2

1.7.1 Introduction

The objectives of Onload Test are the following ones:

- Confirm that the external wiring of the voltage and current analog input channels is correct.
- Check the polarity of the current transformers.
- Check the voltage and current measurements (module and angle).

In order to proceed with the test, primary injections will be done to check the polarity and transformation ratios. These tests can only be carried out if there are no restrictions related to the energization of the bay and all the other devices of the bay where the protection relay is located have already been commissioned.

Before starting the tests, check that all the test leads have been removed and ensure that the external wiring is properly connected (it is possible that during the commissioning tests external wirings have been disconnected).

1.7.2 Voltage Connections

Using a multimeter check that the secondary voltage measurements are correctly rated, and by means of a phase rotation meter confirm that the system phase rotation is the correct one.

Compare the secondary multimeter values with the measurements the relay shows in the measurement screen when the transformation ratio is set to 1. Check not only the module but also the angle. Modify the setting in order to show the measurements in primary values. The measurements that are displays in the HMI of the device or in the communication program should comply with the values which are specified in the Measurement Accuracy paragraph in Chapter 1.3, Technical Data.

1.7.3 Current Connections

Place a multimeter in series with each of the analog current inputs of the relay in order to test the secondary values of each phase. This test will be carried out comparing the value of the multimeter with the value displayed in the HMI of the relay when the transformation ratio is set to 1. Check not only the module but also the angle. Modify the setting in order to show the measurements in primary values. The measurements that are displays in the HMI of the device or in the communication program should comply with the values which are specified in the Measurement Accuracy paragraph in Chapter 1.3, Technical Data.

Check that when injecting a balanced system, the current which is flowing through the neutral circuit of the transformer is negligible.

Ensure the current polarity is the correct one measuring the phase angle between the current and the voltage which are being injected.

Check that for load current flowing outside the bay (forward direction) the active power measurement is positive while for load current flowing inside the bay (reverse direction) the active power measurement is negative.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.8 Standards and Type Tests

1.8.1 Insulation 1.8-2
1.8.2 Electromagnetic Compatibility 1.8-3
1.8.3 Environmental Test 1.8-4
1.8.4 Power Supply 1.8-5
1.8.5 Mechanical Test 1.8-5

The equipment satisfies the standards indicated below. When not specified, the standard is IEC-60255.

1.8.1 Insulation

Insulation Test (Dielectric Strength)	*IEC-60255-5 / 60255-27*
Between all circuit terminals and ground	
Analog Inputs, DIs, DOs and PS	**2 kV**, **50/60 Hz**, for 1min
Communications Ports	**1 kV**, **50/60 Hz**, for 1min
Between all circuit terminals	
Analog Inputs, DIs, DOs and PS	**2 kV**, **50/60 Hz**, for 1min
Measurement of Insulation Resistance	*IEC-60255-5 / 60255-27*
Common mode	**R ≥ 100 MΩ** or **5µA**
Differential mode	**R ≥ 100 kΩ** or **5mA**
Voltage Impulse Test	*IEC-60255-5 (UNED21-136-83/5) / 60255-27*
Common mode	
Analog Inputs, DIs, DOs and PS	**5 kV**; **1.2/50 µs**; **0.5 J**
Communications Ports	**1 kV**; **1.2/50 µs**; **0.5 J**
Differential mode	
DOs	**1 kV**; **1.2/50 µs**
Power Supply	**3 kV**; **1.2/50 µs**

Note: IEC60255-27 standard tests for altitude up to 2 000 m.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.8.2 Electromagnetic Compatibility

100khz and 1 MHz Burst Test	*IEC-60255-22-1 / 61000-4-18*
Common mode	**2.5 kV**
Differential mode	**1 kV**
Damped Oscillatory Magnetic Field Immunity Test	*IEC-61000-4-10*
100KHz and 40 Transients/s	**±100 A/m**
1MHz and 400 Transient/s	**±100 A/m**
Fast Transient Disturbance Test	*IEC-60255-22-4 Class IV (IEC 61000-4-4)* **4 kV (5kz)**
Radiated Electromagnetic Field Disturbance	*IEC 61000-4-3 Class III*
AM 80% 1KHz, range 80MHz-3GHz	**10 V/m**
Amplitude modulated (*EN 50140*)	**10 V/m**
Conducted Electromagnetic Field Disturbance	*IEC 61000-4-6 Class III (IEC 50141)*
Frequency band from 0.15 to 80Mhz	**10 Vrms**
Electrostatic Discharge	*IEC-60255-22-2 Class IV (IEC 61000-4-2)*
Contact Mode	**±8 kV ±10 %**
In Air Mode	**±15 kV ±10 %**

Surge Immunity Test	*IEC-61000-4-5 (UNE 61000-4-5)* **(1.2/50µs - 8/20µs)**
Differential mode	**±2 kV**
Common mode	**±4 kV**

Radiated Electromagnetic Field Disturbance at Industrial Frequency (50/60 Hz)	*IEC-61000-4-8*

Radio Frequency Emissivity	*EN55022* (Conducted) *EN55011* (Radiated)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.8.3 Environmental Test

Temperature	*IEC-60068-2*
Cold work limit conditions	*IEC-60068-2-1* **-40º C**, **96 hours**
Dry heat limit conditions	*IEC-60068-2-2* **+85º C**, **96 hours**
Humid heat	*IEC-60068-2-78* **+40º C, 93% relative humidity, 96h**,
Quick temperature changes	*IEC-60068-2-14 / IEC-61131-2* IED disconnected **-25º C** for **3h** and **+70º C** for **3h** (**5 cycles**)
Changes in humidity	*IEC-60068-2-30 / IEC-61131-2*
Temperature change according to norm	**+55º C** for **12h** and **+25º C** for **12h** (**6 cycles**)
Humidity variable according to norm	
Operating range	From **-25º C** to **+70º C**
Storage range	From **-40º C** to **+85º C**

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.8.4 Power Supply

DC Alimentation Ripple Immunity	*61000-4-17*
Ripple	**15%**
Dips, Interruptions and Gradual On / Off Immunity	*61000-4-29*
Dip 100%	**100ms**
Dip 60%	**200ms**
Dip 30%	**500ms**
Inverse Polarity of the Power Supply	*IEC-61131-2*
Resistance of Ground Connection	*IEC-61131-2*
Surge Capacity	*IEC-60044-1*

1.8.5 Mechanical Test

Vibration (sinusoidal)	*IEC-60255-21-1*
a) Response: (Equipment running). Class II	
b) Endurance: (Equipment off). Class I	
Mechanical Shock and Bump Test	*IEC-60255-21-2 Class I*
Earthquakes	*IEC-60255-21-3 Class I*
External Protection Levels	*IEC-60529 / IEC-60068-2-75*
Front	*IP54* (Mounting into cell with gasket)
Rear Protection	*IP20*
	IP10 in Analog Terminals
Side	*IP30*
Mechanical Protection	*IK07*

CEEIEC: International Electrotechnical Commission / CEI: Comisión Electrotécnica Internacional.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.9 Schemes and Drawings

Analog Channels

Dimension and Drill Hole Schemes

6U x 1/3 19” (GRAPHIC / Extended display included)	>>	4BF0105/0004
6U x 1/2 19” (GRAPHIC / Extended display included)	>>	4BF0105/0005
6U x 1/3 19” (ALPHANUMERIC)	>>	4BF0105/0006
6U x 1/2 19” (ALPHANUMERIC)	>>	4BF0105/0007

External Connection Schemes

CPU	>>	3RX0206/0001
PS and Digital I/O	>>	3RX0206/0002
Digital I/O	>>	3RX0206/0003
Digital I/O	>>	3RX0206/0004
Digital I/O	>>	3RX0206/0009
20 DI all independent (card type digit 5)	>>	3RX0206/0015
Analog Inputs	>>	3RX0206/0010

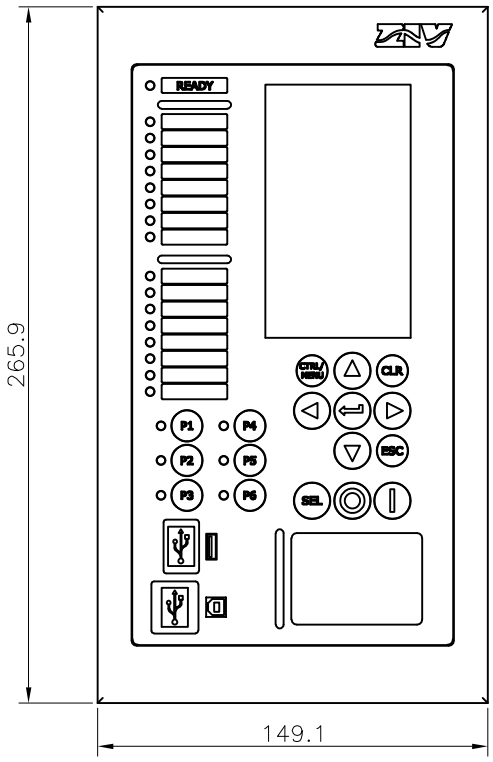
Example: External Connection of Analog Inputs

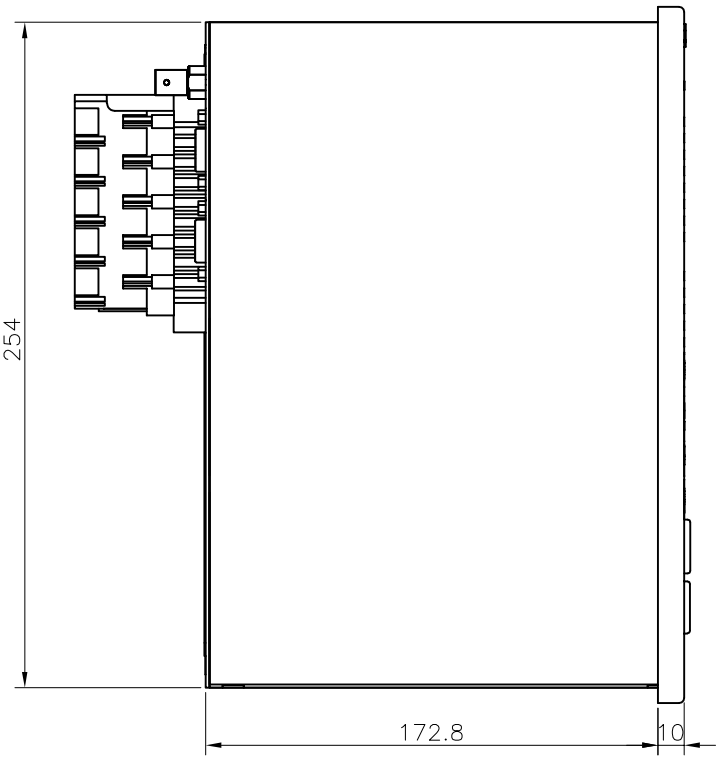
- **Analog Channels RTF-A for models without Short-Circuitable connectors**

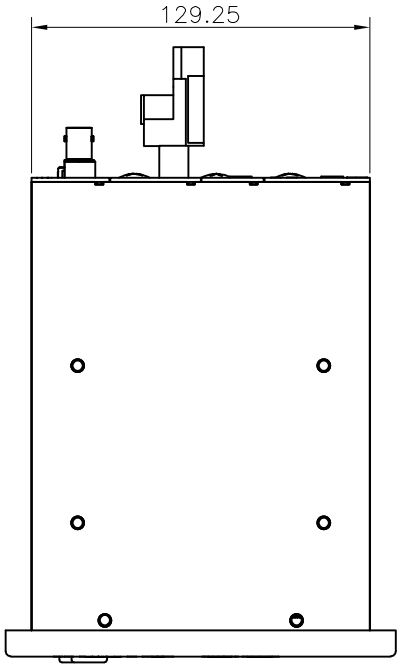
Magnitude	Analog channels	Description of analogue channels	SLOT (1/3 rack)	SLOT (1/2 rack)	SLOT (1 rack)	PINS
CONTROL VOLTAGE	VCTRL	VOLTAGE INPUT 1	C	E	K	1-2
LOCAL CURRENT	ILOC	CURRENT INPUT 1	C	E	K	3-4
PRALLEL CURRENT	IPAR	CURRENT INPUT 2	C	E	K	5-6

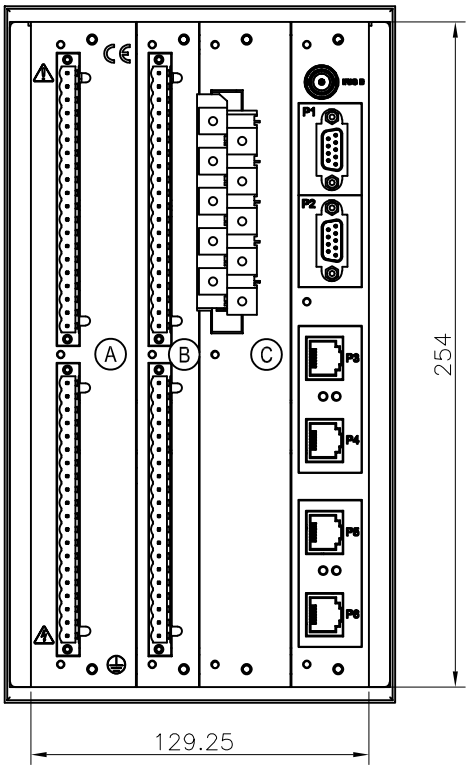
- **Analog Channels RTF-A for models with Short-Circuitable connectors**

Magnitude	Analog channels	Description of analogue channels	SLOT (1/2 rack)	SLOT (1 rack)	PINS
CONTROL VOLTAGE	VCTRL	VOLTAGE INPUT 1	D	J	1-2
LOCAL CURRENT	ILOC	CURRENT INPUT 1	D	J	3-4
PRALLEL CURRENT	IPAR	CURRENT INPUT 2	D	J	5-6









"ATENCION" *"WARNING"*

El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.

The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.		0	CD	1	
2		3		4	
5		6		7	
8		9		10	
11		12		13	
14		15		16	

TITULO: DIMENSIONES CAJA RTF 1/3 RACK DISPLAY GRAFICO
TITLE: RTF BOX 1/3 RACK GRAPHICAL DISPLAY DIMENSIONS

PROYECTO / *PROJECT:* RTF / *RTF*

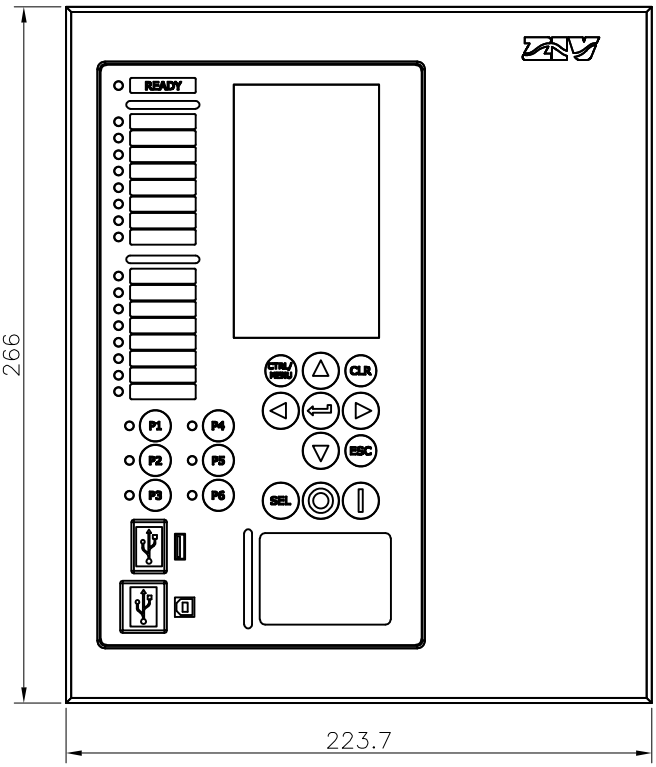
Rev.0

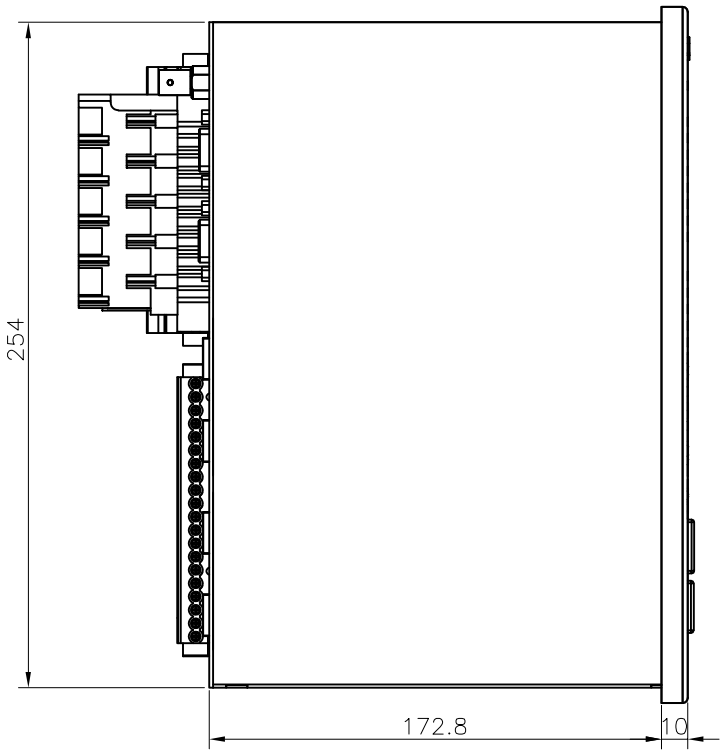
NUM: 4BF0105/0004

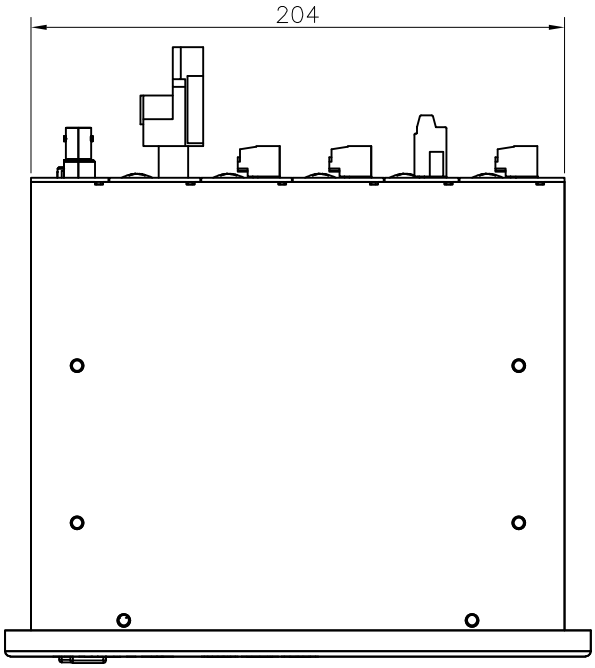
	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	06/02/19	J.M.S.
Aprobado / *Approved*	06/02/19	P.A.

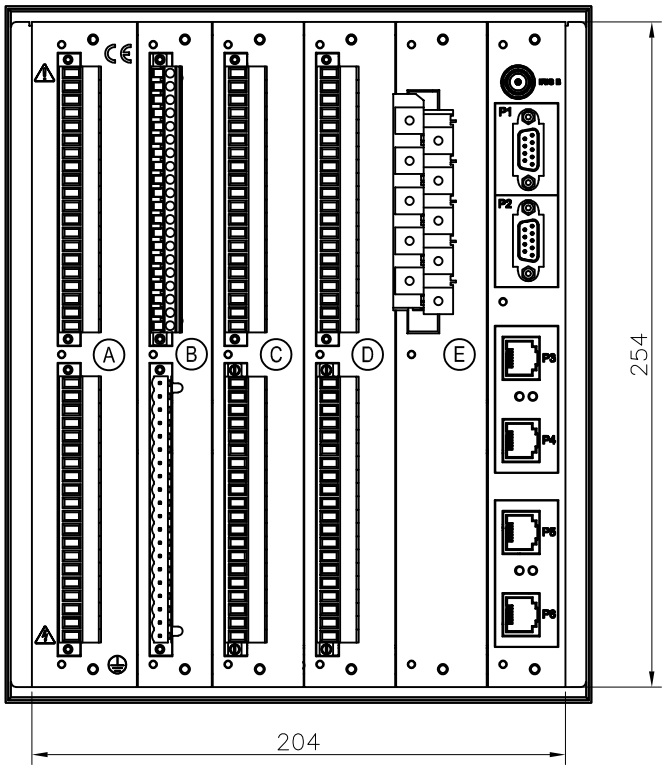
Hoja / *Sheet:* 1

Continua en Hoja: *Continued on sheet:* –









"ATENCION" *"WARNING"*

El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.

The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD	1
2	3		4
5	6		7
8	9		10
11	12		13
14	15		16

TITULO: DIMENSIONES CAJA RTF 1/2 RACK DISPLAY GRAFICO
TITLE: RTF BOX 1/2 RACK GRAPHICAL DISPLAY DIMENSIONS

PROYECTO / *PROJECT:* RTF / *RTF*

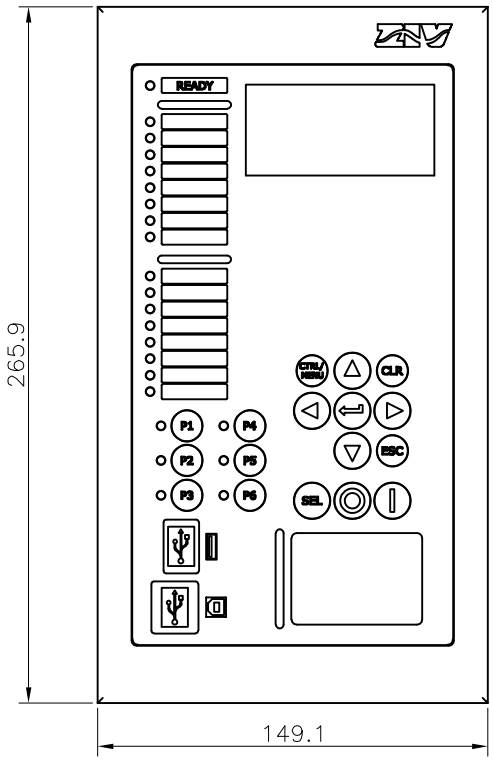
Rev.0

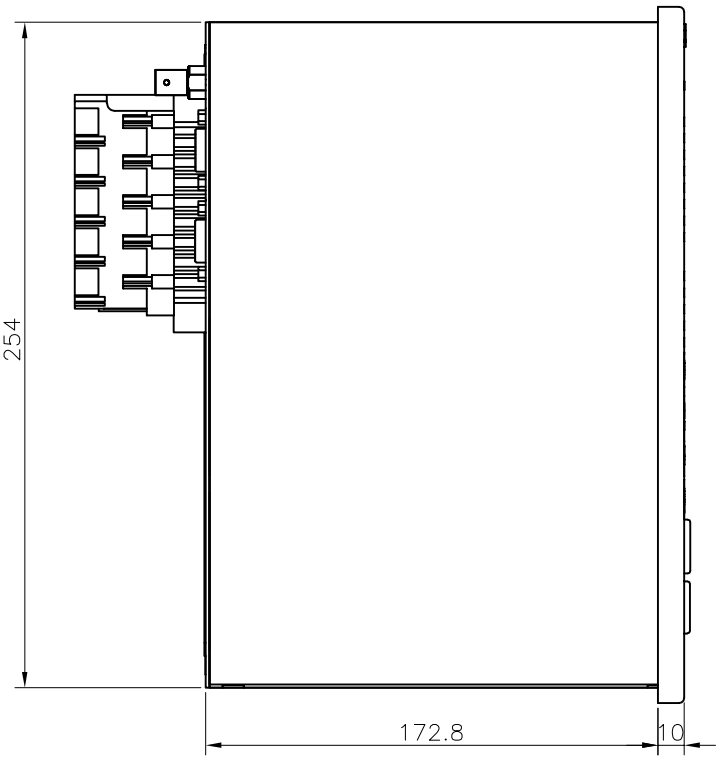
NUM: 4BF0105/0005

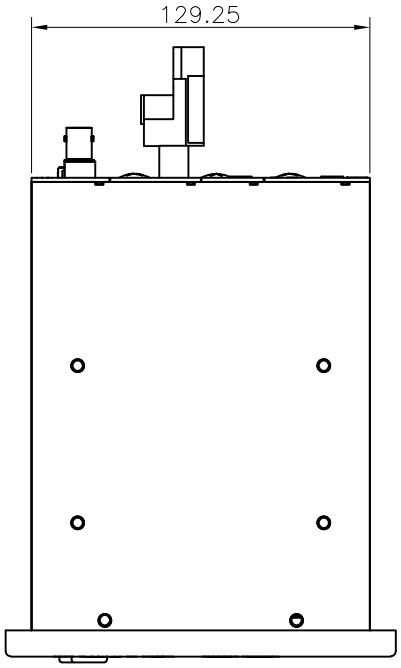
	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	06/02/19	J.M.S.
Aprobado / *Approved*	06/02/19	P.A.

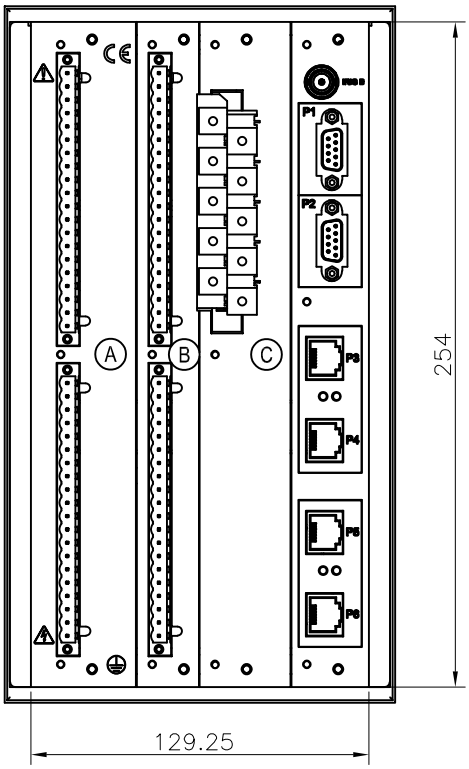
Hoja / *Sheet:* 1

Continua en Hoja: *Continued on sheet:* –









"ATENCION" *"WARNING"*

El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.

The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.		0	CD	1	
2		3		4	
5		6		7	
8		9		10	
11		12		13	
14		15		16	

TITULO: DIMENSIONES CAJA RTF 1/3 RACK DISPLAY ALFANUMERICO
TITLE: RTF BOX 1/3 RACK ALPHANUMERIC DISPLAY DIMENSIONS

PROYECTO / *PROJECT:* RTF / *RTF*

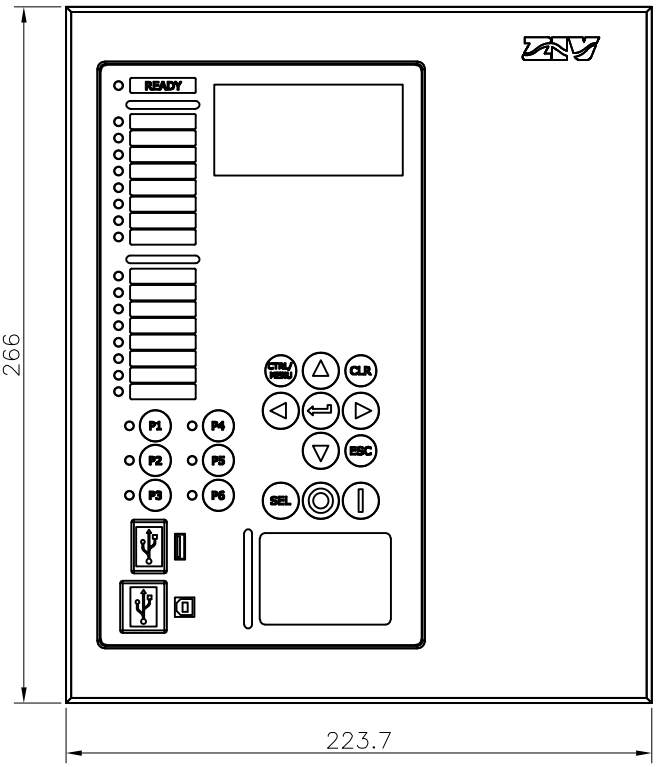
Rev.0

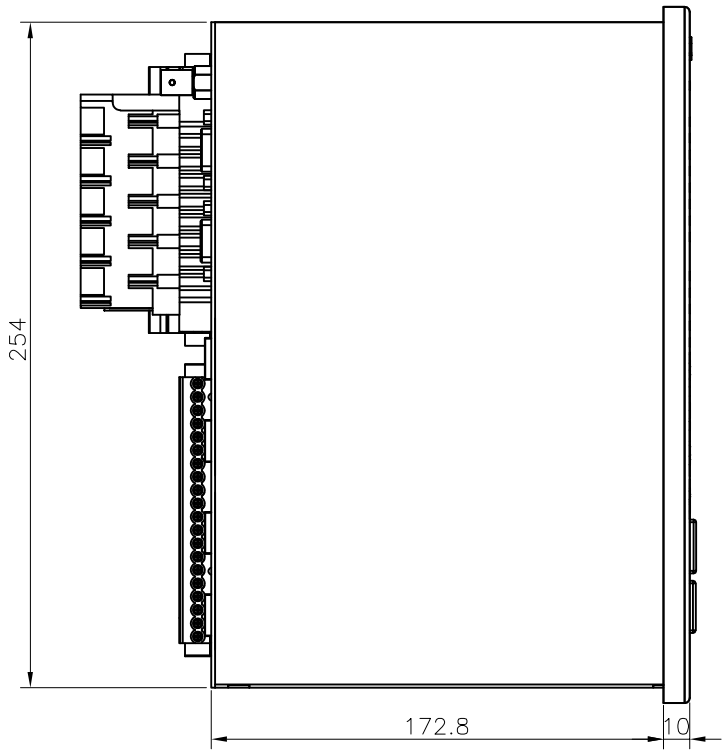
NUM: 4BF0105/0006

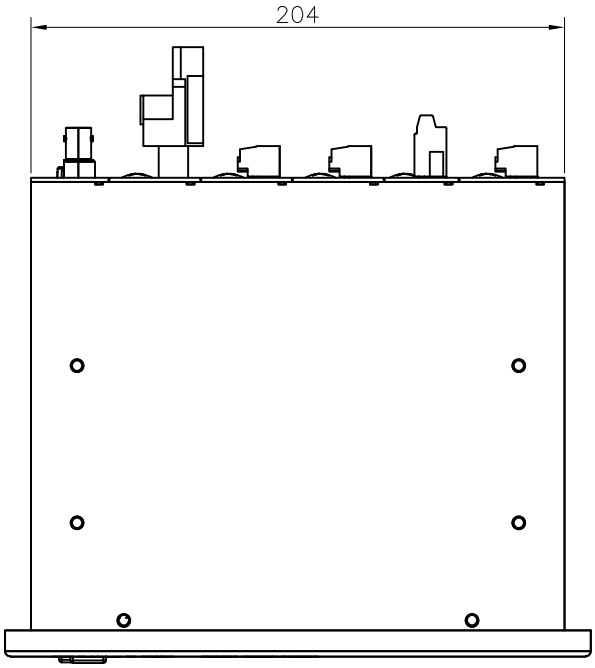
	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	06/02/19	J.M.S.
Aprobado / *Approved*	06/02/19	P.A.

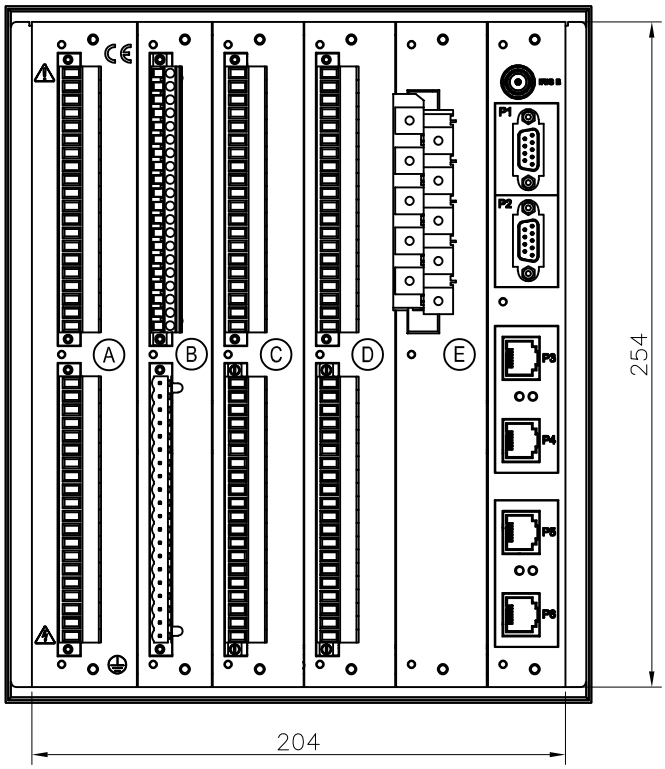
Hoja / *Sheet:* 1

Continua en Hoja: *Continued on sheet:* –









"ATENCION" *"WARNING"*

El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.

The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD	1
2	3		4
5	6		7
8	9		10
11	12		13
14	15		16

TITULO: DIMENSIONES CAJA RTF 1/2 RACK DISPLAY ALFANUMERICO
TITLE: RTF BOX 1/2 RACK ALPHANUMERIC DISPLAY DIMENSIONS

PROYECTO / *PROJECT:* RTF / *RTF*

Rev.0

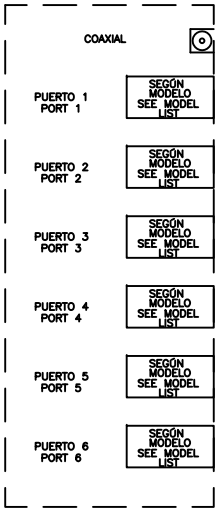
NUM: 4BF0105/0007

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	06/02/19	J.M.S.
Aprobado / *Approved*	06/02/19	P.A.

Hoja / *Sheet:* 1

Continua en Hoja: *Continued on sheet:* –

COMMUNICATION MODULE
MÓDULO COMUNICACIONES



SERIAL PORT
PUERTO SERIE
RS-232 FULL MODEM

PIN	SEÑAL
1	DCD
2	RX
3	TX
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI



SERIAL PORT
PUERTO SERIE
RS-232 / RS-485

PIN	SEÑAL
1	LIBRE / *FREE*
2	RX
3	TX
4	RS485+
5	GND
6	RS485-
7	LIBRE / *FREE*
8	LIBRE / *FREE*
9	LIBRE / *FREE*



SERIAL PORT RJ45
PUERTO SERIE RJ45

PIN	SEÑAL
1	TX+
2	TX-
3	RX+
4	N/C
5	N/C
6	RX-
7	N/C
8	N/C

RACK	1/3			
SLOT	A	B	C	
				CPU
MODEL I#F#-###	#	#	#	XYZW

RACK	1/2					
SLOT	A	B	C	D	E	
						CPU
MODEL I#F#-###	#	#	#	#	#	XYZW

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
												CPU
MODEL I#F#-###	#	#	#	#	#	#	#	#	#	#	#	XYZW

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología .
The contents of this document belong to ZIV Aplicaciones y Tecnología and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnología .

REV.	0	CD500004568	1		2		3		4	
5		6		7		8		9		10
11		12		13		14		15		16

Z I V Aplicaciones y Tecnología

TITULO: CONEXIONES EXTERNAS CPU
TITLE: EXTERNAL CONNECTIONS CPU

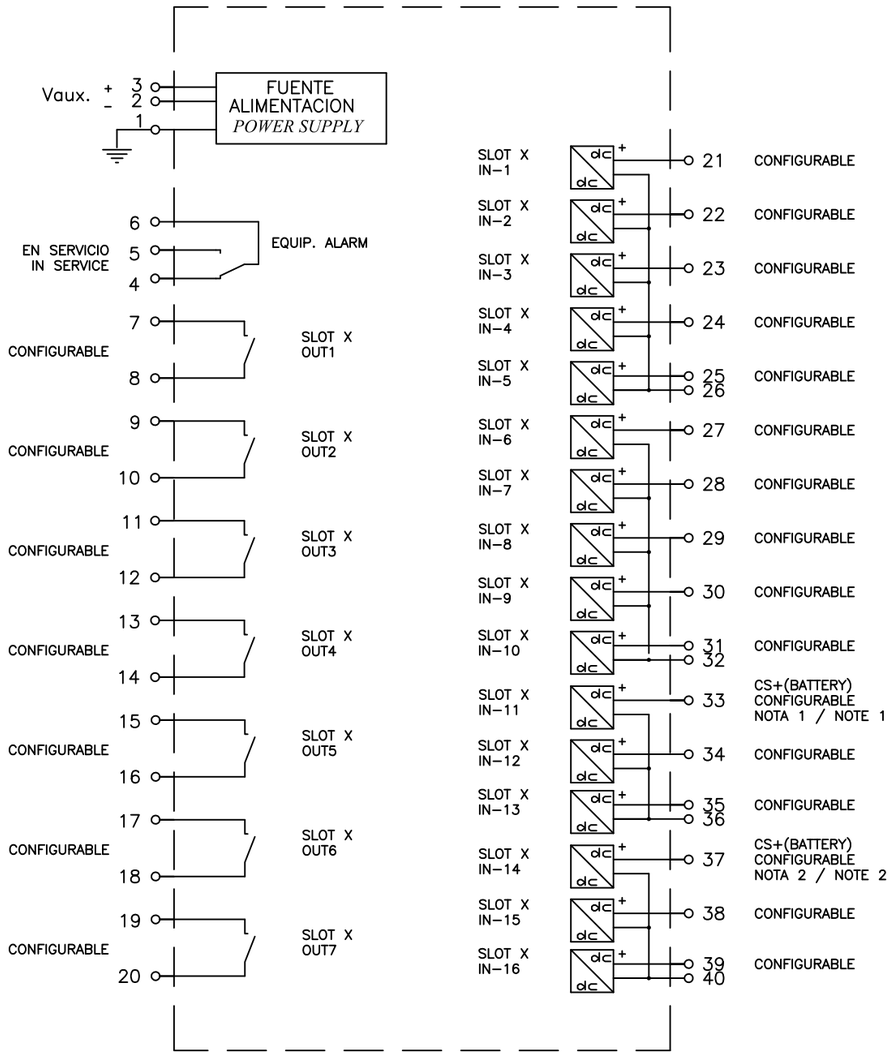
PROYECTO / *PROJECT:* IRF#-###############XYZW

Rev.0

NUM.: 3RX0206/0001

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	17/03/17	J.M.S.
Aprobado / *Approved*	17/03/17	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: –
Continued on sheet:



RACK	1/3			
SLOT	A	B	C	
	X			
MODEL I#F#-###	2	#	#	####
	4	#	#	####

RACK	1/2					
SLOT	A	B	C	D	E	
	X					CPU
MODEL I#F#-###	2	#	#	#	#	####
	4	#	#	#	#	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
	X											CPU
MODEL I#F#-###	2	#	#	#	#	#	#	#	#	#	#	####
	4	#	#	#	#	#	#	#	#	#	#	####

NOTA 1: LA BORNA 33 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN12, IN13 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.
NOTA 2: LA BORNA 37 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN15, IN16 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.

NOTE 1: TERMINAL 33 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN12, IN13 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.
NOTE 2: TERMINAL 37 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN15 OR IN16 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD500004568	1		2		3		4	
5		6		7		8		9		10
11		12		13		14		15		16

Z I V Aplicaciones y Tecnologia

TITULO: CONEXIONES FUENTE ALIMENTACION Y E/S DIGITALES
TITLE: EXTERNAL CONNECTIONS POWER SUPPLY &DIGITAL I/O

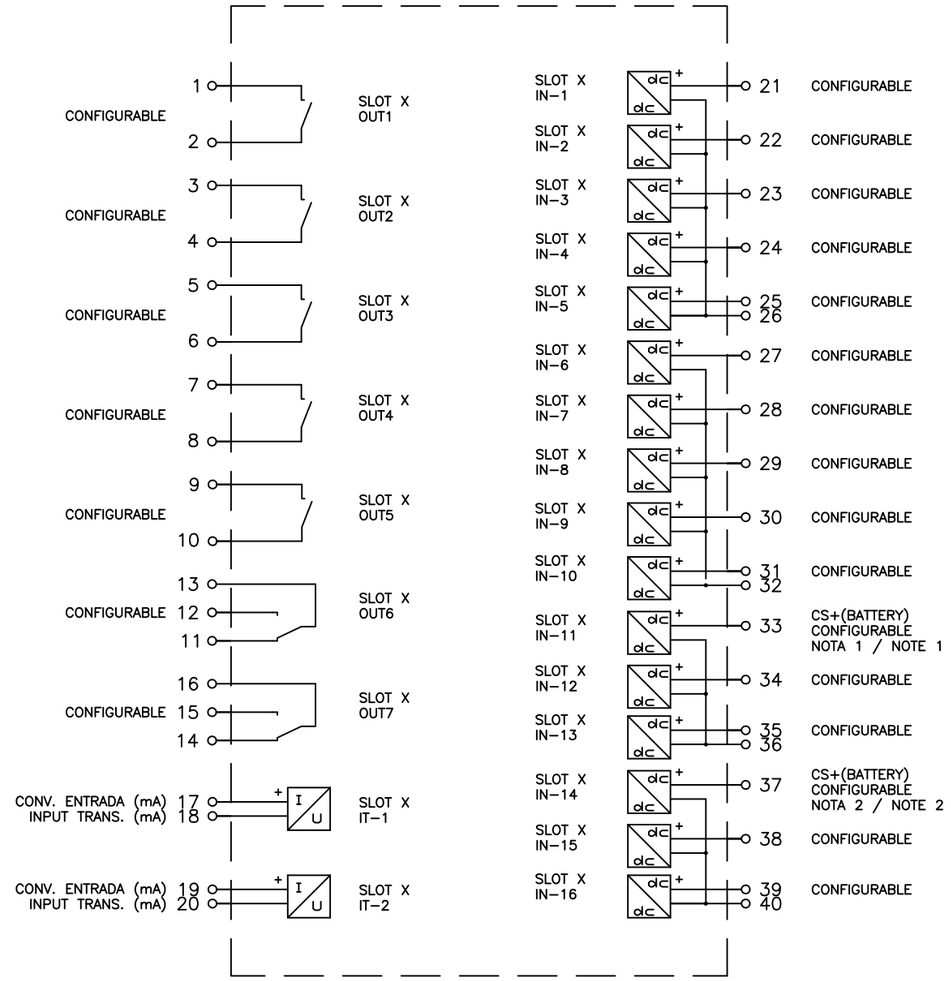
PROYECTO / *PROJECT:* IRF#-###2############## / IRF#-###4##############

Rev.0

NUM.: 3RX0206/0002

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	17/03/17	J.M.S.
Aprobado / *Approved*	17/03/17	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: –
Continued on sheet:



RACK	1/3			
SLOT	A	B	C	
		X	X	
MODEL I#F#-###	#	2	2	####

RACK	1/2					
SLOT	A	B	C	D	E	
		X	X	X	X	
MODEL I#F#-###	#	2	2	2	2	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
		X	X	X	X	X	X	X	X	X	X	
MODEL I#F#-###	#	2	2	2	2	2	2	2	2	2	2	####

NOTA 1: LA BORNA 33 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN12, IN13 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.
NOTA 2: LA BORNA 37 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN15, IN16 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.

NOTE 1: TERMINAL 33 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN12, IN13 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.
NOTE 2: TERMINAL 37 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN15 OR IN16 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD500004568	1		2		3		4	
5		6		7		8		9		10	
11		12		13		14		15		16	

Z I V Aplicaciones y Tecnología

TITULO: CONEXIONES EXTERNAS ENTRADAS/SALIDAS DIGITALES
TITLE: EXTERNAL CONNECTIONS DIGITAL INPUT/OUTPUTS

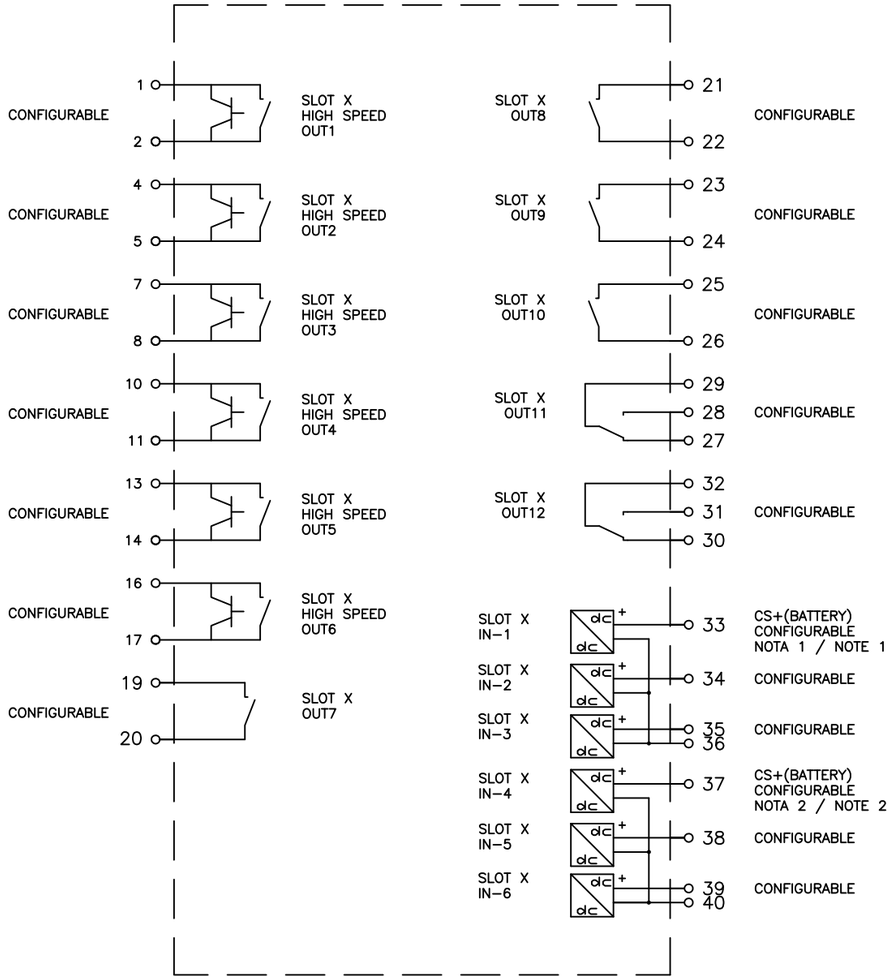
PROYECTO / *PROJECT:* IRF#-####2222222222####

Rev.0

NUM.: 3RX0206/0003

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	17/03/17	J.M.S.
Aprobado / *Approved*	17/03/17	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: – *Continued on sheet:*



RACK	1/3			
SLOT	A	B	C	
		X	X	
MODEL I#F#–###	#	7	7	####

RACK	1/2					
SLOT	A	B	C	D	E	
		X	X	X	X	
MODEL I#F#–###	#	7	7	7	7	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
		X	X	X	X	X	X	X	X	X	X	
MODEL I#F#–###	#	7	7	7	7	7	7	7	7	7	7	####

NOTA 1: LA BORNA 33 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN2, IN3 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.

NOTA 2: LA BORNA 37 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN5, IN6 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.

NOTE 1: TERMINAL 33 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN2, IN3 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.

NOTE 2: TERMINAL 37 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN5 OR IN6 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD500004568	1		2		3		4	
5		6		7		8		9		10	
11		12		13		14		15		16	

Z I V Aplicaciones y Tecnología

TITULO: CONEXIONES EXTERNAS ENTRADAS/SALIDAS DIGITALES
TITLE: EXTERNAL CONNECTIONS DIGITAL INPUT/OUTPUTS

PROYECTO / *PROJECT:* IRF#–####7777777777####

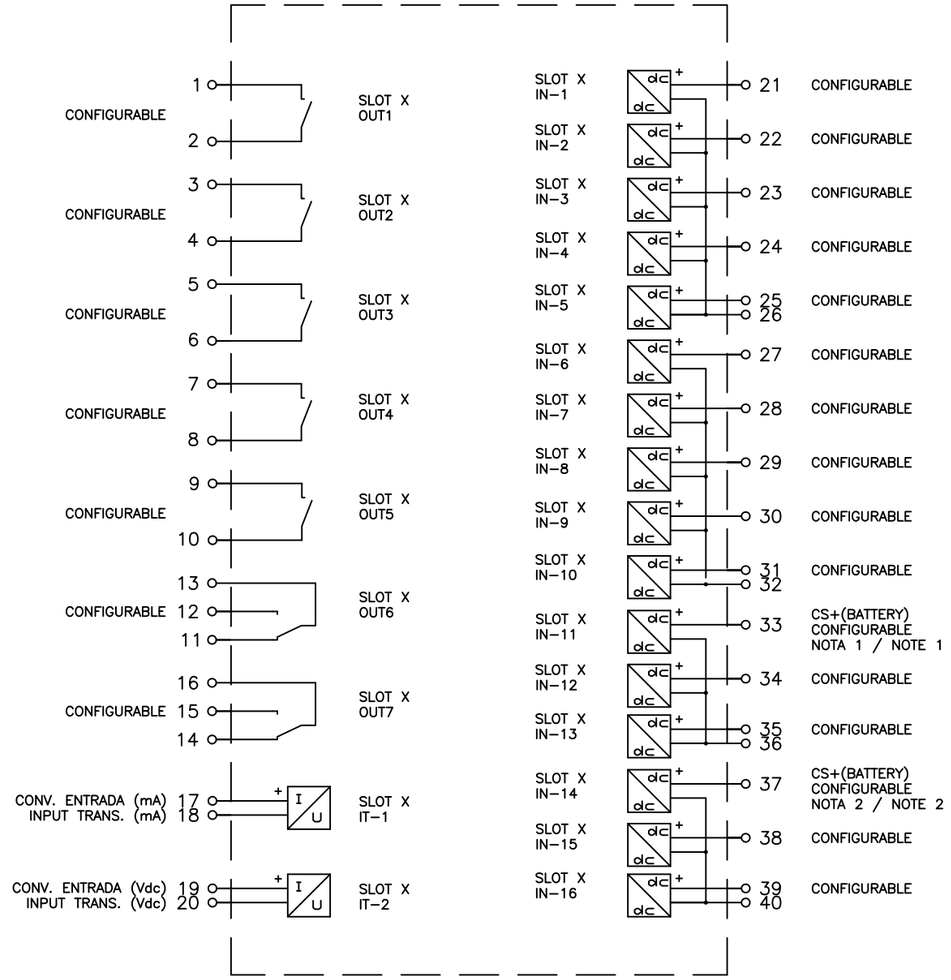
Rev.0

NUM.: 3RX0206/0004

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	17/03/17	J.M.S.
Aprobado / *Approved*	17/03/17	P.A.

Hoja / *Sheet:* 1

Continua en Hoja: – *Continued on sheet:*



RACK	1/3			
SLOT	A	B	C	
		X	X	
MODEL I#F#-###	#	3	3	####

RACK	1/2					
SLOT	A	B	C	D	E	
		X	X	X	X	
MODEL I#F#-###	#	3	3	3	3	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
		X	X	X	X	X	X	X	X	X	X	
MODEL I#F#-###	#	3	3	3	3	3	3	3	3	3	3	####

NOTA 1: LA BORNA 33 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN12, IN13 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.
NOTA 2: LA BORNA 37 DEBERÁ CONECTARSE A POSITIVO SIEMPRE QUE SE USE ALGUNA DE LAS ENTRADAS IN15, IN16 PARA LA FUNCIÓN DE VIGILANCIA DE BOBINAS DE INTERRUPTOR.

NOTE 1: TERMINAL 33 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN12, IN13 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.
NOTE 2: TERMINAL 37 SHOULD BE CONNECTED TO POSITIVE WHEN ANY OF THE INPUTS IN15 OR IN16 ARE BEING USED FOR THE BREAKER COIL SUPERVISION FUNCTION.

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD500004568	1		2		3		4	
5		6		7		8		9		10	
11		12		13		14		15		16	

Z I V Aplicaciones y Tecnología

TITULO: CONEXIONES EXTERNAS ENTRADAS/SALIDAS DIGITALES
TITLE: EXTERNAL CONNECTIONS DIGITAL INPUT/OUTPUTS

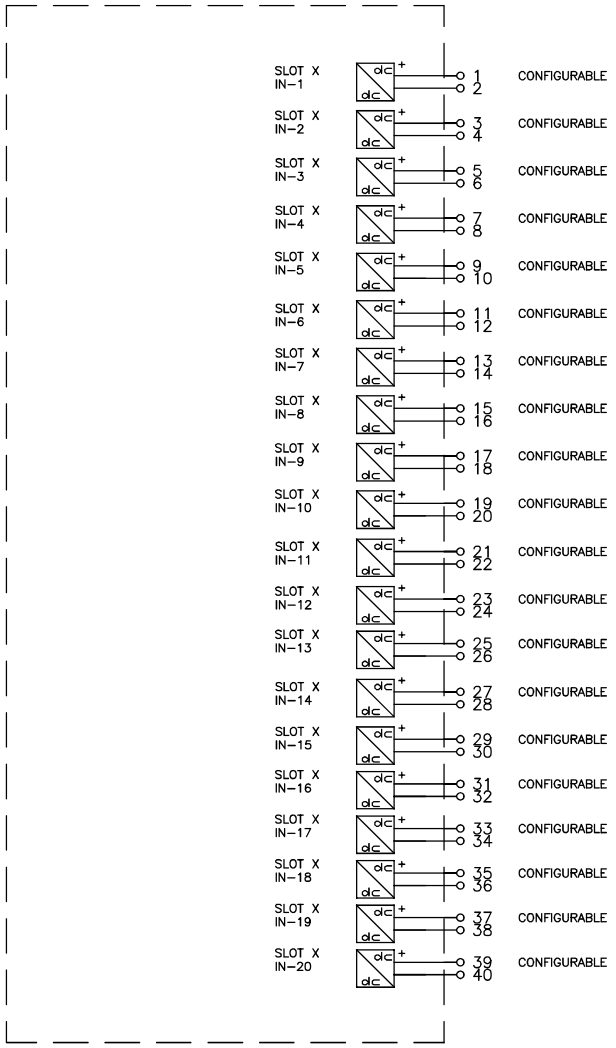
PROYECTO / *PROJECT:* IRF#-####3333333333####

Rev.0

NUM.: 3RX0206/0009

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	12/07/18	J.M.S.
Aprobado / *Approved*	12/07/18	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: – *Continued on sheet:*



RACK	1/3			
SLOT	A	B	C	
		X	X	
MODEL I#F#-###	#	5	5	####

RACK	1/2					
SLOT	A	B	C	D	E	
		X	X	X	X	
MODEL I#F#-###	#	5	5	5	5	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
		X	X	X	X	X	X	X	X	X	X	
MODEL I#F#-###	#	5	5	5	5	5	5	5	5	5	5	####

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnología and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnología.

REV.	0	CD–	1	2	3	4
5		6	7	8	9	10
11		12	13	14	15	16

Z I V Aplicaciones y Tecnología

TITULO: CONEXIONES EXTERNAS ENTRADAS/SALIDAS DIGITALES
TITLE: EXTERNAL CONNECTIONS DIGITAL INPUT/OUTPUTS

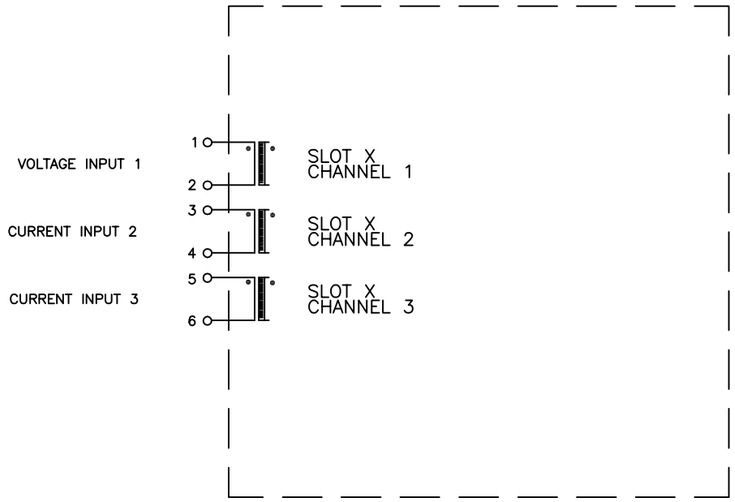
PROYECTO / *PROJECT:* IRF#-####5555555555####

Rev.0

NUM.: 3RX0206/0015

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	06/09/21	J.M.S.
Aprobado / *Approved*	06/09/21	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: –
Continued on sheet:



RACK	1/3			
SLOT	A	B	C	
			X	
MODEL RTF#-###	#	#	I	####

RACK	1/2					
SLOT	A	B	C	D	E	
					X	
MODEL RTF#-###	#	#	#	#	I	####

RACK	1											
SLOT	A	B	C	D	E	F	G	H	I	J	K	
											X	
MODEL RTF#-###	#	#	#	#	#	#	#	#	#	#	I	####

"ATENCION" *"WARNING"*
El contenido del presente documento es propiedad de ZIV Aplicaciones y Tecnología, y no puede ser reproducido ni copiado sin la expresa autorización escrita de ZIV Aplicaciones y Tecnología.
The contents of this document belong to ZIV Aplicaciones y Tecnologia and may not be reproduced or copied without express written authorization from ZIV Aplicaciones y Tecnologia.

REV.	0	CD500004568	1	CD500005026	2		3		4	
5		6		7		8		9		10	
11		12		13		14		15		16	

Z I V Aplicaciones y Tecnologia

TITULO: CONEXIONES EXTERNAS ENTRADAS ANALOGICAS
TITLE: EXTERNAL CONNECTIONS ANALOGUE INPUTS

PROYECTO / *PROJECT:* RTF#

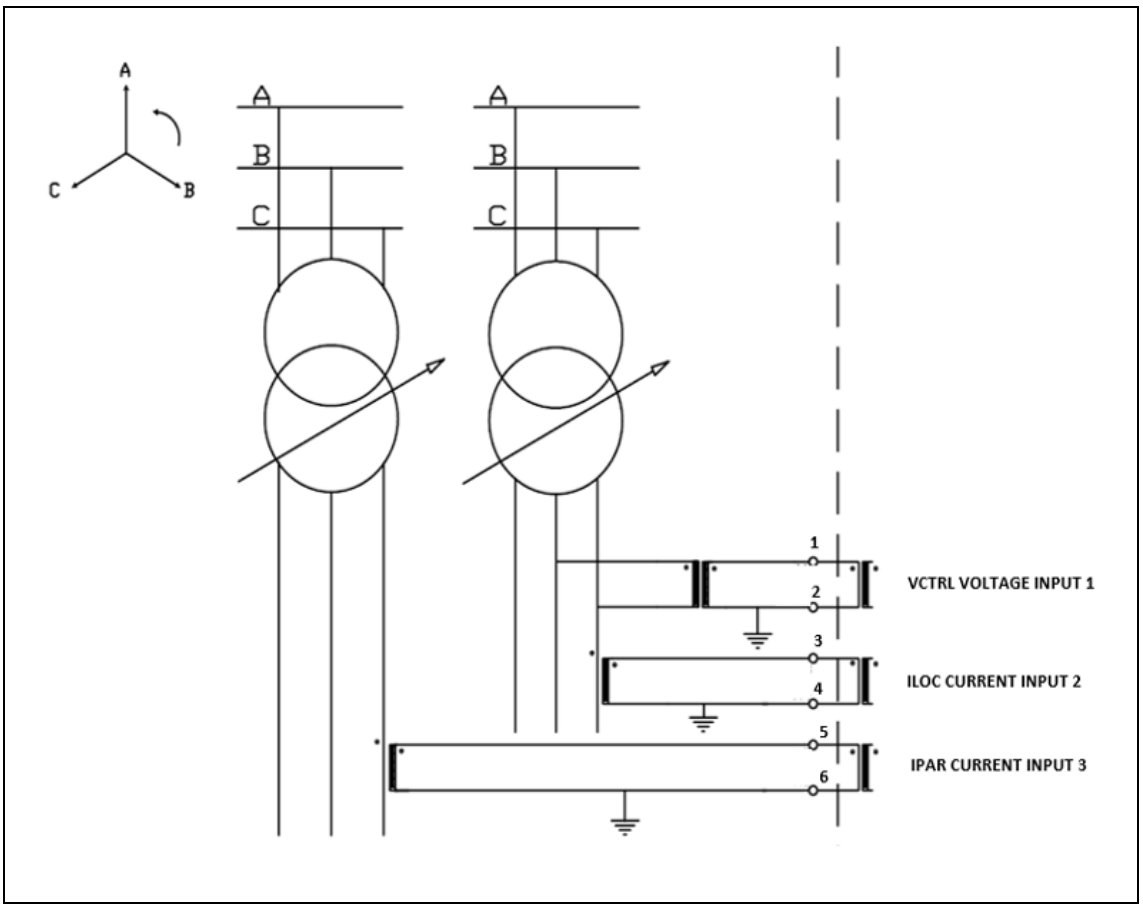
Rev.0
Rev.1 10/09/19

NUM.: 3RX0206/0010

	Fecha / *Date*	Nombre / *Name*
Dibujado / *Drawn*	05/02/19	J.M.S.
Aprobado / *Approved*	05/02/19	P.A.

Hoja / *Sheet:* 1
Continua en Hoja: –
Continued on sheet:

Example: External Connection of Analog Inputs



1.10 Alarm Codes

1.10.1 Introduction 1.10-2
1.10.2 Activation of Signal and Alarm Generation Event 1.10-2
1.10.3 Update of the Alarm Status Magnitude 1.10-2
1.10.4 Indication on the HMI Stand-By Screen 1.10-3
1.10.5 LED Indication and Operating States of the Equipment 1.10-4
1.10.6 General Alarm Counter 1.10-4

1.10.1 Introduction

The occurrence of alarms is notified by following routes:

- Activation of an Alarm Generation Signal and Event.
- Update of the Alarm Status Magnitude.
- Indication on the HMI Stand-by Screen.

1.10.2 Activation of Signal and Alarm Generation Event

The IED has 2 status contact input signals to indicate critical and non-critical level alarms:

- Non-critical system error: **ERR_NONCRIT**
- Critical system error: **ERR_CRIT**

The activation of any of these signals generates its associated event. These signals can be used as inputs to be processed by the user-developed algorithms. Likewise, these signals can be connected to any of the communications protocols for their remote notification.

1.10.3 Update of the Alarm Status Magnitude

The IED has a magnitude whose value is determined by the combination of active alarms in the IED. This magnitude can be used as input to be processed by the user-developed algorithms. Likewise, a user-developed algorithm can connect this magnitude (or the outcome of the processing of the same by the user logic) to any of the communications protocols for transmission.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Following table shows the possible causes of alarm coded by alarm magnitude, together with their level of severity.

Table 1.10-1: Alarm Status Magnitude and Severity Level

Alarm	Value	Severity	Meaning
Alarm in Local Port	0x00000002	NON-CRITICAL	Error while operating with the front USB port.
Protection Out-of-Service Alarm	0x00000004	CRITICAL	Protection error. Protection Out-of-Service.
Error in ADC	0x00000008	CRITICAL	Error in the ADC or in the auxiliary microcontroller that receives and controls the samples.
Digital Inputs / Outputs Alarm	0x00000010	CRITICAL	Problems in the I/O Module.
Error in Flash	0x00000020	CRITICAL	Problems in Flash memory.
Error lack of VCC in circuits	0x00000040	CRITICAL	Internal power failure.
Error IEC 61850	0x00000080	NON-CRITICAL	Problem with data files, CID that accompanies the SW, Unknown relay model, inability to choose a data model or parse error on a previously validated CID.
Error in configuration	0x00000100	NON-CRITICAL	The error occurs if the system cannot be configured with the requested configuration.
Program error	0x00000200	CRITICAL	Unexpected SW problems that prevent its operation.
Remote Port 1 Alarm	0x00000400	NON-CRITICAL	Serial remote port HW error.
Hardware error	0x00000800	CRITICAL	Incorrect HW Configuration. The HW detected by the IED does not correspond to the internal models provided by the SW.
UCONTROLER Alarm	0x00001000	CRITICAL	Error in communication with the auxiliary microcontroller that controls the different boards.
RTC Alarm	0x00002000	NON-CRITICAL	Loss of time or due to no detection of the clock.
Alarm in Transducer Input	0x00004000	CRITICAL	Error in communication with the Transducer Input.

In the case of more than one alarm at once, the sum of the codes of these alarms is seen in hexadecimal form.

1.10.4 Indication on the HMI Stand-By Screen

The activation of the **Critical System Error** signal produces the display of the current magnitude of the status of alarms of the IED in hexadecimal format on the stand-by display of the HMI.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.10.5 LED Indication and Operating States of the Equipment

The LED on the top of the IED together with the label "READY" is not configurable and shows, depending on the color and the blinking, the different operating states of the equipment.

- **Fixed Green**. Equipment in service and under normal operating conditions. As non-critical alarms do not prevent normal operation of the equipment, the equipment will not change this indication.
- **Fixed Red**. Equipment in critical alarm mode:
  - The control logic is still running.
  - PROCOME Protocol only allows control messages.
  - IEC 61850 disables subscriptions and GOOSE messages.
  - The IED continues its measurement tasks, but stops recording historical data.
  - The protection is not operative.
  - Equipment contact indicating out of service.
- **Blinking Red**. Protection setting Out-of-Service.
  - Protection Out-of-Service.
  - Control logic stops working, while maintaining the values it has at that moment, that is, the logic signals do not return to 0 when it is put out of service, freezing the values until they are recalculated when the equipment is put in service again.
  - Protection continues with measures.
  - The IED keeps communicating, the measurements are updated by communications and only digital signals not related with the logic or with the protection will be updated.
  - Equipment contact indicating out of service.
- **Blinking Green**: equipment *booting up*.
- **Blinking Orange**: equipment recording in flash memory.
- **Fixed Orange**: equipment in Test Mode (future functionality).

1.10.6 General Alarm Counter

The relay is provided with three counters on the HMI to inform on the number of starts, re-starts and Traps:

- **Number of starts** (NARRANQS). Informs on the number of times the relay has been cold restarted (relay power supply failure).
- **Number of restarts** (NREARRAQS). Informs on the number of times the relay has been hot restarted (manually through change in configuration, or change of any nominal setting or relay reset).
- **Number of Traps** (NTRAPS). Number of exceptions produced in the relay followed by a reset.

Warning: contact the manufacturer if the unit displays any of these alarms codes.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.11 Troubleshooting

1.11.1 Introduction 1.11-2
1.11.2 Software with Self-Checking 1.11-2
1.11.3 Power Up 1.11-2
1.11.4 In Service / Alarm Contact 1.11-3
1.11.5 Error Messages during Power Up 1.11-3
1.11.6 Error Messages when the Relay is in Normal Operation 1.11-4
1.11.7 Errors while Communicating 1.11-5
1.11.8 Error in Digital Inputs 1.11-7
1.11.9 Error in Digital Outputs 1.11-7
1.11.11 Error in Transducer Inputs 1.11-8
1.11.11 Error in Measurements 1.11-8
1.11.12 Fatal Errors 1.11-8

1.11.1 Introduction

The purpose of this Chapter is to allow identifying error conditions in the device so that the user can carry out the appropriate corrective action in each case.

1.11.2 Software with Self-Checking

The relay performs continuous monitoring and self-checking its hardware and software. If any problem is detected, the device will show an alarm message in the HMI as it is explained in the Chapter 1.9.1, Alarm Codes.

The alarms generated by the self-checking module are divided in two levels, critical and non-critical alarms (table located in Chapter 1.9.1, Alarm Codes). When there is a non-critical alarm, the corresponding alarm message is displayed in the HMI and the device keeps on working due to the fact that the error level detected does not prevent the basic protection functionality, while when there is a critical alarm along with the error message in the HMI the alarm or watchdog contact of the relay changes its position because the protection goes out of service.

1.11.3 Power Up

If the relay does not appear to power up, verify the following points in order to determine if the error is located in the external wiring, in the power supply module or in the display.

Table 1.11-1: Power Up

Test	Check	Actions
1	Measure the auxiliary voltage on terminals of the relay, verifying that the voltage level and polarity is the one defined on the front label. Verify the positive and negative terminal in the external connection drawing.	If the auxiliary voltage is correct, proceed to test 2. If the auxiliary voltage is not the expected one, verify the wiring, fuses and/or minicircuit breakers should be checked.
2	Verify the alarm/watchdog contact of the relay. Check terminals in the external connections scheme of the equipment.	In the device is in service status (contact), the “READY” LED on green and the display is backlit but nothing is displayed, contact your supplier and the ZIV Quality Department. If the device is out of service, contact your supplier and the Quality Department of ZIV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.11.4 In Service / Alarm Contact

Table 1.11-2: In Service / Alarm Contact		
Test	**Check**	**Actions**
1	Access through the HMI or with the communication program to the setting called as “Unit In Service” which is inside General. If it is enabled proceed to test 2.	If the setting is disabled, enable it and verify that the alarm/watchdog contact switched from alarm status to in service status. If it does not change, proceed to test 2.
2	Check if there is any alarm message in the HMI and verify if it is a critical alarm taking into account the table located in the Chapter 1.9, Alarm Codes.	Contact your supplier and the Quality Department of ZIV.

1.11.5 Error Messages during Power Up

If the device, once the power up process has finished, is not showing the default screen (model, date and time) verify the following points.

- **IEC61850 Devices**

Table 1.11-3: Error Messages during Power Up - IEC61850 Devices		
Test	**Check**	**Actions**
1	IEC61850 power up stops showing the following message: ----------.CID	Protection is operating but communications cannot run because the device has no CID file. Load a correct CID file to the relay with correct XML format and IP address equal to that of the equipment in question.
2	IEC61850 power up stops showing the 3010 error	Protection is operating but communications cannot run because there is a problem while loading the IEC61850 profile. Contact your supplier and the Quality Department of ZIV.
3	IEC61850 power up stops showing the 3011 error	Protection is operating but communications cannot run because there is a problem while loading the CID file. Verify in the logs (web server or FTP) the error reason, modify the CID file and load the corrected file.
4	IEC61850 power up stops showing the 3020 error	Protection is operating but communications cannot run because the FW version of the protection and the IEC61850 FW are not matching. Contact your supplier and the Quality Department of ZIV.
5	IEC61850 power up stops showing the 3030 error	Protection is operating but communications cannot run because there is a mistake in the external control logic configuration of the CID (InRefs, LOGGAPC). Verify in the logs (web server or FTP) the error reason, modify the CID file and load the corrected file.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.11-3: Error Messages during Power Up - IEC61850 Devices		
Test	**Check**	**Actions**
6	IEC61850 power up stops showing the 3060 error	Protection is operating but communications cannot run because there is a mistake in the GOOSE subscription configuration. Verify in the logs (web server or FTP) the error reason, modify the CID file and load the corrected file.
7	IEC61850 power up stops showing the 3070 error	Protection is operating but communications cannot run because there is an error in the internal file that manages the Ethernet connection. Contact your supplier and the Quality Department of ZIV.
8	IEC61850 power up stops showing the 3080 error	Protection is operating but communications cannot run because there is a problem in the interfaces. Contact your supplier and the Quality Department of ZIV.
9	IEC61850 power up stops showing the 3200 error	Protection is operating but communications cannot run because there is a problem with the interruptions of the DPRAM. Contact your supplier and the Quality Department of ZIV.
10	If there is a generic non IEC61850 error message in the HMI, check which kind of error it is according to the table that appears in Chapter 1.9, Alarm Codes.	Contact your supplier and the Quality Department of ZIV.

- **Non IEC61850 Devices**

Table 1.11-4: Error Messages during Power Up - IEC61850 Devices		
Test	**Check**	**Actions**
1	If there is an error message in the HMI, check which kind of error it is according to the table that appears in Chapter 1.9, Alarm Codes.	Contact your supplier and the Quality Department of ZIV.

1.11.6 Error Messages when the Relay is in Normal Operation

Table 1.11-5:Error Messages when the Relay is in Normal Operation		
Test	**Check**	**Actions**
1	If there is an error message in the HMI, check which kind of error it is according to the table that appears in Chapter 1.9, Alarm Codes.	Contact your supplier and the Quality Department of ZIV. Take into account that, with non-critical errors, control and protection are still operational.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.11.7 Errors while Communicating

Table 1.11-6: Errors while Communicating

Test	Check	Actions
1	If a communication error takes place when trying to communicate with *ZIV e-NET tool*® program through the frontal port with the following message: Doesn't communicate. Cannot get identifier.	Verify: - That you are using a crossed cable (5-5, 2-3). - That you are using a suitable USB cable and you have all the drivers installed. - That the communication parameters of the device and the ones set in the communications program fit. Click two times in the screen of *ZIV e-NET tool*® and scan the PC port used for the connection with the relay to obtain automatically the suitable parameters. To verify the COM port associated with the USB port and to use it as a parameter for the communication, move the mouse on *Help / About ...* with the Shift + Ctrl + Alt keys pressed and the corresponding port appears in the upper right corner. If even with those parameters the message is still appearing, contact your supplier and the Quality Department of ZIV.
2	If a communication error takes place when trying to communicate with *ZIV e-NET tool*® program through the frontal port with the following message: *Cannot locate the identifier corresponding profile: XXXX*.	Close *ZIV e-NET tool*® program, update the database and run again *ZIV e-NET tool*® in order to communicate with the relay.
3	If a communication error takes place when trying to communicate with *ZIV e-NET tool*® program through the serial rear port of the relay.	Verify: - That you are using a crossed cable. - That the communication parameters of the device and the ones set in the communications program fit. - That the protocol of the rear port has been set to PROCOME. Click two times in the screen of *ZIV e-NET tool*® and scan the PC port used for the connection with the relay to obtain automatically the suitable parameters. If even with those parameters the message is still appearing, contact your supplier and the Quality Department of ZIV.
4	If a communication error takes place when trying to communicate with *ZIV e-NET tool*® program through the LAN port of the relay.	Verify: - The IP address of the relay is the same one set in *ZIV e-NET tool*®. - That the TCP port set in *ZIV e-NET tool*® is 32001. - That the network parameter selected is the transparent. - That the IP address of the PC belongs to the same family address of the one set in the relay and the network masks are correct. If the error is still appearing, contact your supplier and the Quality Department of ZIV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 1.11-4: Errors while Communicating		
Test	**Check**	**Actions**
5	Errors when communicating in Modbus and DNP3 through the serial remote port.	Verify: - That you are using a crossed cable. - That the communication parameters of the device and the ones set in the communications program fit. - That the rear port in the relay has been set with the appropriate protocol (DNP3). - That the control configuration of the relay has the addresses requested by the master. If you cannot communicate, verify the correct behavior of the port trying to communicate in PROCOME with *ZIV e-NET tool*®. If it works, check again the initial points. If it does not work, contact your supplier and the Quality Department of ZIV.
6	Errors when communicating in Modbus RTU and DNP3 through the LAN port.	Verify: - The IP address of the relay is the same one set in the master. - That the TCP/IP port fits. - That the instance is adjusted with the appropriate protocol. - That the control configuration of the relay has the addresses requested by the master. - That the IP address of the PC/master belongs to the same IP family address of the one set in the relay and the network masks are correct. If you cannot communicate, verify the correct behavior of the port trying to communicate in PROCOME with *ZIV e-NET tool*®. If it works, check again the initial points. If it does not work, contact your supplier and the Quality Department of ZIV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.11.8 Error in Digital Inputs

Table 1.11-7:Error in Digital Inputs		
Test	**Check**	**Actions**
1	Verify that the DI is energized (positive and negative as external connection wiring diagram) checking the voltage level and polarity taking into account the indications of the front label (Name Plate) of the relay.	If the voltage supply of the DI is correct (positive and negative) skip to step 2. If the auxiliary voltage is not the expected one, check the external wiring, fuses and/or mini circuit breakers of the circuit.
2	If you are using a DI that can be configured for coil supervision, check that the corresponding setting has been set to NO.	Access through HMI or *ZIV e-NET tool*® to the coil supervision settings and disable them. If they were enabled go to step 3.
3	Check the activation/deactivation voltage levels as the table that appears in Digital Inputs inside Chapter 1.3, Technical Data.	If the voltage is located inside the activation margin and the DI is not activating, verify that the FW of the relay matches with the model of the front label (Name Plate) of the relay. In any case contact your supplier and the Quality Department of ZIV. If the FW does not match, contact your supplier and the ZIV Quality Department.

1.11.9 Error in Digital Outputs

Table 1.11-8:Error in Digital Outputs		
Test	**Check**	**Actions**
1	If the auxiliary contacts are not operating.	Verify the signals that activate the outputs and used in the protection settings for this purpose. If they are correct, make the necessary actions in order to execute the protection or the control logic and give the closing command. Verify if the output is changing the status in the HMI and in the events of the relay. If any of the outputs are not operating contact your supplier or the Quality Department of ZIV. If you are seeing the DO changing in the HMI, verify the activation of the output contact a multimeter, taking into account the external connection wiring diagram. If the physical output is not activating, contact your supplier and the Quality Department of ZIV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.11.10 Error in Transducer Inputs

Table 1.11-9: Error in Transducer Inputs		
Test	**Check**	**Actions**
1	Verify that the input transducer has a suitable input signal taking into account the type of input transducer of the relay (see Model Selection table).	If the input signal is not the expected one, check the external wiring, intermediate devices, etc. If the input signal is the correct one, contact your supplier and the Quality Department of ZIV.

1.11.11 Error in Measurements

- Compare the measurements shown in the HMI of the relay with the magnitudes metered with a multimeter in the terminals of the relay.
- Check that the transformation ratios of the CTs and VTs are the correct ones.
- Check that the terminals wired in the relay are the correct ones.
- Check the angle shift in order to confirm that the inputs are correctly wired.

If all the verifications are correct (external wiring, polarity and measurements in terminals of the relay), contact your supplier and the Quality Department of ZIV because it could be a problem of the equipment HW.

1.11.12 Fatal Errors

The device can reset itself in order to escape from transient anomalies, whose cause could be internal or external to the relay and which do not imply a damage of the relay itself. When there is an evidence of a malfunctionality of the device and/or a spontaneous reset, access through the HMI to the FW information screen (ENT / Information / Relay Information / Software/) and check if it is appearing a Trap indication with the date on which the fault occurred. If so, collect the available information of the relay (events, logs, fault reports, disturbance recorder files, etc.), connect by FTP to the computer with user *coredump* and password *coredump*, download all the information present in the accessed folder and contact your supplier and the Quality Department of ZIV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Chapter 2.

Regulation Automatism

2.1 Voltage Regulator

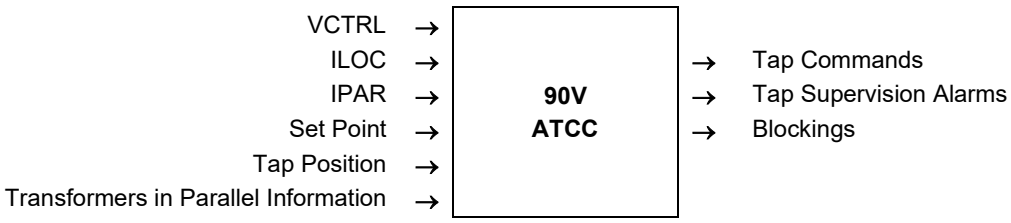
2.1.1 Identification 2.1-3
2.1.2 General Block 2.1-3
2.1.3 Regulator Configuration 2.1-3
2.1.3.a Magnitude Display on Default Screen 2.1-3
2.1.3.b Type of Voltage and Current Wired 2.1-3
2.1.3.c Operation Output Types 2.1-4
2.1.3.d Tap Control and Tap Change Operation Monitoring 2.1-4
2.1.3.e Voltage Set-point and Insensitivity Degree 2.1-4
2.1.4 Regulation Variable 2.1-7
2.1.5 Delay Times 2.1-8
2.1.5.a Delay Time for the First Control Operation: T1 ..... 2.1-8
2.1.5.b Delay Time for Following Control Operations: T2 ..... 2.1-9
2.1.5.c Cancel Timer T_1 ..... 2.1-9
2.1.6 Line Drop Compensation (LDC) 2.1-10
2.1.6.a Line Drop Compensation: LDC-Z 2.1-11
2.1.6.b Line Drop Compensation: LDC-R&X 2.1-12
2.1.7 Voltage Regulation of Parallel Transformers 2.1-13
2.1.7.a Reactive Compensation 2.1-14
2.1.7.b Calculation of the Reactive Current Flowing through two Transformers in Parallel with Current Wiring 2.1-15
2.1.7.c Calculation of Circulating Reactive Current by Communications (Maximum of 5 Transformers in Parallel) 2.1-16
2.1.7.d Calculation of the Reactive Compensation Setting 2.1-16
2.1.7.e Calculation of the Compensation by Circulating Current 2.1-17
2.1.7.f Example 2.1-17
2.1.8 Combined Compensation and Maximum Compensation 2.1-18
2.1.9 Automatic / Manual Regulation Mode 2.1-19
2.1.10 Manual Commands 2.1-19
2.1.11 Tap Control 2.1-20
2.1.11.a Tap Coding 2.1-20
2.1.11.b Number of Taps, Minimum Tap, Upper Limit and Lower Limit 2.1-21
2.1.11.c Tap Indication 2.1-21
2.1.11.d Tap Monitoring 2.1-22
2.1.11.e Tap Change Operation Monitoring 2.1-23
2.1.11.f Tap Change Operation Counters 2.1-23

2.1.12 Blockings 2.1-24
2.1.13 Power Flow Reversal 2.1-28
2.1.14 Voltage Band Recording 2.1-29
2.1.15 Display Information 2.1-30
2.1.16 Settings Recommendation 2.1-31
2.1.17 Settings Calculation Example 2.1-33
2.1.18 Setting Ranges 2.1-36
2.1.19 Analog Inputs to the Unit 2.1-39
2.1.20 Digital Inputs of the Voltage Regulator 2.1-39
2.1.21 Auxiliary Outputs and Events of the Voltage Regulator 2.1-41
2.1.22 IEC 61850 Logical Node 2.1-42
2.1.23 ATCC IEC 61850 Control Commands 2.1-45
2.1.24 Voltage Regulator Test 2.1-46

2.1.1 Identification

Description of the protection unit	IEC 61850 Node	IEC 60617	ANSI/IEEE C37.2
Voltage Automatic Regulator	ATCC	COLTC	90V

2.1.2 General Block



2.1.3 Regulator Configuration

2.1.3.a Magnitude Display on Default Screen

This setting refers only to the units in which the magnitudes will be displayed on the regulator **Default Screen**. Said magnitudes may be displayed in percentage with respect to the nominal voltage of the equipment, in primary voltage values or in secondary voltage values.

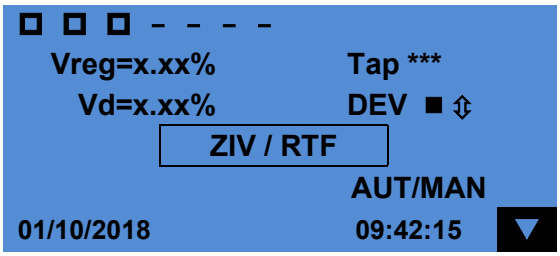


Figure 2.1.1 Alphanumeric Display.

2.1.3.b Type of Voltage and Current Wired

Due to the fact that the user can wire any kind of voltage phase to phase (VAB, VBC, VCA), phase to ground (VA, VB, VC) and any phase current (A, B or C), the IED provides three settings, one setting per input analogue channel, so that the IED will automatically calculate the phase shift due to the connection of the VT and CT to the relay.

So, there Will be one setting to indicate the type of wired voltage and two settings to indicate the type of current wired (local and parallel currents).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.3.c Operation Output Types

Operation outputs (Raise the Tap / Lower the Tap) can be configured for the following activation types:

- **Pulse**, of adjustable duration, between 100 and 5000 msec. (see setting ***Output Pulse Duration***).
- **Level** (only if **Tap Changer Monitoring** is enabled). The output resets when the target tap is reached or after Operation Fail Time times out.

Note: There exists a settings ratio check function to make sure that if the Tap Changer Supervision is disabled,

2.1.3.d Tap Control and Tap Change Operation Monitoring

Settings related to the Tap Control and explained in said section.

2.1.3.e Voltage Set-point and Insensitivity Degree

The purpose of the **RTF** is maintaining the regulation voltage at a given $\mathbf{V_D}$ (desired voltage) set-point value. To this end it is necessary to know the value of the control variable and define the operation through the following settings:

- ***Voltage Origin***: V_{CTRL} or External.
- ***Voltage Set-point***: V_D.
- ***Insensitivity Degree***: GI.
- ***Delay Time***: T.

Both $\mathbf{V_D}$ and **GI** are expressed in % of $\mathbf{V_{nominal}}$. The **Deviation** (**DV**) is calculated at any time as:

$$\mathbf{DV}\ (\%) = \mathbf{V_D}\ (\%) - \mathbf{V_{REG}}\ (\%)$$

Where $\mathbf{V_{REG}}$ is the voltage that the relay will regulate. This $\mathbf{V_{REG}}$ can be the busbar voltage wired to the device (voltage measured through the voltage analogue input) or any other variable or magnitude of the relay, calculated in the control logic or received by communications which will be linked by means of the control logic to an internal variable called EXTERNAL V.

Thus, the **GI** defines the bandwidth or dead band, within which the voltage is deemed acceptable, in view of the discontinuous and finite nature of the voltage transients. An adequate **GI** setting is normally considered equal to the voltage surge related to tap switching. These concepts are clarified in the figure below.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

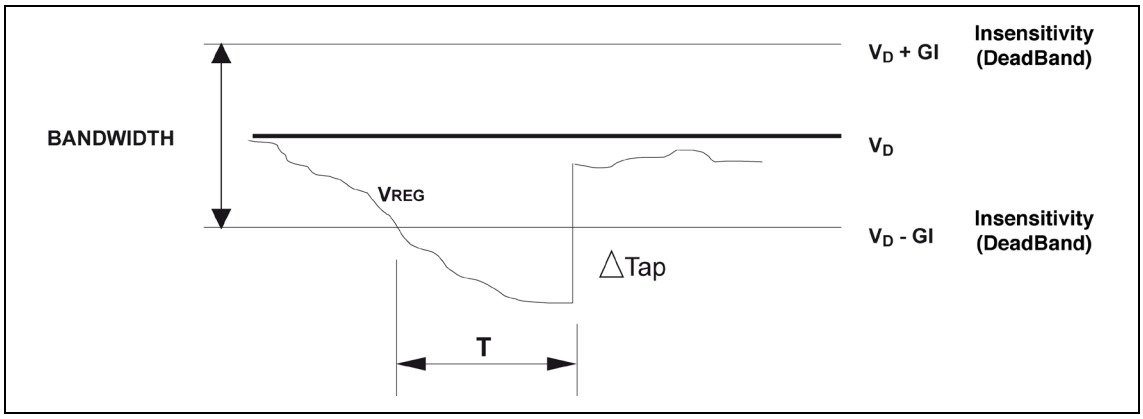


Figure 2.1.2 Insensitivity Degree.

Insensitivity (DeadBand) ≥ 0.6 ∗ tap-change increment [%]

Additionally, it can be mentioned that the dead band (not the GI) can be also defined using the following formula:

Bandwidth ≥ 1.2 ∗ tap-change increment [%] = 2 ∗ Insensitivity (GI)

If the value of the Dead Band would be smaller than the tap-change increment of the transformer, the controlled system can never reach a stable condition as the voltage exceeds the bandwidth selected. If, on the other hand, a very large bandwidth is selected there will be a major control deviation and therefore the control and precision will be less.

A **Delay Time T** is introduced so as to prevent an excessive number of control operations upon short duration $\mathbf{V_{REG}}$ voltage surges outside the dead band. Said delay can be set separately for the first control operation ($\mathbf{T_1}$) and later operations ($\mathbf{T_2}$), in case several operations are required to bring the voltage within the dead band. For more information, refer to section 2.1.3 Delay Times.

The sign of the deviation **DV** defines the type of command (Raise the Tap / Lower the Tap) to be sent to the **tap changer**.

- For a **Direct Tap / Voltage Ratio** (raise the tap is equivalent to raise the voltage):
  - If **|DV| < GI** → At rest (no action).
  - If **|DV| > GI** and $\mathbf{V_D}$ (%) > $\mathbf{V_{BUS}}$ (%)→ Raise the Tap.
  - If **|DV| > GI** and $\mathbf{V_D}$ (%) < $\mathbf{V_{BUS}}$ (%)→ Lower the Tap.
- For an **Indirect Tap / Voltage Ratio** (raise the tap is equivalent to lower the voltage):
  - If **|DV| < GI** → At rest (no action).
  - If **|DV| > GI** and $\mathbf{V_D}$ (%) > $\mathbf{V_{BUS}}$ (%)→ Lower the Tap.
  - If **|DV| > GI** and $\mathbf{V_D}$ (%) < $\mathbf{V_{BUS}}$ (%)→ Raise the Tap.

Raise the Tap or Lower the Tap commands are sent in accordance with a **Time Characteristic** that takes into account the voltage deviation **|DV|** absolute value and the settings of ***Insensitivity Degree*** **(GI)** and ***Time Factor*** **(FT)**:

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

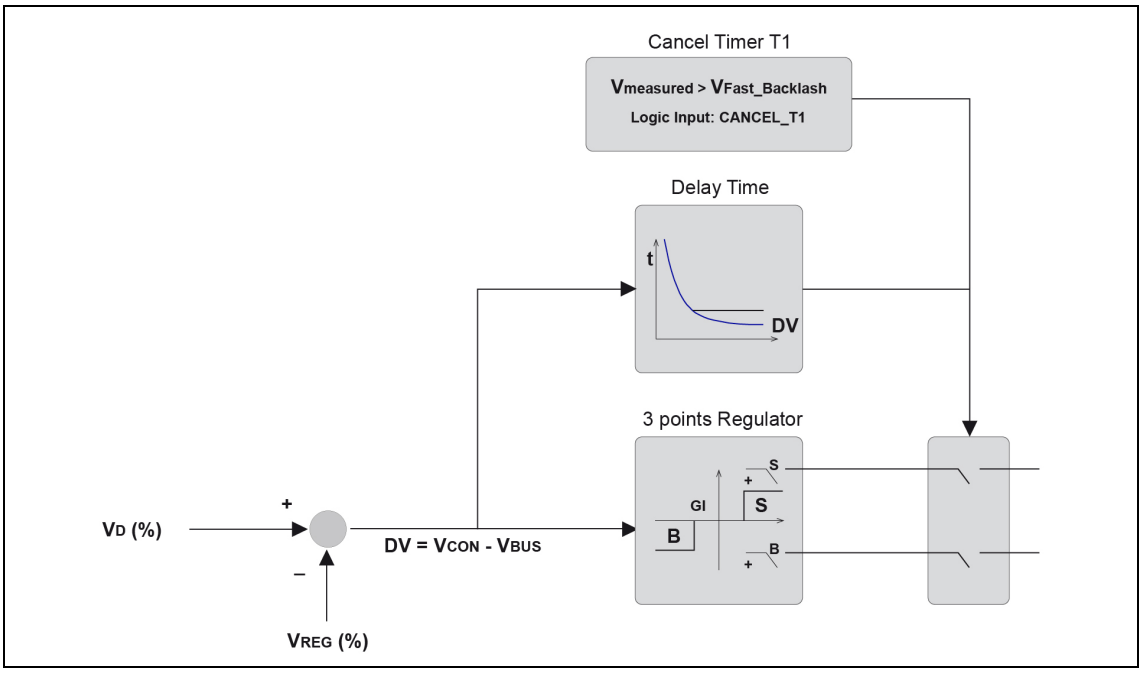


Figure 2.1.3 Schematic Representation of Raise / Lower the Tap.

The relay includes 1 setpoint setting and 5 values that can loaded to the setpoint so that a quick setpoint setting change can be done without changing the setting group. The setpoint setting can be changed in four different ways:

- Using the setting ***Setpoint***.
- Giving a digital setpoint up/down command. The percentage that the setpoint will change in each step is configurable (1 to 6%).
- Giving an analogue setpoint command so that in the command itself it is indicated exactly the setpoint value you want to use in voltage primary values.
- Using control logic input signals (**Setpoint activation command 1, Setpoint activation command 2**, etc.) that can be activated through digital inputs, signals calculated in the control logic, commands, signals received through communications, etc. or using the corresponding integer activation command (where you set the value you want to use from 1 to 5). It could also be used the IEC 61850 command in which by means of an integer value you can define the corresponding setpoint value you want to activate. The setpoint will be activated when one of the corresponding signals activates, taking into account internally just the rising edge of that signal to generate the change so that if the signal remains in active status and a second signal is activated, the setpoint will change to this second signal. If after the activation of any signal all of them go to deactivate status, the IED will keep on working with the last setpoint which was activated

When the setpoint, due to any of the indicated ways to be changed, reaches to one of its extreme values, the signal **Extreme Setpoint** activates.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.4 Regulation Variable

The $\mathbf{V_{REG}}$ variable which is displayed in the HMI of the device shows the voltage measurement that the device will regulate. This voltage that is going to be regulated can be the busbar voltage wired to the device (voltage measured through the voltage analogue input) or any other variable or magnitude of the relay, calculated in the control logic or received by communications which will be linked by means of the control logic to an internal variable called EXTERNAL V.

The user can define which is the voltage the IED will regulate inside the automatism using the Voltage Source setting (voltage measured or external measurement):

- V_{CTRL}: The variable the IED will regulate would be the voltage measured. The angle reference for all the measurements will be this voltage, this is, the voltage analogue input. There are no limitations regarding the compensations that can be enabled and therefore the compensations that can be applied during the regulation.
- External: Once the user defines as External the Voltage Source setting, the IED will use the variable linked in the control configuration to the **EXTERNAL V** measurement as the measurement to regulate. In this case the angles will take the local current as reference measurement, therefore the angle of **ILOC** will take a value of 0º. **LDC R-X** compensation method and circulating current method cannot be enabled.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.5 Delay Times

2.1.5.a Delay Time for the First Control Operation: T1

A **Delay time for the first control operation: T1** is implemented so as to prevent an excessive number of operations upon short duration voltage surges outside the dead band. The settings involved are:

- ***Curve type***: Inverse or Definite Time Curve.
- ***Time Factor***: From 1 to 10 sec.
- ***Definite Time T1*** ($T_{definite1}$): From 1 to 600 sec.

Where:

GI: Insensitivity Degree Setting Value (in %).
|DV|: Voltage Deviation absolute value (in %).

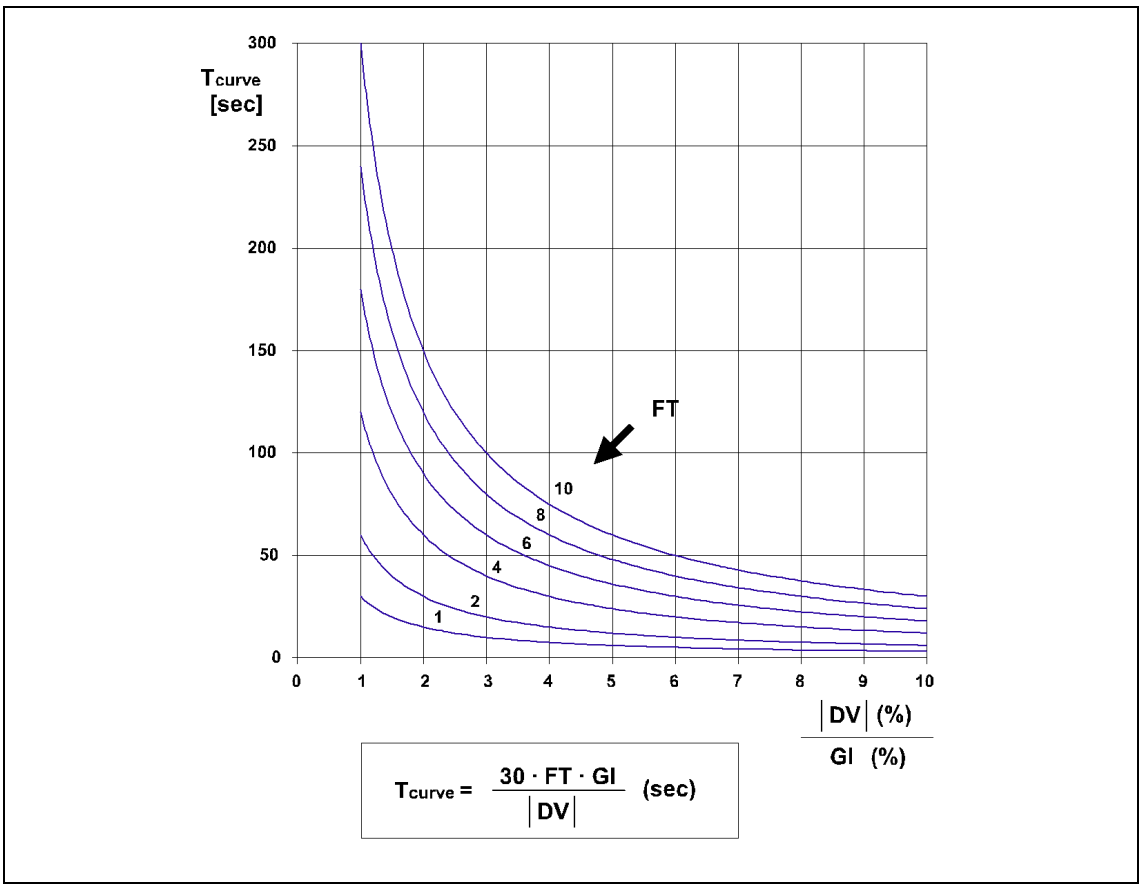


Figure 2.1.4 Time Curve for the First Control Operation: T1.

If **Inverse Curve** is selected, if T_{curve} values obtained from the equation in the above figure are below $T_{definite1}$, $T_{definite1}$ is used. Refer to the summary table in the next page.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.5.b Delay Time for Following Control Operations: T2

Should more than one tap change be required to bring the V_{BUS} voltage back within the dead band **($V_D \pm$ GI)**, the second and following operations will take place after the **Definite Time T_2**.

This is because after the first tap change, if an **inverse curve** is used, taking into account that the delay is inversely proportional to the deviation **|DV|**, the next tap change commands can be delayed too much (time delay greater than **T_1**).

T_2 time will start when the previous command is finished, this is, once the output configured to give the tap up/down command resets. So, when configuring the **RTF** in ***Pulse*** mode, the configurable pulse time has to be taken into account and, when configuring the **RTF** in ***Continuous*** mode, the moment in which the tap status changes.

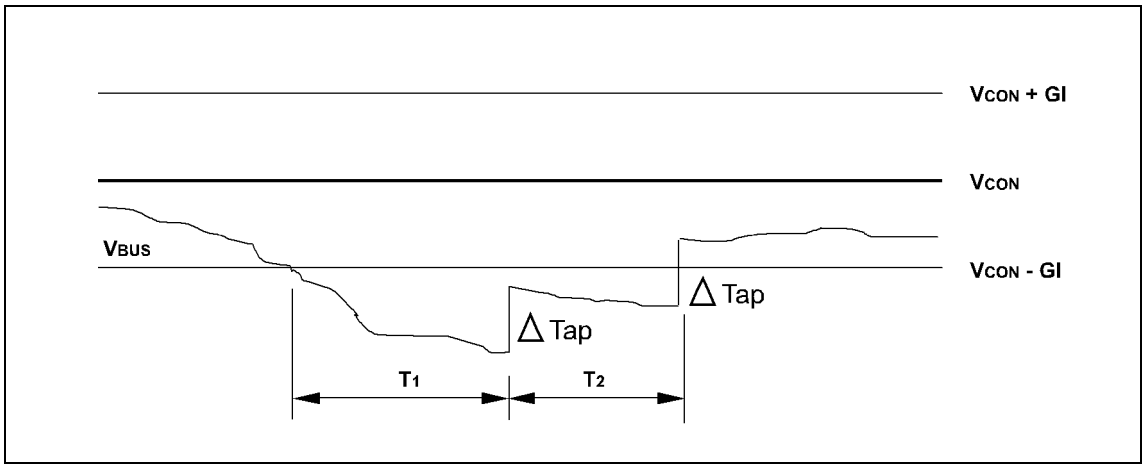


Figure 2.1.5 Delay Time for Following Control Operations: T2

Table 2.1-1: Delay Time Summary Table			
		1º Tap Switching (T_1)	Following Tap Switching
Curve Type	Inverse Curve	$T_{curve} > T_{definite1} \rightarrow T_1 = T_{curve}$	T_2
		$T_{curve} < T_{definite1} \rightarrow T_1 = T_{definite1}$	
	Definite Time	$T_1 = T_{definite1}$	T_2

2.1.5.c Cancel Timer T_1

Timer **T_1** can be cancelled in two ways as represented in the upper part of figure 3.1.4 (Cancel Timer T_1):

- The measured voltage goes above **Runback Voltage** setting.
- Logic input **CANCEL_T1** is activated (Cancel Timer T1).

In both cases, the first tap change command will occur in a maximum time of 0.5 to 1.5 seconds, and the following commands, if required, are sent after **T_2**.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.6 Line Drop Compensation (LDC)

The main purpose of the **RTF** is keeping the busbar voltage $\mathbf{V_{BUS}}$ supplied by the transformer at a given level $\mathbf{V_D}$. The final target is keeping constant the load voltage $\mathbf{V_{LOAD}}$ the voltage drop between the transformer and the load is a function of the current supplied by the transformer, the **RTF** must take into account said current and compensate for the line voltage drop.

Commonly known as **LDC** (Line Drop Compensation), it is also known as **Current Compensation** as it comes to compensate for current flow effects.

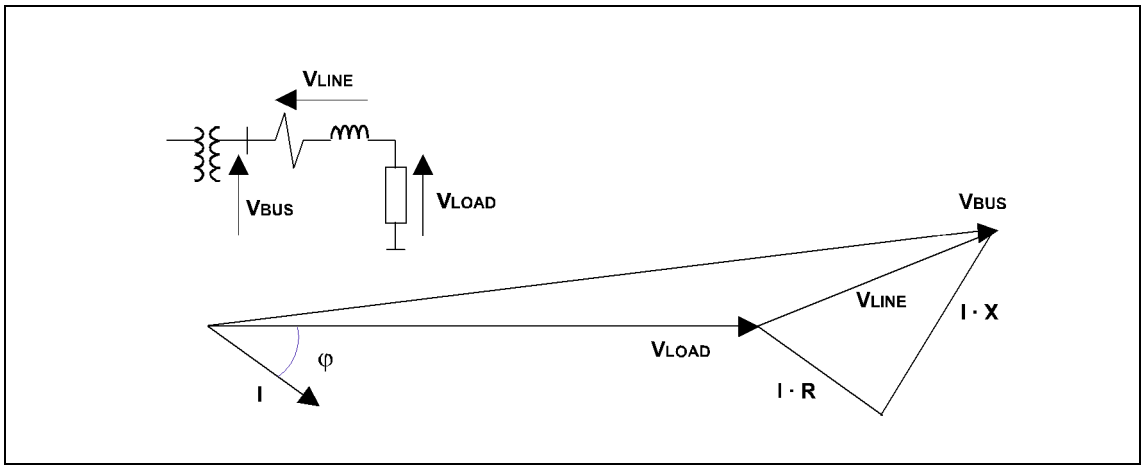


Figure 2.1.6 Line Drop Compensation (LDC).

Two **Line Drop Compensation** (**LDC**) methods are available:

- **LDC-Z**: Magnitude sum compensation, which depends only on the magnitude of the current. This compensation method is adequate when the busbar feeds a number of lines, networks or with small cosφ variation. LDC-Z setting in % (slope ΔU/I) (from 0% to 10%).
- **LDC-R&X**: Vector sum compensation, as it depends on line impedance, current and cosφ. This compensation method is appropriate when the load concentrates at the line end, and line parameters are known. Required settings: LDC-R and LDC-X in Volts (0 to 30 V).

When there is more than one power transformer working in parallel conditions, the current flowing through the cable will be the sum of currents flowing by each transformer bay so in order to take that into account, RTF will multiply the compensation applied by the number of power transformers placed in parallel conditions. RTF will know the number of parallel transformers by the activation of the **EXIST_TRF_PARAL_X** signals.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.6.a Line Drop Compensation: LDC-Z

LDC-Z setting, also known simply as K_C, and expressed in **%** of $V_{nominal}$, represents the line voltage drop when the circulating current is $I_{nominal}$. It is a magnitude sum compensation, i.e. depends only on the magnitude of the current. Said compensation is added to the voltage set-point V_D, resulting into V_{DCOMP}.

$$V_{DCOMP}\ (\%) = V_D\ (\%) + [\ K_C\ (\%) \cdot I_{pu}\ ] * N_{umTrf}$$

Where:

V_{COMP}	Compensated voltage, in % of $V_{nominal}$.
V_D	Set-point voltage, in % of $V_{nominal}$.
K_C	Current compensation or **LDC-Z** setting, in % of $V_{nominal}$.
I_{pu}	Local current per unit, i.e., I_{LOCAL} / $I_{nominal}$
NumTrf	Number of transformers in parallel conditions (automatically calculated taking into account the corresponding transformer in parallel conditions input signals).

For this to have any effect, the following setting values are required:

- Line Drop Compensation (LDC) enable: **YES**
- Line Drop Compensation (LDC) type: **LDC-Z**

Once the **compensated voltage** V_{DCOMP} has been obtained, the **deviation DV** is calculated taking into account the latter value, in place of **set-point voltage** V_D.

$$DV\ (\%) = V_{DCOMP}\ (\%) - V_{BUS}\ (\%)$$

Example:

Kc = 2% → A voltage drop 2% of $V_{nominal}$ is produced when the circulating current is $I_{nominal}$.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.6.b Line Drop Compensation: LDC-R&X

LDC-R and **LDC-X** settings represent the voltage drop (in volts, not in ohms), based on $\mathbf{V_{nominal}}$, when the circulating current is $\mathbf{I_{nominal}}$. For this to have any effect, the line drop compensation must be enabled and the **Line Drop Compensation Type** must be **LDC-R&X**.

It cannot be enabled when the ***Voltage Source*** has been set to **External**.

$$\mathbf{LDC\text{-}R = I_n \cdot (RT_{CT}/RT_{VT}) \cdot r \cdot L \quad (V)}$$

Where,

$$\mathbf{LDC\text{-}X = I_n \cdot (RT_{CT}/RT_{VT}) \cdot x \cdot L \quad (V)}$$

$\mathbf{I_n}$	Rated current (1 or 5 A).
r	Line resistance in Ω/Km per phase.
x	Line reactance in Ω/Km per phase.
L	Line length in Km

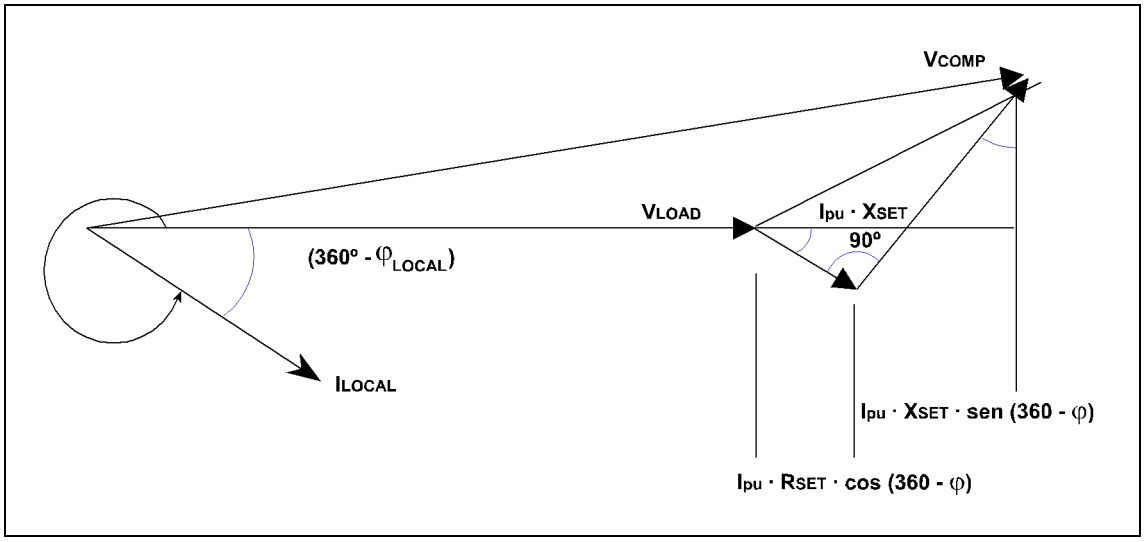


Figure 2.1.7 Line Drop Compensation: LDC-R&X.

$$\mathbf{V_{DCOMP} = V_N + [\ Setting_{LDC\text{-}R} \cdot I_{pu} \cdot Cos\ (360\text{-}\ \Phi_C) + Setting_{LDC\text{-}X} \cdot I_{pu} \cdot Sin\ (360 - \Phi_C)\ ] * N_{umTrf}}$$

Where $\Phi_C = \varphi_{LOC} - \varphi_{phase\ displacement\ TT/TC\ LOC}$

Example:

LDC-R = 6 V ; LDC-X = 0V ; φ=0º ; V_n = 120 V ; I_n = 5 A ; I_{LOCAL} = 2 A
V_{COM} = 120 + (2/5) · 6 = 122.4 V

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.7 Voltage Regulation of Parallel Transformers

Transformers are connected in parallel to increase transformer power when a single transformer cannot supply the load power demand.

Both single phase and three phase transformers can be connected in parallel. In order to operate in parallel, transformer electrical characteristics must comply with a number of conditions.

- Conditions for the **connection of single phase transformers**:
  - Similar transformer ratio (secondary voltage).
  - Connected with correct polarity.
  - Similar impedance.
  - Similar power.
- Conditions for the **connection of three phase transformers**:
  - Similar transformer ratio (secondary phase to phase voltage).
  - Similar phase difference between primary and secondary (compatible vector group and clock hour figure).
  - Similar tap/voltage ratio.
  - Similar impedance.
  - Similar power.

In such cases there are a number of regulation strategies, two of them being highlighted in view of their broad use:

- **Master / Slave**:
  - Rather used method.
  - It is intended to maintain the same tap for all parallel regulators.
  - One master controls the rest.
  - It requires knowing the taps of all LTC (Load Tap Changer).
- **Reactive Circulating Current (Reactive Compensation)**:
  - Most used method.
  - The **Circulating Current** is considered to be reactive and can be calculated from transformer impedances (X_{1T} and X_{2T} in %).
  - This requires the use of a CT to measure the current of the other transformer (parallel) or to receive data from the other transformers through communications.
  - Knowing the taps is not required.
- **Negative reactance:**
  - This could be the least used method.
  - This uses LDC R-X as compensation and regulation method but with negative value of the reactance factor.
  - Communications between equipment not required.
  - Knowledge of the taps not required.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.7.a Reactive Compensation

Even with transformers of same design and construction, there exist small differences between electrical characteristics. When secondary windings are connected in parallel, both are forced to have the same voltage, thus, a reactive power flow could be established between both transformers, which only serves to increase losses and temperature.

The meaning of the reactive power flow is that one transformer is forced to generate more reactive power than the load consumption and is absorbed by the other transformer. The purpose of **reactive compensation** is minimizing tap difference between both transformers, thus reducing the reactive power flow generated.

Reactive compensation can be used:

- Only for transformers complying with the similarity conditions (ideal condition).
- If ***Reactive Compensation Enable*** setting is activated.
- If the device is in parallel condition with others (the IED will calculate it taking into account the number of **EXIST_TRF_PARAL_X** signals which are activated)

The following table shows a diagram of two transformers **T1** and **T2** of different impedances expressed in % working in parallel. As the transformer short circuit impedances are mainly reactive, they are represented by $\mathbf{X_1}^{(\%)}$ and $\mathbf{X_2}^{(\%)}$.

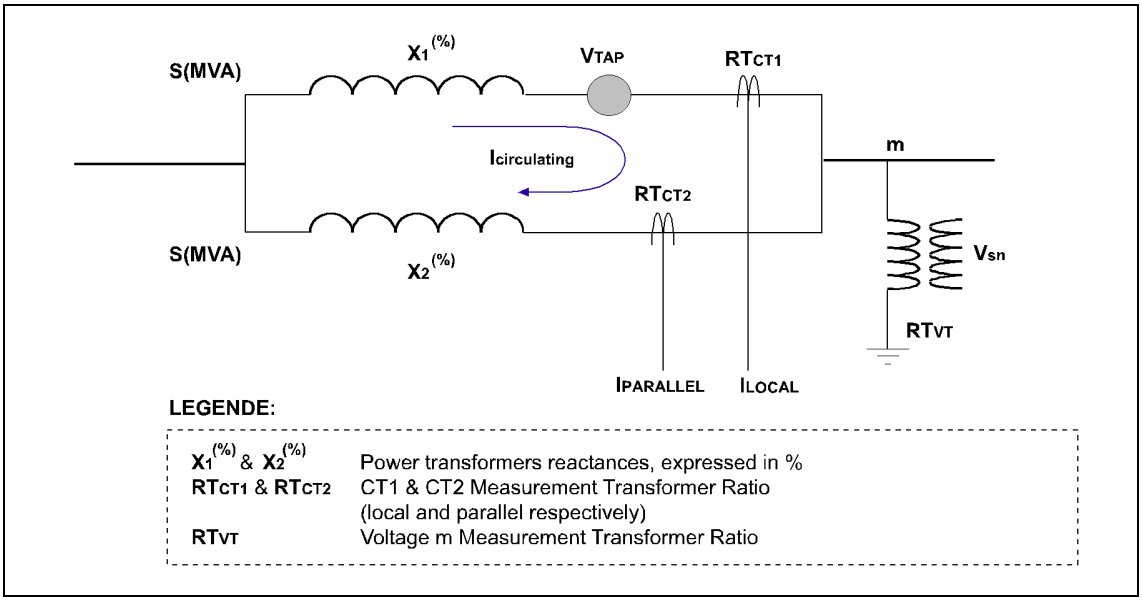


Figure 2.1.8 Diagram of two Transformers with Different Impedances Working in Parallel.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.7.b Calculation of the Reactive Current Flowing through two Transformers in Parallel with Current Wiring

For calculating the **Reactive Circulating Current** through the secondary winding of both power transformers **T1** and **T2** connected in parallel, the regulator has the following data:

I_1^m: current through **T1**, measured by the regulator (I_Local).
I_2^m: current through **T2**, measured by the regulator (I_Parallel).
φ_1: phase angle between I_1^m and voltage.
φ_2: phase angle between I_2^m and voltage.

Where I_1 and I_2 are actual currents through the secondary windings of power transformers **T1** and **T2**:

$$I_1 = I_1^m \cdot RT_{CT1}$$
$$I_2 = I_2^m \cdot RT_{CT2}$$

The **circulating current** through the **secondary** of both transformers, $I_{circulating}$, expressed in Amps, is calculated by the regulator thus:

$$I_{circ} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - I_2^m \cdot RT_{CT2} \cdot \text{sen}\,\varphi_2}{2}$$

Where:

$\varphi_1 = \varphi_{LOC} - \varphi_{PHASE\text{-}DIFFERENCE\ TT/TI\ LOC}$
$\varphi_2 = \varphi_{PAR} - \varphi_{\ PHASE\text{-}DIFFERENCE\ TT/TI\ PAR}$

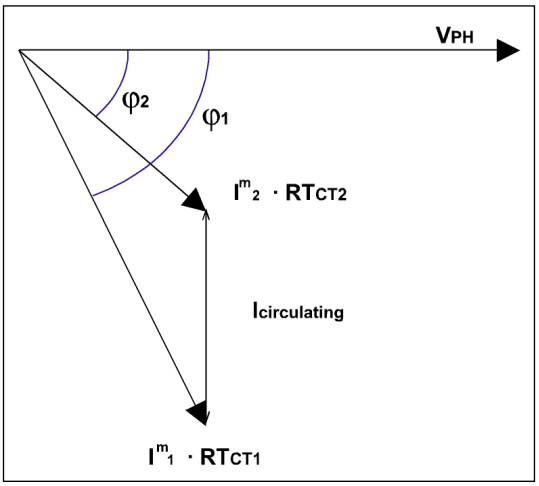


Figure 2.1.9 Diagram Representing the Reactive Circulating Current.

So, in this case, it will be necessary two CTs per each voltage regulator in order to wire not just the local current which is flowing through the transformer where the RTF is located but also the current which is flowing by the other transformer in parallel conditions.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.7.c Calculation of Circulating Reactive Current by Communications (Maximum of 5 Transformers in Parallel)

In this case, regulators will interchange through communications (GOOSE messages) their own **Reactive Power** measurement, such that each relay will receive a maximum of 4 magnitudes through GOOSE messages subscription (the so called Q_x^m). In this way, and taking into account that transformers in parallel must be at the same voltage, the calculation of the **current flow** will be carried out through the following formulas:

$$I_{circ12} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - \left(\frac{Q_2^m}{3 \cdot V_1^m \cdot RT_{VT1}} \right)}{2}$$

$$I_{circ13} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - \left(\frac{Q_3^m}{3 \cdot V_1^m \cdot RT_{VT1}} \right)}{2}$$

$$I_{circ14} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - \left(\frac{Q_4^m}{3 \cdot V_1^m \cdot RT_{VT1}} \right)}{2}$$

$$I_{circ15} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - \left(\frac{Q_5^m}{3 \cdot V_1^m \cdot RT_{VT1}} \right)}{2}$$

Where V_1^m is the measured voltage that will depend on the ***Wired Voltage Type*** setting.

Then the relay will calculate the final current flow:

$$I_{circ} = I_{circ12} + I_{circ13} + I_{circ14} + I_{circ15}$$

In this way, for the application of this scheme it is necessary to wire a single current transformer per regulator.

2.1.7.d Calculation of the Reactive Compensation Setting

As a general rule, power transformer manufacturers specify the impedance in **percentage** (**%**) or **per unit** (**pu**) of the nominal values which are displayed in the nameplate.

Per unit impedance values of same type machines are all within a very close margin, even if the ohmic values are very different, for different values of voltage and power ratings.

The device will have 5 settings to indicate the impedance of each of the Transformers that will be included in the scheme and K_R factor will be calculated automatically and in a dynamic mode based on the signals that indicate if a transformer is in parallel condition:

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- With two transformers in parallel conditions:

$$K_R = \frac{X_1(\%) + X_x(\%)}{10}$$

- With more than two Transformers in parallel conditions:

$$K_R = \frac{X_1(\%) + X_{PAR}(\%)}{10}$$

$$\frac{1}{X_{PAR}(\%)} = \frac{1}{X_2(\%)} + \frac{1}{X_3(\%)} + \frac{1}{X_4(\%)} + \frac{1}{X_5(\%)}$$

2.1.7.e Calculation of the Compensation by Circulating Current

Once the circulating current has been calculated, the device will compensate the setpoint value in the following way:

$$\mathbf{V_{DCOMP}\ (\%) = V_D\ (\%) + K_R\ (\%) \cdot [\ (\ I_{circ}\ /\ RT_{CT1}\ )\ /\ 0{,}1 \cdot\ I_n]}$$

2.1.7.f Example

- Transformer T1 data: 15 MVA; 69 kV / 13.8 - 11.9 KV; 12.95%;
- Transformer T2 data: 15 MVA; 69 kV / 13.8 - 11.9 KV; 13.00%;

- Voltage measurement transformer ratio (VT):

$$V_{sn} = 120\ V\ ; \rightarrow RT_{VT} = 13800/120$$

- Tap voltage variation (17 taps):

$$\Delta V_{tap} = 862.5\ V \text{ (referred to primary)}$$
$$\Delta V_{tap} = 862.5 * (13.8/69) = 172.5\ V \text{ (referred to secondary)}$$

- Power transformer rated secondary current:

$$I_{sn} = 627.55\ A\ ; \rightarrow RT_{CT1} = RT_{CT2} = 800/5$$

- Calculation of circulating current due to ΔV_{tap} :

$$\Delta I_{circ} = 172.5 / 3.295 = 52.358\ A$$

- Calculation of loop impedance Z_{loop} (Ω) :

$$Z_{base1} = Z_{base2} = U_{sn}^2 / S = 13.8^2 / 15 = 12.696\ \Omega$$
$$Z_{loop} = (Z_{pu1} + Z_{pu2}) \cdot Z_{base} = (0.1295 + 0.13) \cdot 12.696 \approx 3.295\ \Omega$$

- Simplified calculation of reactive compensation setting $K_R^{(\%)}$:

$$K_R^{(\%)} = (X_1^{(\%)} + X_2^{(\%)}) / 10 = (12.95 + 13) / 10 = 2.59\%$$

- Exact calculation of reactive compensation setting $K_R^{(\%)}$:

$$K_R^{(\%)} = \frac{X_1^{(\%)} + X_2^{(\%)}}{10} \cdot \frac{V_{s\,LN}^T}{V_{pn}^m} \cdot \frac{I_{pn}^{ml}}{I_{sn}^T}$$

$$K_R^{(\%)} = 2.59\% \cdot (13800/13800) \cdot (800/627.55) = 3.30\ \%$$

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.8 Combined Compensation and Maximum Compensation

The two types of ***Set-point voltage V_D*** setting compensation used by the **RTF** to obtain the **Compensated voltage V_{DCOMP}** have been described separately. In case both compensation methods were applied simultaneously, the calculation of the **Compensated voltage V_D** will be the sum of both compensations.

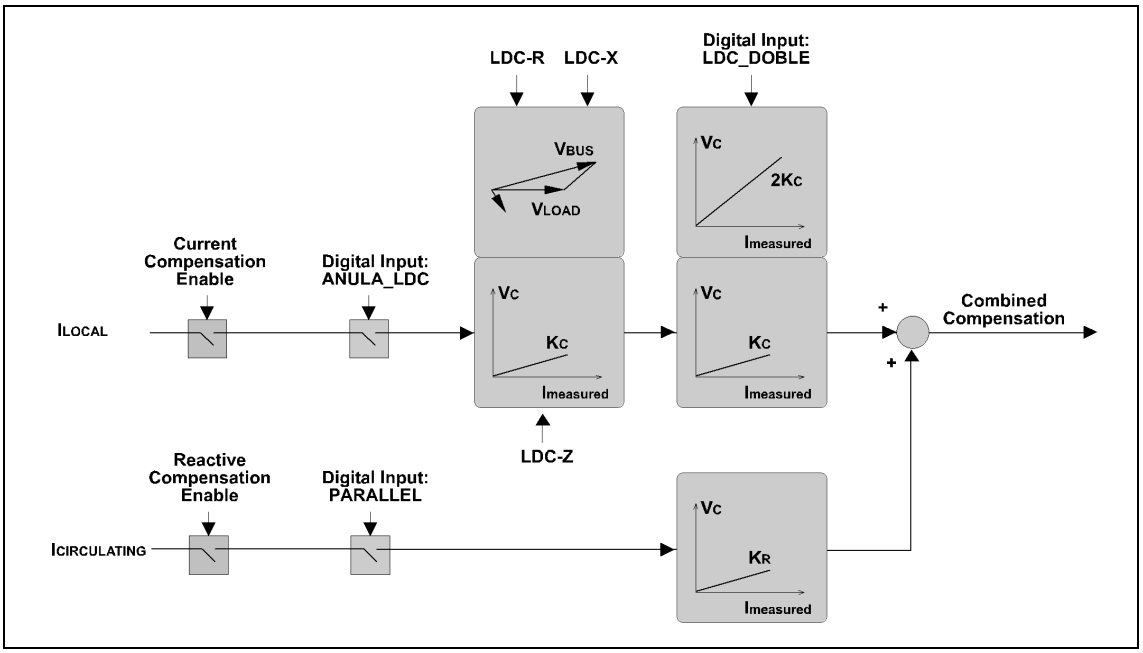


Figure 2.1.10 Combined Compensation and Maximum Compensation.

The ***Maximum Compensation*** setting limits the voltage compensation to a given value, such that if the sum of both current and reactive compensation values or each of said compensation values separately, exceeds said setting, this latter setting is used for the calculation of the voltage value.

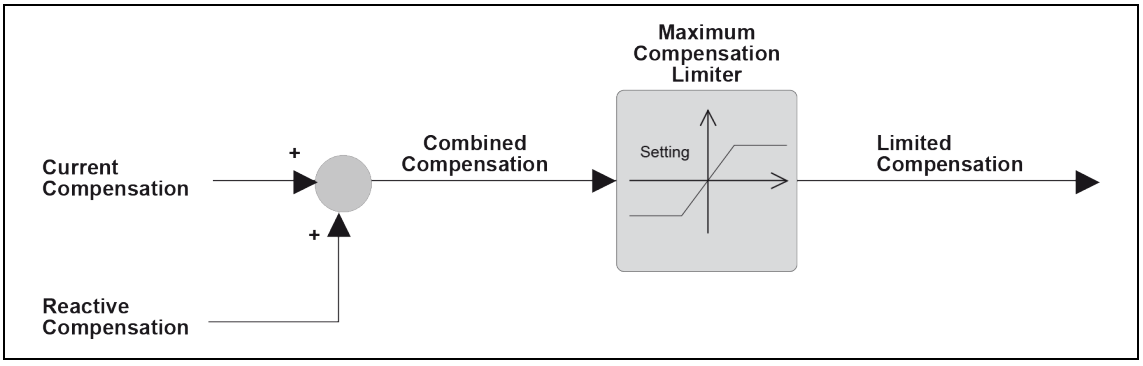


Figure 2.1.11 Maximum Compensation Setting.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.9 Automatic / Manual Regulation Mode

The **RTF** can operate on the following **Regulation Modes**:

- **Automatic Mode**: enables the main regulator control loop **DV** deviation signal input to the regulator, which calculates the **Raise / Lower the Tap commands**.
- **Manual Mode**: the regulator does not calculate the **Raise / Lower the Tap commands**. Refer to the following section on how to carry out manual tap change operations.

Methods can be switched through **Switch to Automatic Command / Switch to Manual Command** commands, either through front pushbuttons, digital inputs or communications system.

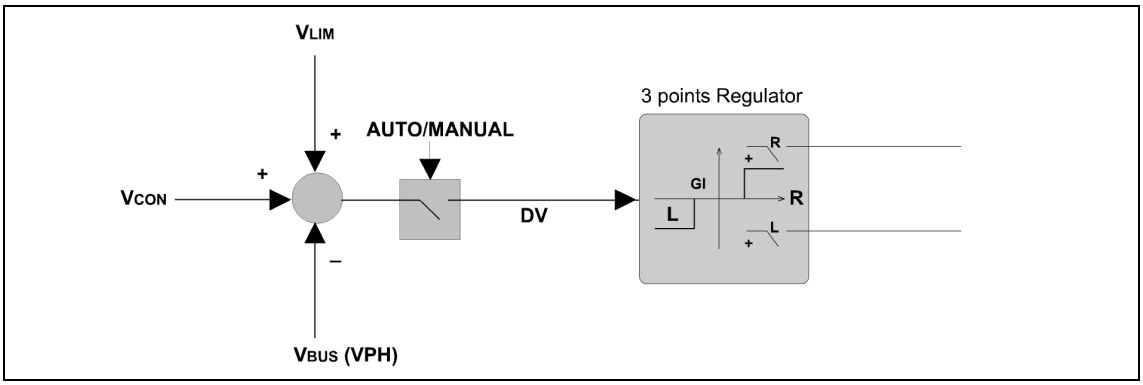


Figure 2.1.12 Main Regulator Control Loop (Automatic Mode).

There exists a specific situation when the regulator will switch spontaneously from **Automatic Mode** to **Manual Mode**. Refer to Blockings section.

2.1.10 Manual Commands

The **RTF** can execute manual **Raise and Lower the Tap** commands through:

- Raise the Tap Command
- Lower the Tap Command

These commands can be configured using the Configuration program, connecting to:

- Front keypad pushbuttons
- Digital inputs
- Communications system

To be able to execute these commands, the equipment must be in **Manual Mode**, since being in **Automatic Mode** the manual commands are blocked by the automatism.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.11 Tap Control

2.1.11.a Tap Coding

RTF relays are provided with 40 logic inputs to the protection (INXX_TAP) for detecting the **Active Tap** (Refer to section 2.1.17, Voltage Regulator Digital Inputs).

The coding can be **Direct** or in **BCD Code** (Binary Coded Decimal).

- **Direct** coding: every input represents a Tap value, which must be configured through the configuration program. That is to say, IN01_TAP input activation will result in the **Active Tap** being equal to the **Minimum Tap** setting value.
- **BCD Code***:* using up to a maximum of 7 (seven) digital inputs associated with the first seven inputs of protection logic used to assign the taps (IN01_TAP to IN07_TAP) configured using the configuration program. Assuming that the **Minimum Tap** setting is set to 1, the **Active Tap** is coded as specified in the following table:

Active Tap	IN07_TAP	IN06_TAP	IN05_TAP	IN04_TAP	IN03_TAP	IN02_TAP	IN01_TAP
1							X
2						X	
3						X	X
4					X		
5					X		X
6					X	X	
7					X	X	X
8				X			
9				X			X
10			X				
11			X				X
12			X			X	
13			X			X	X
14			X		X		
15			X		X		X
16			X		X	X	
17			X		X	X	X
18			X	X			
19			X	X			X
20		X					

Active Tap	IN07_TAP	IN06_TAP	IN05_TAP	IN04_TAP	IN03_TAP	IN02_TAP	IN01_TAP
21		X					X
22		X				X	
23		X				X	X
24		X			X		
25		X			X		X
26		X			X	X	
27		X			X	X	X
28		X		X			
29		X		X			X
30		X	X				
31		X	X				X
32		X	X			X	
33		X	X			X	X
34		X	X		X		
35		X	X		X		X
36		X	X		X	X	
37		X	X		X	X	X
38		X	X	X			
39		X	X	X			X
40	X						

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.11.b Number of Taps, Minimum Tap, Upper Limit and Lower Limit

Number of Taps, Minimum Tap, Upper and Lower Limits are the settings related to **Tap Control**.



The **Maximum Tap** is calculated as a function of the Minimum Tap and the Number of Taps, according to the formula:

Maximum Tap = Minimum Tap + Number of Taps - 1

Example 1:Minimum Tap = -3 ; Number of Taps = 7 → Maximum Tap = +3
Example 2:Minimum Tap = 0 ; Number of Taps = 16 → Maximum Tap = +15
Example 3:Minimum Tap = 40 ; Number of Taps = 40 → Maximum Tap = +79

2.1.11.c Tap Indication

Tap Indication stands for the fact of having a number of digital inputs configured and hard wired for this purpose. No settings are therefore involved and is independent of whether there is monitoring or not.

The **Active Tap** indication will be a function of the **Minimum Tap** and **Maximum Tap** settings:

- Active Tap value: (Minimum Tap< = Tap< = Maximum Tap), or
- invalid value, for the display to show "***".

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.11.d Tap Monitoring

Tap Monitoring stands for the fact of alarm or blocking generation upon special conditions. It involves a setting.

With the **Tap Monitoring** setting enabled, when the tap reaches any of the Minimum Tap, Maximum Tap, Lower Limit and Upper Limit, the corresponding logic outputs are activated, and can be used for regulator blocking.

Alarms are **Logic Outputs**:

- Invalid tap alarm (no tap, simultaneous, etc.).
- Upper tap limit alarm.
- Lower tap limit alarm.
- Maximum tap alarm.
- Minimum tap alarm.
- Command failure alarm.
- Runaway alarm.

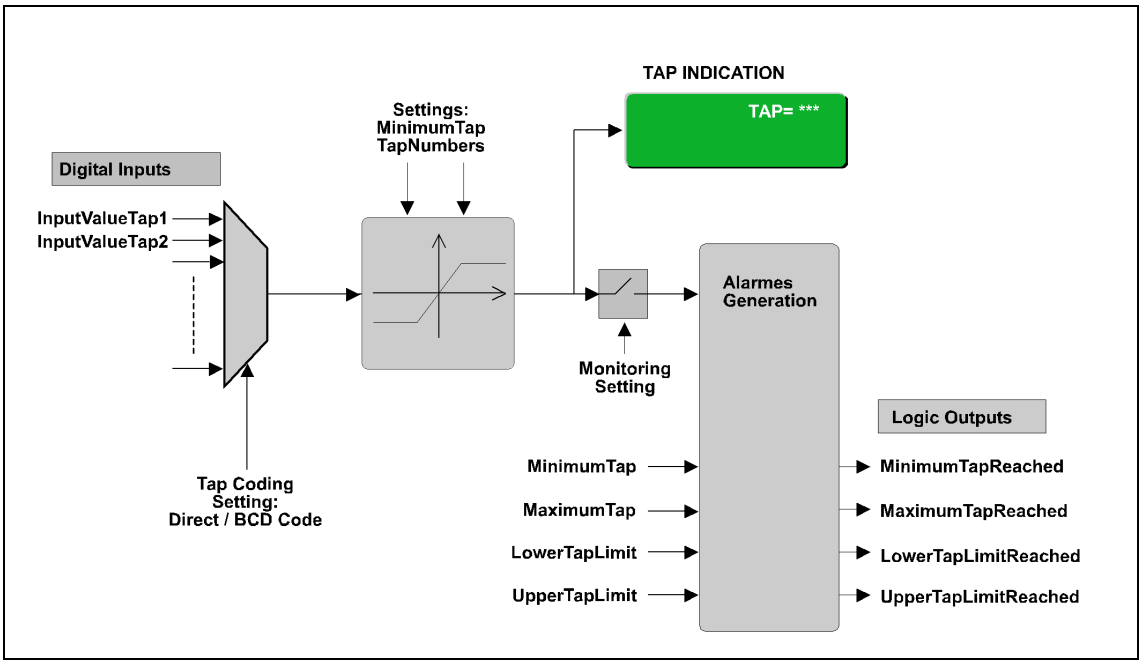


Figure 2.1.13 Tap Monitoring Setting Diagram.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.11.e Tap Change Operation Monitoring

When **Tap Monitoring** is enabled, three settings are available to monitor the tap change operation after a command. Said settings are **Command Failure Time**, **Maximum Simultaneous Tap Time and Maximum No Active Tap Time**.

- **Command Failure Time**: waiting time for tap change command execution. If no tap change occurs before the timer times out, a new command is sent. If this second command fails, the **Raise / Lower Tap Command Fail** outputs activate. The tap must change to the next up or down tap, respectively, in order to be acknowledged as correct. This time is also used to generate runaway alarm such that if after a raise/lower tap command the relay detects two tap changes, going through both taps, within the operation failure time setting, then the relay generates a runaway alarm.
- **Maximum Simultaneous Tap Time**: time elapsed from the time the relay detects various **Active Taps** until **Blocking on Simultaneous Tap** state is reached.
- **Maximum No Active Tap Time**: time elapsed from the time the relay detects no **Active Tap** until the **Blocking on No Active Tap** state is reached.

Refer to section 2.1.12, **Blockings** to check activation and reset conditions.

2.1.11.f Tap Change Operation Counters

In order to make tap changer maintenance operations easier, 2 (two) counters are provided:

-
- **Number of Raise the Tap Operations** (RAISE_OPER_CNT)
- **Number of Lower the Tap Operations** (LOWER_OPER_CNT)

Counters can be reset through the digital input **Tap Changer Operation Counter Reset**.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.12 Blockings

The regulator must remain blocked on a number of circumstances. Some blockings only affect the **Automatic Mode** and other blockings only the **Manual Mode**. Also, some blockings are a function of **Tap Monitoring**.

- **Blocking Limits**

These blocks only affect the Automatic Mode and therefore the automatic tap up/down commands will be blocked while the manual tap up/down commands will be accepted and processed.

Minimum Voltage Blocking

The regulator is blocked when the measured voltage is below the **Minimum Voltage** setting value (refer to **Blocking Limits** settings). The blocking condition resets when the measured voltage is above said setting. The blocking could be delayed through the setting **Minimum Voltage Timer**.

Maximum Switched Current Blocking

The regulator is blocked when the measured current is above **Maximum Switched Current** setting value (refer to **Blocking Limits** settings). This protects the tap changer contacts from excessive wear.

Blocking by voltage out of range

The regulator blocks when the measured voltage is out of the regulation range for a time exceeding the **Time for Voltage out of Range** setting. The blocked condition resets when the measured voltage is again within the regulation range. The blocking could be disabled or reset from the control logic by using the signals **Voltage out of Range Blocking Enable** and **Voltage out of Range Timer Reset**.

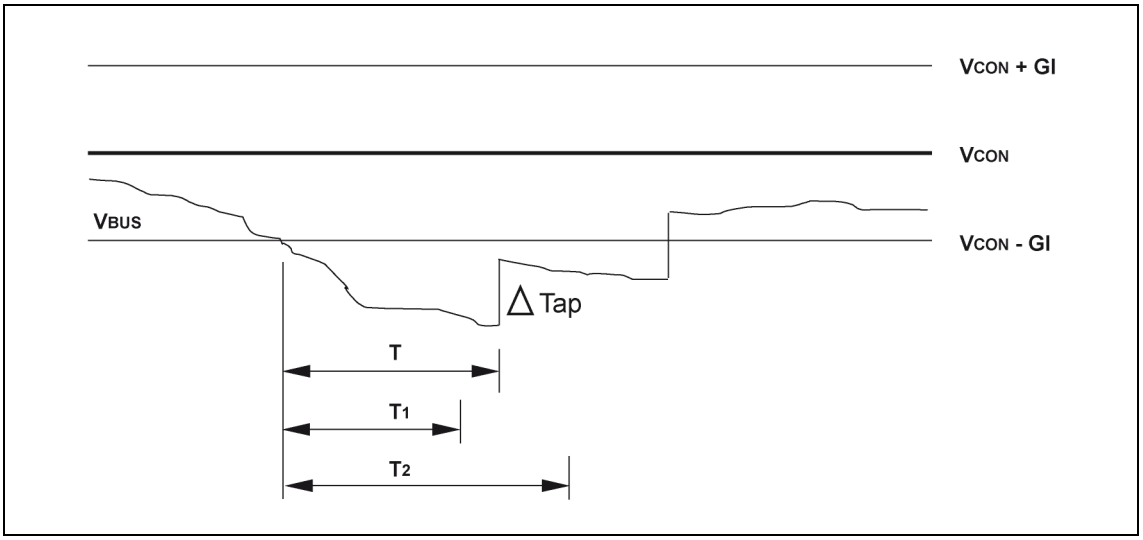


Figure 2.1.14 Blocking by Voltage out of Range.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Example:

Case 1: T1 (Blocking by voltage out of range) < T (Time for changing tap). The regulator blocks after T1.
Case 2: T2 (Blocking by voltage out of range) > T (Time for changing tap). The regulator changes tap and blocks after T2.

- **Blockings Dependent on Tap Monitoring**

*These blockings only operate when the **Tap Monitoring** feature is enabled and they affect to both, the automatic and manual modes so all the tap up/down commands (automatic and manual) will be blocked.*

No Active Tap or Simultaneous Tap Blocking

The relay remains blocked if after an adjustable time setting (**Maximum Time with No Active Tap** setting), no active tap exists or if after another adjustable time setting (**Maximum Time with Simultaneous Taps** setting), more than one tap is active simultaneously.

To exit the blocked condition simply activate one tap if the blocking occurred by no active tap, or else deactivate all taps but one if the blocking occurred by excess of taps.

Extreme Tap Blocking

When being in the maximum or minimum tap, if the voltage goes out of the desired area so that a tap up/down command is expected respectively (direct tap/voltage relation), the AVR will not execute the command. The only way to unblock the IED is giving an opposite tap command (if the tap is the minimum one, a tap up command and if the tap is the maximum one a tap down command).

Tap failure Command Blocking

If **Tap Monitoring** is enabled, commands are monitored so that the IED can confirm that the value of the tap is changing accordingly. The behavior of the device depends on the Selectable Outputs Type setting (pulse or level):

- Pulse: the command is executed two consecutive times; this is, if, once a tap command has been issued, the corresponding tap change does not occur before the fail tap change timer times out, a new command is sent, and if the corresponding tap change does not occur before the tap change fail timer times out again, the **Tap Failure Command Blocking** activates.
- Level: the command is executed only one time; this is, if, once a tap command has been issued and the corresponding tap change does not occur before the fail tap change timer times out, the **Tap Failure Command Blocking** activates directly.

Under these circumstances, the relay switches to **Manual Mode**. The relay can be unblocked by switching again to **Automatic Mode**.

Tap change must be step by step; this is, the relay waits for the tap to change to the next step up if it is a raise the tap command, or to the next step down if it is a lower the tap command. If tap changes are not produced in this way, the tap change is not acknowledged and the block is equally activated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Runaway blocking

With the tap supervision enabled, commands are supervised, such that if after a command the relay detects two consecutive tap changes within the command failure time setting, namely, the relay goes to the next tap, the target tap, and from this to another, the relay switches to **Block by Runaway**.

- **Logic Blocking Inputs**

These blocks affect to both, the automatic and manual modes so all the tap up/down commands (automatic and manual) will be blocked.

The following logic inputs can be allocated to physical inputs or configured in logic cards through the configuration program. Inputs will remain deactivated if not allocated or configured.

- **External Blocking.**
- **Automatic Raise Tap Operation Blocking.**
- **Automatic Lower Tap Operation Blocking.**
- **Manual Raise Tap Operation Blocking.**
- **Manual Lower Tap Operation Blocking.**

The two figures below show the positions of all blockings within the regulator control loop.

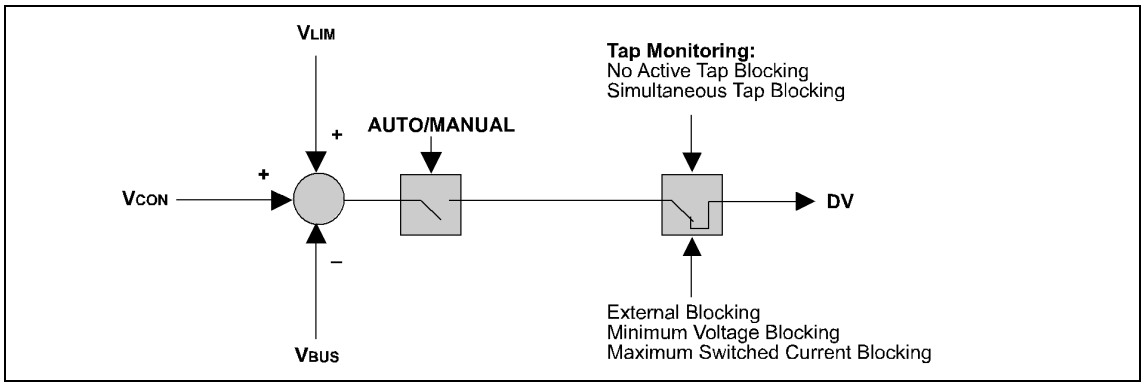


Figure 2.1.15 Blockings within the Main Regulator Control Loop (Automatic Mode).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

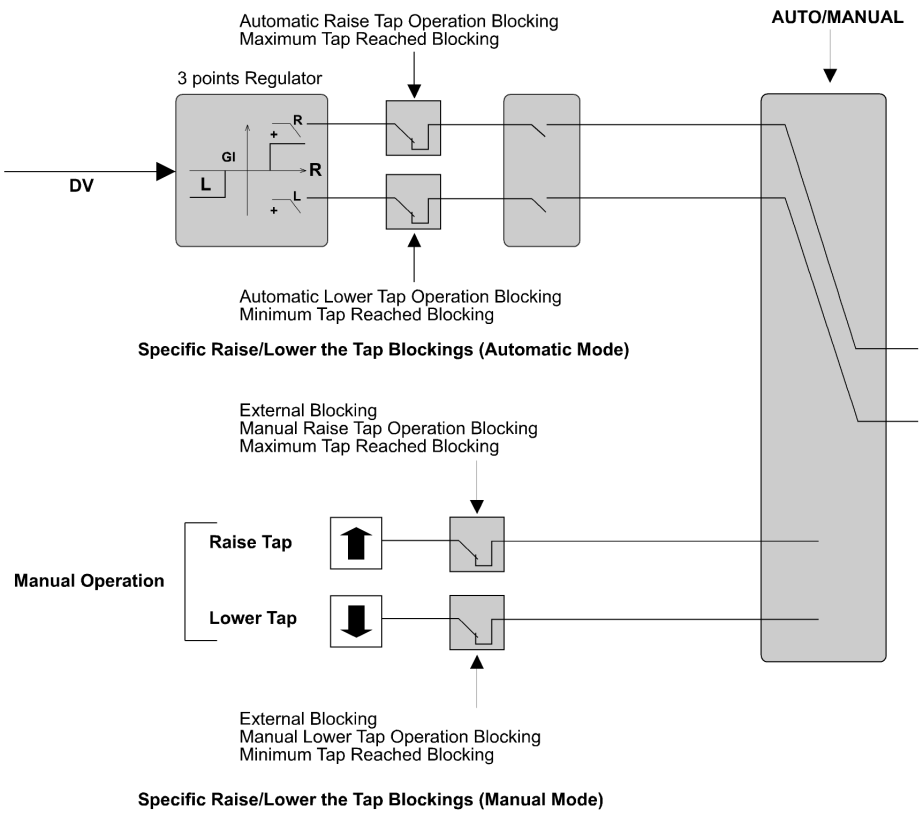


Figure 2.1.16 Specific Raise / Lower the Tap Blockings (Automatic and Manual Modes).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.13 Power Flow Reversal

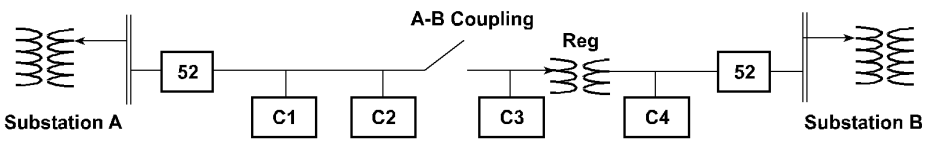


Figure 2.1.17 Power Flow Reversal Diagram.

Normally, the **A-B Coupling** is open and loads are supplied radially from their respective substations. If Substation B is put out of service, C3 and C4 loads could be supplied from Substation A, simply closing the **A-B Coupling**. The power flow through **Reg Regulator** would be reversed.

To regulate the voltage under this situation, the regulator should be provided with a VT on the original power supply side (Substation B side), or calculate said voltage from known data. Another valid option could be blocking the regulator on **power reversal** detection.

The **RTF** activates the logic **Detected Power Reversal** output when the angle between V_{PH} and I_{LOCAL}, once corrected by the setting ***Local VT/CT Phase Difference*** is:

$$90º < \varphi < 270º$$

and resets said output when:

$$85º > \varphi > 275º$$

This logic output can be configured through logic to block the regulator or to position it at an intermediate tap (e.g. neutral tap).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.14 Voltage Band Recording

Voltage Band settings define a set of limits to compare the voltage (in % of $V_{nominal}$). This way a reference band is available, three upper level bands and another three lower level bands.

Bands can be represented as in the following diagram:

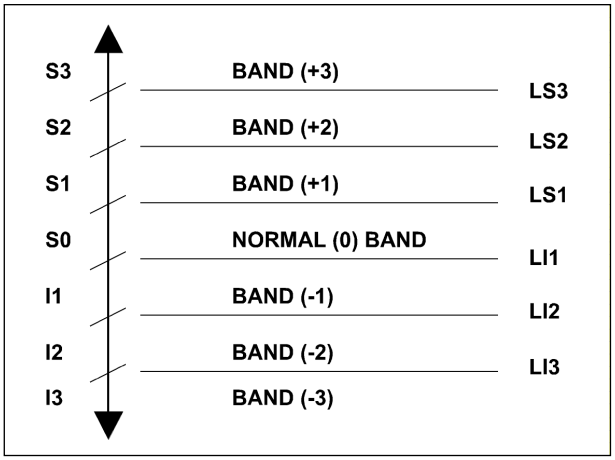


Figure 2.1.18 Band Diagram.

Voltage Band Records are cumulative monthly periodical records, that is, there is a record every month (12 months). The following information is written:

-
- Number of **Raise the Tap** Operations (NRaiseTapOperations), in the month.
- Number of **Lower the Tap** Operations (NLowerTapOperations), in the month.
- Permanence time (in seconds) of the voltage within each band, in a month.
- Number of times the voltage has been within each band, in a month.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.15 Display Information

Vd: represents the setpoint value the AVR Works with (once the compensations have been applied)
Vreg: measurement to be regulated (measured voltage or external).
Tap: current tap value. When the IED is not detecting the tap, there are simultaneous taps activated or the taps are not configured, three stars will be displayed.
DEV: indicates if the measured to be regulated is inside (square with empty background) or out of (square with black background) the defined area (setpoint ± GI). When the regulated measurement is out of the area it will appear an arrow indicating if the measurement is under or over the desired area.
AUT/MAN: Indicates the automatic or manual status.

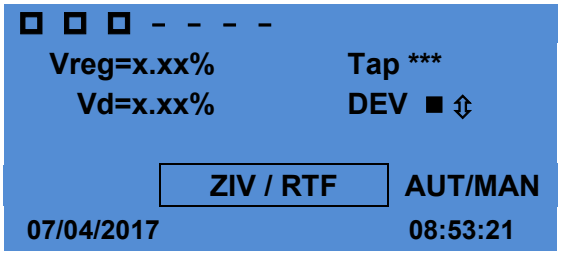


Figure 2.1.19 Information in Default Screen. Alphanumeric Display.

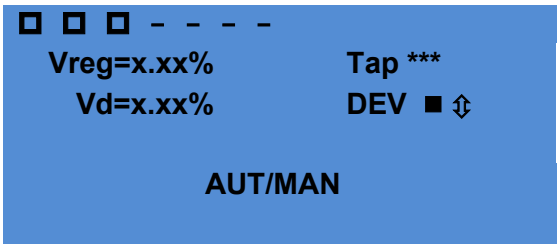


Figure 2.1.20 Information in Control Screen (once the information element has been added in the control configuration of the device). Graphical Display.

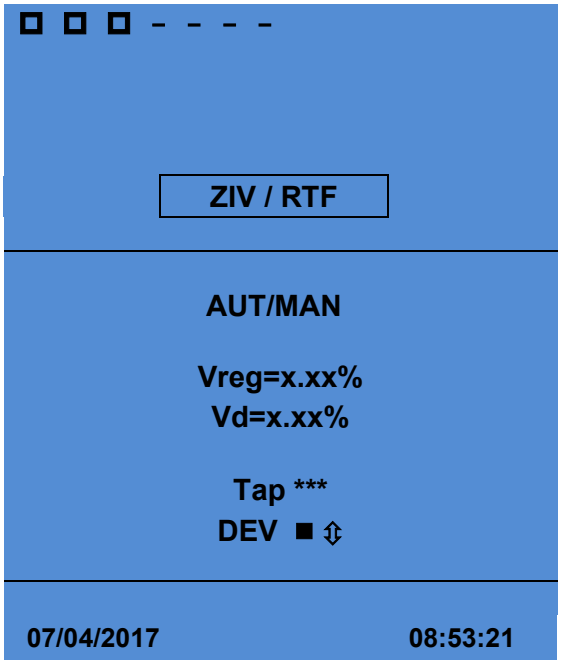


Figure 2.1.21 Information in Default Screen. Graphical Display.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.16 Settings Recommendation

Nominal Values	
VControl	Set the nominal voltage the relay is going to measure and control in secondary values (taking into account if it is a phase to phase or phase to ground voltage). This way the default setpoint setting will be 100%.
IABC	Nominal current of the local CT in secondary values (1A or 5A).

General Settings	
VT and CT ratios	Set the ratios (primary divided by secondary) for the VT and CT. The relay will use this just to show the measurements in the display in primary values multiplying the setting by the value measured and to send them by communications.
Voltage input type	Define the wired voltage.
LOCAL and PARALLEL input type	Define the wired currents
Voltage source	VPH

Voltage Regulator Configuration	
Tap Changer Supervisory Control	Yes, but just if the tap value is received.
Tap Codification Type	It depends on how the tap value is received. BCD if BCD code is wired and Direct in any other case.
Units in Main Display	Primary.
Selectable outputs type	Pulsed with 500ms. When activating the supervisory control, it is recommended using the Continuous mode and so the output will reset when reaching to the expected tap value or after the failure time.

Voltage Regulator Control	
Voltage Setpoint (Bandcenter)	100%
Voltage Setpoint (Bandcenter) 1 to 5	As required.
Voltage Setpoint Increment	1%
Dead Band (bandwidth/2)	Normally is set with the value of one tap, this is the voltage difference between two taps is percentage. If the value of the Bandwidth (2 times the setting) is smaller than the tap-change increment of the transformer, the controlled system can never reach a stable condition as the voltage exceeds the bandwidth selected. If, on the other hand, a very large bandwidth is selected there will be a major control deviation and therefore the control and precision will be less. It must be ensured that. It must be ensured that: $\frac{Insensitivity}{DeadBand} \geq 0.6 * \text{tap-change increment [\%]}$
Tap/voltage Relation	it depends on the tapchanger type and where the voltage is measured/control. The default value is Direct, this is reducing the voltage means tapping down.
Runback Voltage	115%. Normally transformers regulate between 100 ± 10% so it should be set above the maximum voltage. This way the relay will detect great variations of the voltage and will skip the first delay time.
Time Delay Type	Inverse or Definite for the first delay time.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Voltage Regulator Control (continue)	
Time Factor for Inverse Curve	Just necessary when defining Inverse in the previous setting.
Definite Time T1	10 to 15 seconds.
Definite Time T2	10 to 15 seconds.

Compensations	
Line Drop Compensation	Enable it when required.
Line Drop Compensation Type Selector	It depends on the electrical system where the RTV is installed. Normally LDC R-X is used when line parameters are known and the load is concentrated at the end of one line and LDC-Z is used when many lines are involved or the line parameters are not known.
Z	100*Vline/VN.
R	Resistance voltage drop in the line.
X	Reactance voltage drop in the line.
Circulating Current Compensation	Enabled when required.
Parallel Transformer Data Source	Communications or wired depending on the system design. In case of selecting Communications, the RTVs will exchange the information by GOOSE message (LAN port).
Maximum Voltage Compensation Limit	10%.
Transformer Impedances	X1, X2, X3, X4 and X5 of each transformer.

Lockout Limits	
Under Voltage	80%.
Under Voltage Timer	Set a time if required.
Maximum Switching Current	120%.
Time for Out of Voltage	Greater than T1 + T2 x (maximum number of taps -1).

Tap Control	
Number of Taps	Depending on the system/design. It is not necessary.
Minimum Value	Minimum value of the tap.
Low Limit Value	Value of the tap that will generate the low tap value reached alarm and block.
Upper Limit Value	Value of the tap that will generate the high tap value reached alarm and block.
Operation Failure Time	Greater than time to send the command + time passed till the tapchager receives the command + mechanical time that takes the tapchanger to change the tap. It has to be equal or less than the T2 delay time.
Maximum Simultaneous Time	10 to 15 seconds.
Maximum Time without Active Tap	10 to 15 seconds.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.17 Settings Calculation Example

- **Example 1**

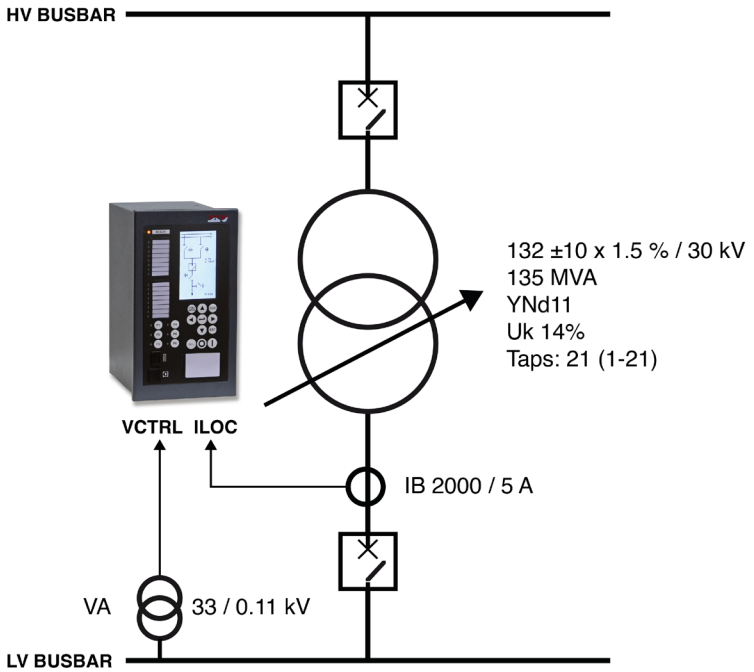


Figure 2.1.22 Example 1 Information.

Table 2.1-2: Example 1 for Settings Calculation	
Voltage wired to the relay	Phase A → VA → 57.73V in secondary values.
Nominal values	IABC: 5A
	VControl: 57.73V
	Frequency: 50 or 60Hz
General	TT Ratio: 300
	CT Ratio: 400
	Type of voltage: VA
	Type LOCAL current: IB
	Voltage source: VPH (wired)
Voltage Regulator Configuration	TapChanger Supervisory Control: Yes.
	Tap Codification type: Direct.
	Units in Main Display: Primary Values.
	Selectable Output Type: continuous.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 2.1-2: Example 1 for Settings Calculation	
Voltage Regulator Control	Voltage Setpoint (Bandcenter): 100 % (57.73V in secondary values, this is 30kV in primary side).
	Voltage Setpoint (Bandcenter) 1, 2, 3, 4, 5: N/A.
	Voltage Setpoint Increment: 1
	Dead Band (Bandwith/2): 2.6% Δtap = 1980V HV side → 450V LV side. This voltage referred to the secondary of the VT is: 450 / 300 = 1.5V. Referring this voltage to the nominal voltage of the device: 100 x 1.5 / 57.73 = 2.6 %.
	Tap/Voltage Relation: Direct.
	Runback Voltage *: > 151.8/132 = 1.15 → 115%
	Time Delay Time: Definite Time.
	Time Factor for Inverse Curve: N/A.
	Definite Time T1: 10 s.
	Definite Time T2: 10 s.
Compensations	As required
Lockout Limits	Under Voltage: < 112.2/ 132 (= 85%) → 75%
	Under Voltage Timer: 0s.
	Maximum Switching Current: 115%
	Time for Out of Voltage: 10s + 10s x 22 taps (three tap change at central tap) = 230s.
Tap Control	Number of Taps: 21
	Minimum Tap: 1
	Low Limit Tap Value: 1
	Upper Limit Tap Value: 21
	Operation Failure Time: 15s.
	Maximum Simultaneous Time: 10s.
	Maximum Time without Active Tap: 10s.
	External Resitor Chain: N/A.
Voltage Bands	115%, 110%, 105%, 100%, 95%, 90%

(*) Over the maximum regulation voltage, even though the Overvoltage Unit (59) will not allow reaching to this voltage level unless it is set to trip with values over 115 % Un.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Example 2**

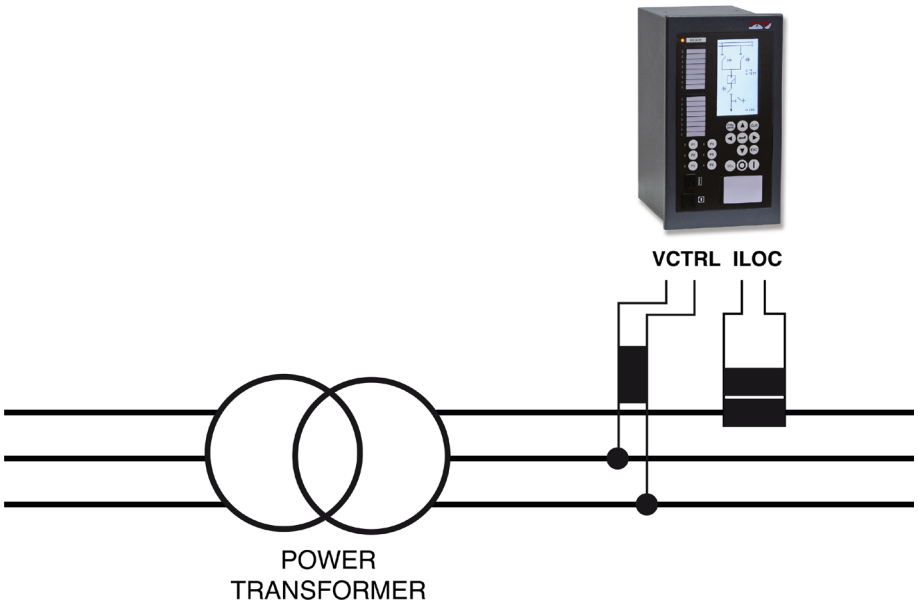


Figure 2.1.23 Example 2 Information (Modifying the VT/CT Connection).

Table 2.1-3: Example 2 for Settings Calculation	
Nominal values	IABC: 5A
	VControl: 110V
General	TT Ratio: 300
	CT Ratio: 400
	Type of voltage: VBC
	Type of LOCAL current: IA

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.18 Setting Ranges

Settings / Voltage Regulator / Regulator Configuration					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Tap Monitoring	Enable Tap Superv.	ATCC1.TapGrd	YES / NO		NO
Tap Coding	Tap Code	ATCC1.TapInTyp	Direct BCD Code		Direct
Magnitude Display (Default Screen)	Display Units	ATCC1.UnitsDisp	Primary Secondary Percentage		PERC.
Voltage Type	Voltage Type	ATCC1.VCtlTyp	VA VB VC VAB VBC VCA		VA
Local Current Type	Type Loc Current	ATCC1.ALocTyp	IA IB IC		IA
Parallel Current Type	Type Par Current	ATCC1.AParTyp	IA IB IC		IA
Control Voltage Origin	Voltage Source	ATCC1.CtrVar	V Measured External V		V MEA.
Output Type (*)	Outputs Type	ATCC1.TapOutTyp	Pulse Level		Pulse
Output Pulse Duration	Pulsed Output Time	ATCC1.TapPlsTmms	0.1 - 5s	0.01s	1s

(*) There is a settings ratio check function to make sure that if *Tap Monitoring* is disabled, the Output Type may not be on Level.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Voltage Regulator / Voltage Regulator Control					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Voltage Setpoint	Volt. Setpoint	ATCC1.BndCtr	80 - 120%	0.01%	100%
Voltage Setpoint 1	Volt. Setpoint 1	ATCC1.BndCtrVal1	80 - 120%	0.01%	100%
Voltage Setpoint 2	Volt. Setpoint 2	ATCC1.BndCtrVal2	80 - 120%	0.01%	100%
Voltage Setpoint 3	Volt. Setpoint 3	ATCC1.BndCtrVal3	80 - 120%	0.01%	100%
Voltage Setpoint 4	Volt. Setpoint 4	ATCC1.BndCtrVal4	80 - 120%	0.01%	100%
Voltage Setpoint 5	Volt. Setpoint 5	ATCC1.BndCtrVal5	80 - 120%	0.01%	100%
Voltage Setpoint Increment	Volt Setp Incr	ATCC1.BndCtrInc	1 - 6%	1%	1%
Insensitivity Degree	Bandwidth/2	ATCC1.BndWid	0.4 - 5%	0.01%	3%
Tap / Voltage Relation	Tap/Volt Relation	ATCC1.TapVRl	Inverse Direct		Direct
First Operation Time Curve	First Op. Time Curve	ATCC1.TmDlChr	Inverse Definite Time		Inverse
Time Factor	Time Factor	ATCC1.TmMult	1 -10	0.01	10
Definite Time T1	Definite Time T1	ATCC1.DlTmmsT1	1 - 600s	0.01s	10s
Definite Time T2	Definite Time T2	ATCC1. DlTmmsT2	1 - 600s	0.01s	10s
Runback Voltage (cancel T1)	Runback Voltage	ATCC1.RnbkRV	100 - 130%	0,01%	110%

Settings / Voltage Regulator / Compensation					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Line Drop Compensation Enable (LDC)	Enable LDC	ATCC1.LDC	YES / NO		NO
Line Drop Compensation Type (LDC)	LDC Type	ATCC1.LDCTyp	LDC Z LDC R-X		LDC Z
Line Drop Compensation Z (LDC-Z)	LDC-Z parameter	ATCC1.LDCZ	0 - 10%	0.01%	0%
Line Drop Compensation R (LDC-R)	LDC-R parameter	ATCC1.LDCR	-30 - 30V	0.01V	0V
Line Drop Compensation X (LDC-X)	LDC-X parameter	ATCC1.LDCX	-30 - 30V	0.01V	0V
Reactive Compensation Enable	Enable Circ. Curr.	ATCC1.ReacComEna	YES / NO		NO
Data Source Parallel Transformers	Ext Trafos Source	ATCC1.ReacComSrc	Wired Communications		Wired
Maximum Compensation	Max Compensation	ATCC1.MaxComp	0.1 - 15%	0.01%	10%
Transformer Impedances					
X1	X1	ATCC1.Imp1	1 - 25%	0.01%	10%
X2	X2	ATCC1.Imp2	1 - 25%	0.01%	10%
X3	X3	ATCC1.Imp3	1 - 25%	0.01%	10%
X4	X4	ATCC1.Imp4	1 - 25%	0.01%	10%
X5	X5	ATCC1.Imp5	1 - 25%	0.01%	10%

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings / Voltage Regulator / Lockout Limits					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Minimum Volt	Min. Voltage	ATCC1.BlkUnCtlV	0.1 - 100%	0.01%	70%
Minimum Voltage Timer	Max. Current	ATCC1.BlkUnVTmms	0 - 600s	0.01s	0s
Maximum Switched Current	Out of Voltage	ATCC1.LimLodA	0.1 - 135%	0.01%	100%
Time for Voltage Out of Range	Under Volt Timer	ATCC1.VBlkDlTmms	1 - 1200s	0.01s	120s

Settings / Voltage Regulator / Tap Control					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Number of Taps	Number of Taps	ATCC1.TapNum	0 - 40	1	1
Minimum Tap Value	Minimum Tap Value	ATCC1.MinTap	-20 - 20	1	1
Low Limit Tap Value	Low Limit Tap	ATCC1.TapBlkL	-40 - 79	1	1
Upper Limit Tap Value	Upper Limit Tap	ATCC1.TapBlkR	-40 - 79	1	1
Operation Failure Time	Oper.Failure Time	ATCC1.FailOpTmms	5 - 20s	0.01s	10s
Maximum Simultaneous Time	Max.Simul. Time	ATCC1.SimTapTmms	5 - 20s	0.01s	10s
Maximum Time without Active Tap	Max. Time w/o Tap	ATCC1.NoTapTmms	5 - 20s	0.01s	10s

Notes:
1. Maximum Tap is calculated as: Maximum Tap = Minimum Tap + Number of Taps – 1
2. A settings check function exists to make sure that: Minimum Tap <= Lower Tap Limit <= Upper Tap Limit <= Maximum Tap

Settings / Voltage Regulator / Voltage Bands					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Voltage Band S3 Limit	Band Limit S3	ATCC1.LimVBndR3	0 - 130%	0.01%	115%
Voltage Band S2 Limit	Band Limit S2	ATCC1.LimVBndR2	0 - 130%	0.01%	110%
Voltage Band S1 Limit	Band Limit S1	ATCC1.LimVBndR1	0 - 130%	0.01%	105%
Voltage Band I1 Limit	Band Limit I1	ATCC1.LimVBndL1	0 - 130%	0.01%	100%
Voltage Band I2 Limit	Band Limit I2	ATCC1.LimVBndL2	0 - 130%	0.01%	95%
Voltage Band I3 Limit	Band Limit I3	ATCC1.LimVBndL3	0 - 130%	0.01%	90%

Note: There exists a settings ratio check function to make sure that:

S3 > S2 > S1 > I1 > I2 > I3

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.19 Analog Inputs to the Unit

Table 2.1-4: Analog Inputs to the Voltage Regulator Module		
Name	**Description**	**IEC 61850**
VCTRL / VEXT	Measure to control	ATCC1.CtlV
ILOC	Local Current	ATCC1.LodA MMXU1.AmpLoc
IPAR	Parallel Transformer Current	ATCC1.ParLodA MMXU1.AmpPar
PARALLEL T1 VAR	Parallel Transformer 1 Reactive Power	ATCC1.ParTotVAr1
PARALLEL T2 VAR	Parallel Transformer 2 Reactive Power	ATCC1.ParTotVAr2
PARALLEL T3 VAR	Parallel Transformer 3 Reactive Power	ATCC1.ParTotVAr3
PARALLEL T4 VAR	Parallel Transformer 4 Reactive Power	ATCC1.ParTotVAr4
TAP	Tap Position	ATCC1.TapChg
Setpoint	Setpoint	ATCC1.BndCtr
VCTRL	Wired voltage	MMXU1.Vctrl

2.1.20 Digital Inputs of the Voltage Regulator

Table 2.1-5: Digital Inputs of the Voltage Regulator					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN01_TAP	Logic Inputs to Protection	ATCC1.TapAct1	Input Value Tap 01		Logic inputs for Active Tap detection.
...		...	…		
IN40_TAP		ATCC1.TapAct40	Input Value Tap 40		
CANCEL_T1		ATCC1.InhDITm	Cancels Timer T1		Cancels Timer T1
BLK_EXT_REG		ATCC1.LTCBlk	Regulator External Blocking	I	Blocking Inputs.
BLK_MAN_RAISE		ATCC1.BlkOpManR	Manual Raise the Tap Operation Blocking	I	
BLK_MAN_LOWER		ATCC1.BlkOpManL	Manual Lower the Tap Operation Blocking	I	
BLK_AUT_RAISE		ATCC1.BlkOpAutoR	Automatic Raise the Tap Operation Blocking	I	
BLK_AUT_LOWER		ATCC1.BlkOpAutoL	Automatic Lower the Tap Operation Blocking	I	
ENBL_LDC	Module Enabling Control	ATCC1.LDCEna	Line Drop Compensation Enabled Input		The activation / deactivation of these inputs enables / disables the corresponding functionality. It can be assigned to DIs by level or to a command from the HMI. The default value of this logic input signal is a “1.”
ENBL_CREAC		ATCC1.ReacEna	Reactive Compensation Enabled Input		
ENBL_TIME_OUT_V		ATCC1.BlkVEna	Out of Voltage Block Enable Input		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 2.1-5: Digital Inputs of the Voltage Regulator					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
CMD_RAISE_STP	Commands Sequence	ATCC1.BndCtrChg	Raise the Voltage Set-point Command		Input commands to the automatism.
CMD_LOWER_STP		ATCC1.BndCtrChg	Lower the Voltage Set-point Command		
CMD_RAISE_TAP		ATCC1.TapChg	Raise the Tap Command		
CMD_LOWER_TAP		ATCC1.TapChg	Lower the Tap Command		
CMD_MANUAL		ATCC1.AutoCmd	Switch to Manual State Command	I	
CMD_AUTO		ATCC1.AutoCmd	Switch to Automatic State Command	I	
CMD_STP1		ATCC1.BndCtrAct1	Set Point 1 Activation Command		Commands to activate each setpoint value
...		...	…		
CMD_STP5		ATCC1.BndCtrAct5	Set Point 5 Activation Command		
RST_TAP_CNT	Reset Commands	ATCC1.TapCntRs	Tap Change Operation Counter Reset		Reset Commands
RST_TEMP_OUT_V		ATCC1.ResTOV	Reset Out of Voltage Timer		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

2.1.21 Auxiliary Outputs and Events of the Voltage Regulator

Table 2.1-6: Auxiliary Outputs and Events of the Voltage Regulator					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
ST_AUTO	Automatisms	ATCC1.Auto	Regulator Status: Automatic Mode (1) or Manual Mode (0)	I	Automatic Mode (1) or Manual Mode (0).
RAISE_OUTPUT		ATCC1.TapOpR	Raise the Tap Physical Output	I	RAISE operation executed by the IED.
LOWER_OUTPUT		ATCC1.TapOpL	Lower the Tap Physical Output	I	LOWER operation executed by the IED.
BLK_MIN_VOLT		ATCC1.LTCBlkVLo	Minimum Voltage Blocking	I	Measured voltage is below Minimum Voltage setting.
BLK_MAX_CURR		ATCC1.LTCBlkAHi	Maximum Switched Current Blocking	I	Measured local current is above Maximum Switched Current setting.
BLK_SEV_TAPS		ATCC1.BlkMultTap	Simultaneous Tap Blocking	I	Blockings
BLK_NO_TAPS		ATCC1.BlkNoTap	No Tap Blocking	I	
BLK_LIMIT_TAP		ATCC1.BlkLimTap	Limit Tap Blocking	I	
BLK_OUT_TIME		ATCC1.BlkVDlTm	Out of Voltage Timer Block	I	
BLK_INT_FAIL		ATCC1.BlkFailTap	Command Failure Blocking	I	
BLK_RUNAWAY		ATCC1.BlkRunAway	Runaway Blocking	I	
EXTREME_STP		ATCC1.LimBndCtr	Extreme set-point	I	Extreme set-point
FAIL_RASE		ATCC1.TapOpRFail	Raise the Tap Command Fail	I	Tap Command Failures.
FAIL_LOWER		ATCC1.TapOpLFail	Lower the Tap Command Fail	I	
MAX_TAP_REACH		ATCC1.EndPosR YLTC1.EndPosR	Maximum Tap reached	I	The active tap equals the Minimum Tap Setting. + Tap Number - 1
MIN_TAP_REACH		ATCC1.EndPosL YLTC1.EndPosL	Minimum Tap reached	I	The active tap equals the Minimum Tap setting.
SUP_TAP_REACH		ATCC1.LimTapR	Upper Tap Limit reached	I	The active Tap equals the Upper Tap Limit setting.
INF_TAP_REACH		ATCC1. LimTapL	Lower Tap Limit reached	I	The active Tap equals the Lower Tap Limit setting.
REVERSE_POWER		ATCC1.RvPwrDet	Power Reversal detected	I	90º < Φ < 270º Φ=Angle between VCTRL and ILOCAL
VOLT_OUT_BAND		ATCC1.BndOut	Voltage out of Dead Band	I	|VD| > GI
VM_GT_VD		ATCC1.BndOutR	Voltage over Dead Band	I	|VD| > GI & $V_{REG} > V_D$
VM_LT_VD		ATCC1.BndOutL	Voltage under Dead Band	I	|VD| > GI & $V_{REG} < V_D$

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 2.1-6: Auxiliary Outputs and Events of the Voltage Regulator					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN_BAND_REF	Automatisms	ATCC1.VBndCtr	Voltage in Reference Band		Signals of the Voltage Band Recorder.
IN_BAND_01		ATCC1.VBndO1	Voltage in Upper Band 1		
IN_BAND_02		ATCC1.VBndO2	Voltage in Upper Band 2		
IN_BAND_03		ATCC1.VBndO3	Voltage in Upper Band 3		
IN_BAND_U1		ATCC1 VBndU1	Voltage in Lower Band 1		
IN_BAND_U2		ATCC1 VBndU2	Voltage in Lower Band 2		
IN_BAND_U3		ATCC1.VBndU3	Voltage in Lower Band 3		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

2.1.22 IEC 61850 Logical Node

CLASS ATCC		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Controls		
OpCntRs	INC	Resettable operation counter. Sum of the raise operation counter (NMANIOMBRASSUBIRTOMA) and the lower operation counter (NMANIOMBRASBAJARTOMA). When giving the reset commands both internal counters will reset.
TapChg	BSC	Change tap position digital command
BndCtrChg	BAC	Band centre change in % step values
ParOp	SPC	Parallel/Independent operation. Status Only. It will show if the RTF is in parallel or individual conditions. Status calculated as an OR of PTR2Par, PTR3Par, PTR4Par, PTR5Par
LTCBlk	SPC	Block automatic control
Auto	SPC	Automatic/manual operation
Measured Values		
CtlV	MV	Control Voltage (VREG)
LodA	MV	Load Current
CircA	MV	Circulating Current
PhAng	MV	Phase Angle of LodA relative to CtlV
Status Information		
TapOpR	SPS	Change tap position raise
TapOpL	SPS	Change tap position lower
LTCBlkVlo	SPS	LTC inhibit due to under voltage
LTCBlkAHi	SPS	LTC inhibit due to over current
EndPosR	SPS	End position reached or highest allowed tap position reached
EndPosL	SPS	End position reached or lowest allowed tap position reached
Settings		
BndCtr	ASG	Band center voltage
LDCR	ASG	LDC line resistance component
LDCX	ASG	LDC line reactance component

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings		
RnbkRV	ASG	Runback raise voltage
LimLodA	ASG	Limit load current
LDC	SPG	LDC Z or RX
TmDlChr	SPG	Time delay linear or inverse characteristic
LDCZ	ASG	Line impedance por LDCZ
TapBlkR	ING	Tap position of LTC where automatic raise commands are blocked
TapBlkL	ING	Tap position of LTC where automatic lower commands are blocked
Extended Data		
SptVol	APC	Voltage setpoint analogue command
LDCEna	EXT_SPC	LDC Enable Input
ReacEna	EXT_SPC	Reactive Current Enable Input
BlkVEna	EXT_SPC	Out of Voltage Block Enable Input
PTR2Par	EXT_SPC	Power Transformer 2 in parallel conditions Input
PTR3Par	EXT_SPC	Power Transformer 3 in parallel conditions Input
PTR4Par	EXT_SPC	Power Transformer 4 in parallel conditions Input
PTR5Par	EXT_SPC	Power Transformer 5 in parallel conditions Input
BlkOpManR	EXT_SPC	Manual Raise Tap Operation Blocking Input
BlkOpManL	EXT_SPC	Manual Lower Tap Operation Blocking Input
BlkOpAutR	EXT_SPC	Automatic Raise Tap Operation Blocking Input
BlkOpAutL	EXT_SPC	Automatic Lower Tap Operation Blocking Input
InhDlTm	EXT_SPC	Cancel Time Delay (Immediate Operation) Input
ResTOV	EXT_SPC	Reset Out of Voltage Timer Input
CtlVPct	EXT_MV	Control Voltage in % of VN
LodAPct	EXT_MV	Load Current in % of IN
LodParPct	EXT_MV	Parallel Current in % of IN
ParLoadA	EXT_MV	Parallel Current
ParTotVAr1	EXT_MV	Parallel Transformer 1 Reactive Power
ParTotVAr2	EXT_MV	Parallel Transformer 2 Reactive Power
ParTotVAr3	EXT_MV	Parallel Transformer 3 Reactive Power
ParTotVAr4	EXT_MV	Parallel Transformer 4 Reactive Power
BlkMultTap	EXT_SPS	Simultaneous Tap Blocking
BlkNoTap	EXT_SPS	No Tap Blocking
BlkLimTap	EXT_SPS	Limit Tap Reached
BlkVDlTm	EXT_SPS	Out of Voltage Timer Block
BlkFailTap	EXT_SPS	Tap Failure Command Block
BlkRunAway	EXT_SPS	Block by runaway
LimBndCtr	EXT_SPS	Extreme setpoint
TapOpRFail	EXT_SPS	Tap up command fail
TapOpLFail	EXT_SPS	Tap down command fail
LimTapR	EXT_SPS	Upper tap limit reached
LimTapL	EXT_SPS	Lower tap limit reached
RvPwrDet	EXT_SPS	Power Flow reversal detected
BndOut	EXT_SPS	Voltage out of deadband
BndOutR	EXT_SPS	Voltage over deadband
BndOutL	EXT_SPS	Voltage under deadband

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Extended Data		
VBndCtr	EXT_SPS	Voltage within Band Ref
VBndO1	EXT_SPS	Voltage within Band O1
VBndO2	EXT_SPS	Voltage within Band O2
VBndO3	EXT_SPS	Voltage within Band O3
VBndU1	EXT_SPS	Voltage within Band U1
VBndU2	EXT_SPS	Voltage within Band U2
VBndU3	EXT_SPS	Voltage within Band U3
TapGrd	EXT_SPG	Tap Changer Monitor
TapInTyp	EXT_ENG	Tap Condification Type
UnitsDisp	EXT_ENG	Units in Main Display
VCtlTyp	EXT_ENG	Voltage Type
ALocTyp	EXT_ENG	Local Current Type
AParTyp	EXT_ENG	Parallel Current Type
CtrVar	EXT_ENG	Control Voltage Source
TapOutTyp	EXT_ENG	Tap Outputs Type
TapPlsTmms	EXT_ASG	Pulse Output Time
BndCtrVal1	EXT_ASG	Setpoint Value 1
BndCtrVal2	EXT_ASG	Setpoint Value 2
BndCtrVal3	EXT_ASG	Setpoint Value 3
BndCtrVal4	EXT_ASG	Setpoint Value 4
BndCtrVal5	EXT_ASG	Setpoint Value 5
BndCtrSel	EXT_INC	Setpoint Selection Value Command
BndCtrInc	EXT_ING	Setpoint Increment
BndWid	EXT_ASG	Deadband
TapVRl	EXT_ENG	Tap/Voltage Relation
TmMult	EXT_ASG	Inverse Curve Time Factor
DlTmmsT1	EXT_ASG	Definite Time T1
DlTmmsT2	EXT_ASG	Definite Time T2
LDCTyp	EXT_ENG	Type of LDC
ReacComEna	EXT_SPG	Circulating Current Enable
ReacComSrc	EXT_ENG	Parallel Trf Source
MaxComp	EXT_ASG	Max Compensation Limit
Imp1	EXT_ASG	Impedance local transformer
Imp2	EXT_ASG	Impedance parallel transformer 1
Imp3	EXT_ASG	Impedance parallel transformer 2
Imp4	EXT_ASG	Impedance parallel transformer 3
Imp5	EXT_ASG	Impedance parallel transformer 4
BlkUnCtlV	EXT_ASG	Under Voltage
BlkUnVTmms	EXT_ASG	Under Voltage Timer
VBlkDlTmms	EXT_ASG	Time for Out of Voltage
TapNum	EXT_ING	Number of taps
MinTap	EXT_ING	Minimum tap value
FailOpTmms	EXT_ASG	Operation Failure Time
SimTapTmms	EXT_ASG	Max Simultaneous Time
NoTapTmms	EXT_ASG	Max Time Without Tap
ExtResist	EXT_SPG	External Resistor
LimVBndR3	EXT_ASG	Voltage Band O3 Limit
LimVBndR2	EXT_ASG	Voltage Band O2 Limit

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Extended Data		
LimVBndR1	EXT_ASG	Voltage Band O1 Limit
LimVBndL1	EXT_ASG	Voltage Band U1 Limit
LimVBndL2	EXT_ASG	Voltage Band U2 Limit
LimVBndL3	EXT_ASG	Voltage Band U3 Limit

CLASS YLTC		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Controls		
TapChg	BSC	Change tap position digital command. Same as ATCC1.TapChg
Status Information		
OpCnt	INS	Operation counter. Sum of the raise operation counter (NMANIOMBRASSUBIRTOMA) and the lower operation counter (NMANIOMBRASBAJARTOMA). Equal to ATCC1.OpCntRs but without reset command.
EndPosR	SPS	End position reached or highest allowed tap position reached. Same as ATCC.
EndPosL	SPS	End position reached or lowest allowed tap position reached. Same as ATCC.

2.1.23 ATCC IEC 61850 Control Commands

Commands:

- APC (ATCC1.SptVol): Analogue command over the control variable (setpoint). Controllable analogue process value. Write the setpoint voltage value in primary values.
- BSC (ATCC1.TapChg): Digital command over the taps. Binary controlled step position information. Tap up/down commands.
- BAC (ATCC1.BndCtrChg): Digital command over the setpoint. Binary controlled analogue process value. Rise/lower setpoint digital commands.

None of the above commands will need a control configuration to work. The device will check the commands hierarchy and therefore will accept the command taking into account the control status (local/panel controlled/remote/etc.)

- SptVol:
  - Status: VD (setpoint). Active setpoint in primary voltage values.
  - The IED will accept commands whose new value falls within the allowed range (max/min value of the setpoint in primary values).
  - Commands whose new value falls outside the allowed range (max/min value of the setpoint in primary values) will be refused with AddCause inconsistent parameters.
- TapChg:
  - Status: current tap position value.
  - The IED will execute a tap up/down command when the corresponding command arrives.
  - Tap up / down commands will be refused with AddCause Step-limit when the tap value is in the maximum/minimum value.
  - Tap up / down commands will be refused with AddCause Blocked-by-process when the manual tap up/down commands are in blocked status according to those internal signals.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- BndCtrChg:
  - Status: VD (setpoint). Active setpoint in percentage.
  - The setpoint value will be incremented/decremented according to the percentage defined in the Setpoint increment setting (1% a 6%).
  - Rise up / down commands will be refused with AddCause Step-limit when the setpoint value is in the maximum/minimum value.

2.1.24 Voltage Regulator Test

- **Measurement Test**

Measurements are shown in engineering units (V or A) and in percentage (%) of the rated value and are displayed in:

- The default screen.
- The Cyclic Menu (pressing the front F2 key).
- The information menu >> Measurements.
- The ***ZivercomPlus***® (State >> Measurements).

The steps to carry out the metering test are:

- Set **Voltage**, **Frequency** and **Rated Currents** (Settings>> Rated Values):
  - Rated VABC: 115 V
  - Rated Freq: 50 Hz
  - Rated Local I.: 5 A
  - Rated Parallel I.: 5 A

- Set **Transformer Ratios** (Settings>> General):
  - Transformer Ratio V.T. Phase: 1
  - Transformer Ratio C.T. Local: 1
  - Transformer Ratio C.T. Parallel: 1

- Voltage Type: VA.
- Local Current Type: IA.
- Parallel Current Type: IA.
- Apply a voltage, close to the rated voltage, between voltage input terminals.
- Apply a current, close to the rated current, between local current terminals.
- Apply a current, close to the rated current, between parallel current terminals.

Voltage Measurement

Apply the voltage shown in following Table between voltage input terminals:

Table 2.1-7: Voltage Measurement Test

Applied Voltage	Measured value (%)	Measured value (secondary)
x Vac	$(\frac{x}{V_n}\cdot 100 \pm \frac{x}{V_n}\cdot 0.5)\%$	**x** $\pm$ 0.005**x** Vac

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Local and Parallel Current Measurement

Apply the current shown in following Table between local current input terminals and check measurements. Repeat the test applying current between parallel current terminals and check measurements.

Table 2.1-8: Local and Parallel Current Measurement Test		
Applied Current	**Measured Value (%)**	**Measured value (secondary)**
x Aac	$(\frac{x}{I_n}\cdot 100 \pm \frac{x}{I_n}\cdot 0.5)\%$	**x** $\pm$ 0.005**x** Aac

Angle Measurement

The angles shown in the HMI and the ***ZivercomPlus***® are the angles of the currents with respect to the voltage phasor, which is taken as reference for angles, measured **counterclockwise**.

If the voltage does not exceed a certain threshold (around 1 V), a reference for angles will not exist, and these will appear as invalid values.

Circulating Current Measurement

- Apply a voltage in order to have a reference for angles.
- Apply a current in ILOC.
- Apply a current IPAR.
- Formula for calculating $\mathbf{I_{circulating}}$

$$I_{circ} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - I_2^m \cdot RT_{CT2} \cdot \text{sen}\,\varphi_2}{2}$$

In the calculation of $\mathbf{I_{Circulating}}$ Transformer Ratios (RT_{Local} and $RT_{Parallel}$) are involved, so that units are **Primary Amps**. As can be seen in the above formula, the sign of the circulating current $\mathbf{I_{Circulating}}$ can be either positive or negative.

The angles in the following table appear in the ***ZivercomPlus***® or the HMI.

Table 2.1-9: Circulating Current Measurement Test				
$\mathbf{I_{Local}}$	φ_L (º)	$\mathbf{I_{Parallel}}$	φ_P (º)	- $I_{Circulating}$ (A)
5	30º	0	0	

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Regulator Operation Test**

There is no need for applying any current or voltage during this test. Configuring the correct DIs with the input signals to the automatism is necessary.

The following steps are needed for testing the regulator operation:

- Apply a pulse (>200 ms) to an input configured as **Switch to Automatic** and check that the relay switches to **Automatic Mode**, that is, the corresponding outputs and LEDs activate.
- Apply a pulse (>200 ms) to the input configured as **Switch to Manual** and check that the relay switches to **Manual Mode**, that is, the corresponding outputs and LEDs activate.
- Repeat the test by sending **Switch to Automatic** and **Switch to Manual** commands through the communications system.

  Leave the regulator in **Manual Mode** for the rest of the test.

- Apply a pulse (>200 ms) to an input configured as **Raise the Tap Command** and check that the relay activates the corresponding outputs and LEDs during the set time.
- Apply a pulse (>200 ms) to an input configured as **Lower the Tap Command** and check that the relay activates the corresponding outputs and LEDs during the set time.

For models with tap monitoring and signaling, this operation can be executed two times, that is, if after the tap change command the tap change fail timer times out with no tap change, the Raise/Lower the Tap LED lights again for three seconds. If the tap change fail timer times out (from the time when the LED is lit) again with no tap change, the relay switches to internal anomaly blocking and to manual state.

For models with no tap monitoring, the **Raise / Lower the Tap** command can be given an indefinite number of times until the voltage is within the range. The time lapse between commands is the delay time when the Runback Voltage has not been exceeded. In case said voltage is exceeded, the first command would be given immediately and the time between consecutive commands is 12 seconds.

- **Insensitivity Degree (GI)**

No configuration is needed for this test.

The steps to be followed are:

- Set ***Rated Voltage*** to 115 V (Settings>> Rated Values>> Rated Voltage ABC).
- Apply a voltage $\mathbf{V_{CTRL}}$ (close to rated voltage). No current is needed to be applied, but in case there is any current applied, set ***Line Drop Compensation Enable*** and ***Reactive Compensation Enable*** to **NO**.
- Set ***Voltage Set-point*** to 100% (Settings>> Voltage Regulator >> Regulation Control >> Set-point).
- Set ***Insensitivity Degree*** to 1% (Settings>> Voltage Regulator >> Regulation Control >> Insensitivity).
- Set ***Tap/Voltage Ratio*** to Direct (Settings>> Voltage Regulator >> Regulation Control >> Tap/Voltage ratio).
- Check the deviation value by means of the formula below, where V_D is the set ***Voltage Set-point*** value:

$$\mathbf{DV\ (\%) = V_D\ (\%) - V_{CTRL}\ (\%)}$$

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Check that:

- If the absolute value of the calculated deviation **|DV|** is smaller than the set insensitivity degree **GI**, the voltage is **within the range**, and the default screen shows: **DESV** □ .
- If, on the contrary, the absolute value of the deviation **|DV|** is greater than the insensitivity degree **GI**, the voltage is **outside the range**, and the default screen shows **DESV** ■ .
- Check that the sign of the deviation generates adequate tap change commands, that is, if the measured voltage is greater than the voltage set-point value, the **Lower the Tap** (**LOWER contacts**) output is activated. On the contrary, if the measured voltage is smaller than the voltage set-point value, the **Raise the Tap** (**RAISE contacts**) output is activated. This can be seen on the default screen: **DESV** ■ ↑ o **DESV** ■ ↓ .
- Repeat the test switching the **Tap / Voltage Ratio** setting to Inverse, checking that the sign of the deviation generates adequate tap change commands, that is, if the measured voltage is greater than the voltage set-point value, the **Raise the Tap** (**RAISE contacts**) output is activated. On the contrary, if the measured voltage is smaller than the voltage set-point value, the **Lower the Tap** (**LOWER contacts**) output is activated
- Check the default screen and the generated events

Bear in mind that the accuracy of voltage measurement is ±0.1%.

- **Line Drop Compensation LDC-Z**

No configuration is needed for this test.

The steps to be followed are:

- Set **Rated Voltage** to 100 V (Settings>> Rated Values>> Rated Voltage ABC).
- Set ***Local Rated Current*** to 5 A (Settings>> Rated Values >> Local Rated I).
- Apply a voltage (close to rated voltage) in order to have a reference for angles (100 ∠ 0º).
- Apply a local current.
- Set ***Line Drop Compensation Enable*** setting to: YES.
- Set ***Line Drop Compensation Type*** to*:* Z Type.
- Set ***Voltage Set-point*** V_D to 100% (Settings>> Voltage Regulator >> Regulation Control>> Set-point).
- Set ***Maximum Compensation*** to 15%.
- Disable any other type of compensation (***Reactive Compensation***).
- Set ***Line Drop Compensation Z*** (LDC-Z *)* to 10%.

Calculate the **Compensated Voltage V_{COMP}** through the formula:

$$V_{DCOMP}\ (\%) = V_D\ (\%) + K_C\ (\%) \cdot I_{pu}\ ,$$

where I_{pu} = Per unit Current (that is, I_{LOCAL} / $I_{nominal}$).

Table 2.1-10: Line Drop Compensation LDC-Z Test

V_D (%)	LDC-Z or K_C (%)	I_{LOCAL} (A)	I_{pu}	V_{DCOMP} (%)
100 %	10 %	1 A	0.2	102 %
100 %	10 %	2 A	0.4	104 %
100 %	10 %	3 A	0.6	106 %
100 %	10 %	4 A	0.8	108 %
100 %	10 %	5 A	1.0	110 %

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- Check **Deviation Value** through the following formula, where $\mathbf{V_{COMP}}$ is the value calculated above:

$$\mathbf{DV\ (\%) = V_{DCOMP}\ (\%) - V_{CTRL}\ (\%)}$$

- **Line Drop Compensation LDC R-X**

  - Set ***Line Drop Compensation Type*** to*:* R-X Type instead of Z Type.

Calculate the **Compensated Voltage V_{COMP}** through the formula:

$$\mathbf{V_{DCOMP} = V_D + LDC\text{-}R \cdot I_{pu} \cdot Cos\ (360 - \Phi_L) + LDC\text{-}X \cdot I_{pu} \cdot Sin\ (360 - \Phi_L)}$$

where $\mathbf{I_{pu}}$ = Per unit Current (that is, $\mathbf{I_{LOCAL}}$ / $\mathbf{I_{nominal}}$).

Table 2.1-11: Line Drop Compensation LDC R-X Test

V_D (%)	VN	IN	LDC-R (V)	LDC-X (V)	I_{LOC} (A)	V_{DCOMP}
100	110	5	1	-5	5 ∟0º	111.1V (101%)
100	110	5	1	-5	5 ∟30º	113.70V (103.37%)
100	110	5	1	-5	5 ∟45º	114.77V (104.24%)
100	110	5	1	-5	2.35 ∟125º	111.821V (101.66%)
100	110	5	1	-5	2.81 ∟310º	108.0295V (92.21%)
80	100	5	5	2	2∟45º	80.849V (80.85%)
100	100	5	1	3	3∟280º	101.877V (101.88%)
110	100	5	5	5	4∟330º	115.464V (115.46%)
110	100	5	5	-15	4∟330º	107.464V (107.46%)
90	110	5	10	-20	2.3 ∟245º	87.689V (79.72%)
90	110	5	10	-30	2.3 ∟245º	83.104V (75.549%)
90	110	5	30	-30	2.3 ∟245º	78V (71%) => 75%

- **Reactive Compensation with Wired Currents**

The steps to be followed for the **Reactive Compensation** test are:

- Apply voltage, close to rated voltage, in order to have a reference for angles.
- Apply a current $\mathbf{I_{LOCAL}}$.
- Apply a current $\mathbf{I_{PARALLEL}}$.
- Set following settings (Voltage Regulator >> Compensation):

Reactive Compensation Enable: YES
X1: 25%
X2: 25%
Maximum Compensation: 15%

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

All other settings must remain at default values.

- Calculate **Circulating Reactive Current $I_{circulating}$** through the formula:

$$I_{circ} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 - I_2^m \cdot RT_{CT2} \cdot \text{sen}\,\varphi_2}{2}$$

$$K_R^{(\%)} = \frac{X_1^{(\%)} + X_2^{(\%)}}{10}$$

- Calculate **Compensated Voltage V_{DCOMP}** through the formula:

$$V_{DCOMP}\,(\%) = V_D\,(\%) + K_R\,(\%) \cdot (I_{CIRC} / 0{,}1 \cdot I_n)$$

- Calculate **Deviation DV** through the formula:

$$DV\,(\%) = V_{DCOMP}\,(\%) - V_{CTRL}\,(\%)$$

- Check that if the calculated deviation is below the set insensitivity degree, the voltage is **within the range**. If, on the contrary, the deviation is above the insensitivity degree, the voltage is **outside the range**.
- Check that, since there is no parallel transformer, the **Reactive Compensation** effect disappears, that is: **V_{DCOMP} (%) = V_D (%)**
- Check that as long as **$I_{LOCAL} \angle \varphi_L = I_{PARALLEL} \angle \varphi_P$**, then **$V_{DCOMP}$ (%) = V_D (%)** also.

Table 2.1-12: Reactive Compensation through Wiring Test

V_D (%)	$I_{LOCAL} \angle \varphi_L$	$I_{PARALLEL} \angle \varphi_P$	I_{CIRC}	V_{COMP} (%)
100 %	1 \330º	1 \0º	- 0.25	97.5
100 %	1 \0º	1 \330º	0.25	102.5
100 %	1 \330º	1 \330º	0	100
100 %	5 \330º	5 \330º	0	100
100 %	1 \330º	1 \120º	- 0.683	93.17
100 %	1 \330º	1 \90º	- 0.75	92.5
100 %	2 \0º	2 \30º	-0.5	95
100 %	2 \30º	2 \0º	0.5	105
100 %	1.3 \20º	2.8 \25º	-0.36935	96.3065
100 %	3.6 \70º	2.1 \40º	1.0165	110.165
100 %	2.25 \160º	2.31 \173º	0.244	102.44

- **Reactive Compensation through Communications**

Below are the steps to be followed for the **Reactive Compensation** test:

- Load a CID or a configuration to each relay that include the logic input **EXIST_TRF_PARAL_1 (Parallel Transformer 1)** and the analog input **VAR T1 PARALELO (receipt of the reactive power measured by the other RTF)**.
- Communicate both IEDs or simulate the reception of the information in the **RTF**.
- Apply voltage, close to the nominal value, in order to have angle reference.
- Apply a current **I_{LOCAL}**.
- Set the following settings (Voltage regulator >> Compensation):

Reactive compensation enable:	YES
X1:	4.03%
X2:	3.85%
Maximum compensation:	15%
Parallel transformer data source	Communications

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

All other settings must remain at default values.

- The **Circulating reactive current I_{CIRC}** is calculated by the formula:

$$I_{circ12} = \frac{I_1^m \cdot RT_{CT1} \cdot \text{sen}\,\varphi_1 + \left(\frac{Q_2^m}{3 \cdot V_1^m \cdot RT_{VT1}} \right)}{2}$$

$$I_{circ} = I_{circ12}$$

$$K_R = \frac{X_1(\%) + X_2(\%)}{10} = 0,788$$

- The **Compensated voltage V_{DCOMP}** is calculated by the formula:

$$V_{DCOMP}(\%) = V_D(\%) + K_R(\%) \cdot (I_{CIRC} / 0,1 \cdot I_n)$$

Table 2.1-1:Reactive Compensation Test through Communications							
$I_{RTF1}\angle\varphi_L$	$I_{RTF2}\angle\varphi_P$	Q_{RTF1}	Q_{RTF2}	$I_{CIRC}1$	$I_{CIRC}2$	V_{DCOMP} (%)1	V_{DCOMP} (%)2
1∠330º	1∠0º	172.5	0	-0.25	0.25	99.606	100.394%
1∠0º	1∠330º	0	172.5	0.25	-0.25	100.394	99.606%
1∠330º	1∠330º	172.5	172.5	0	0	100	100%
5∠330º	5∠330º	862.5	862.5	0	0	100	100%
1∠330º	1∠120º	172.5	-298.77	- 0.683	0.683	98.9236	100.076%
1∠330º	1∠90º	172.5	-345	- 0.75	0.75	98.818	101.182%

- **Delay Time**

In order to carry out this test, the regulator must be configurated to switch the relay to **Automatic Mode** and to configure **CANCEL_T1** input (Cancel Timer T_1).

Apart from loading said configuration the steps below must be followed:

- Apply voltage close to rated voltage.
- No current must be applied.
- Set all settings to default values.

In this test, the time elapsed from the time the voltage comes out of the regulation range until the Raise/Lower the Tap command is given is measured, checking the operation of the contacts marked on the backside sticker as **RAISE** and **LOWER**.

Calculate the **Delay Time**, according to the inverse curve, through the following expression:

$$T_{curva} = \frac{FT \cdot 30 \cdot GI}{|DV|}$$

For example, if default settings are considered:

V_D = 100% GI = 3% FT = 10 s Runback Voltage = 110%

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- Starting from a situation where the voltage is **within the range**, 90% voltage is applied. The theoretical time obtained through the above formula is 90 seconds, after which the operation of the **RAISE** contacts is checked. In this situation, the next commands must be activated after the ***Definite Time T_2*** setting value (10 seconds after the reposition of the previous tap command).
- Starting from a situation where the voltage is **within the range**, 110% voltage is applied. The theoretical time obtained through the above formula is 90 seconds, after which the operation of the **LOWER** contacts is checked. In this situation, the next commands must be activated after the **Definite Time T_2** setting value (10 seconds after the reposition of the previous tap command).
- Repeat the test for FT = 1s and bear in mind that for the ***T_{curve}*** values obtained from the above formula smaller than ***$T_{definido1}$***, ***$T_{definido1}$*** shall be used. Refer to summary table in section 2.1.5.b Time for following operations: T_2.
- Repeat the test for ***First Operation Curve Type*** setting: Definite Time.
- Starting from a situation where the voltage is **within the range**, activate the input configured as **Cancel Timer** and apply a voltage **outside the range**. Check that the operation time is between 0.5 s and 1.5 s.
- Similarly, starting from a situation where the voltage is **within the range** apply a voltage above the ***Runback Voltage*** setting value and measure the time elapsed until the tap change command is given. This time must be between 0.5 s and 1.5 s.

In both cases, **Cancel Timer** and ***Runback Voltage***, the first tap change command is sent immediately, and following commands, if required, are sent after **T_2**, after the reposition of the previous tap command, no matter the calculated ***Delay Time***.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Chapter 3.

Voltage and Frequency Protection Units

3.1 Voltage Elements

3.1.1	Common Principles	3.1-2
3.1.1.a	Operation and Reset	3.1-2
3.1.1.b	Trip Blocking	3.1-2
3.1.1.c	Enabling and Disabling the Unit	3.1-2
3.1.1.d	Restoration Settings	3.1-2
3.1.1.e	Logical Node: Common Characteristics (Voltage Elements Reset Settings)	3.1-2
3.1.2	Phase Overvoltage Elements	3.1-3
3.1.2.a	Identification	3.1-3
3.1.2.b	General Block	3.1-3
3.1.2.c	Operation Principles and Block Diagram	3.1-3
3.1.2.d	Application	3.1-5
3.1.2.e	Setting Ranges	3.1-5
3.1.2.f	Analog Inputs to the Unit	3.1-5
3.1.2.g	Digital Inputs to the Phase Overvoltage Unit	3.1-6
3.1.2.h	Auxiliary Outputs and Events of the Phase Overvoltage Modules	3.1-7
3.1.2.i	IEC 61850 Logical Node	3.1-8
3.1.2.j	Protection Element Test	3.1-8

Voltage Protection Elements		
1	Phase Overvoltage Element	**59-1**

3.1.1 Common Principles

3.1.1.a Operation and Reset

For a given voltage unit, pickup occurs when the measured value is equal to or greater / less than the set value, and the resets with a selectable percentage value (lower than 99%) on the setting.

3.1.1.b Trip Blocking

Voltage Elements can program block trip inputs, which prevents the operation of the element if this input is activated before the trip is generated. If activated after the trip, it resets. Even if the element is blocked it remains operative so that if the relay is under trip conditions at the moment when the blocking input deactivates, the relay will issued a trip command instantaneously.

To be able to use these logic input signals, it is necessary to program the status contact inputs defined as **Block Trip**.

3.1.1.c Enabling and Disabling the Unit

All elements include an enable and disable input in such a way that, the element being enabled by protection settings, it may be disabled through logic upon given circumstances. In this way, when the enable input is disabled, the element is not operative and the element starts operation from zero the moment the enable input is activated.

3.1.1.d Restoration Settings

The reset value of each set of voltage elements is settable and one setting per set is provided to this end.

Protection / Voltage / Voltage Restoration					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Phase UV reset	`Ph OV Reset`	PVCF1.PhUnVRs	101-150%	1	105%

3.1.1.e Logical Node: Common Characteristics (Voltage Elements Reset Settings)

CLASS PVCF		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Settings		
PhUnVRs	ASG	Phase undervoltage reset

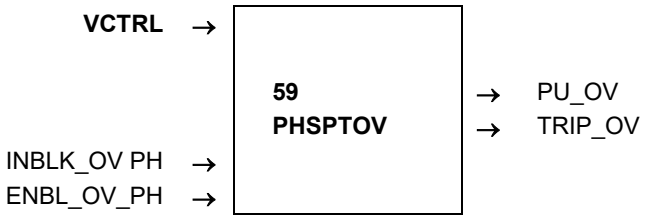
© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.1.2 Phase Overvoltage Elements

3.1.2.a Identification

Description of the Protection Unit	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Phase Overvoltage Unit 1	PHSPTOV1	3U>	59-1

3.1.2.b General Block



3.1.2.c Operation Principles and Block Diagram

Pickup occurs for a given overvoltage element when the value measured is equal to or greater than one times the set value, and resets at a selectable percentage (less) over the setting.

The overvoltage element pickup enables the timing function. This is done by applying increments on a meter that picks up the element when it times out. The time setting included allows selecting a ***Fixed Time*** or ***Inverse Curve*** timing sequence.

When the RMS falls below the pickup setting, a rapid reset of the integrator occurs. The activation of the output requires the pickup to continue operating throughout the integration. Any reset leads the integrator to its initial conditions so that a new operation initiates the time count from zero.

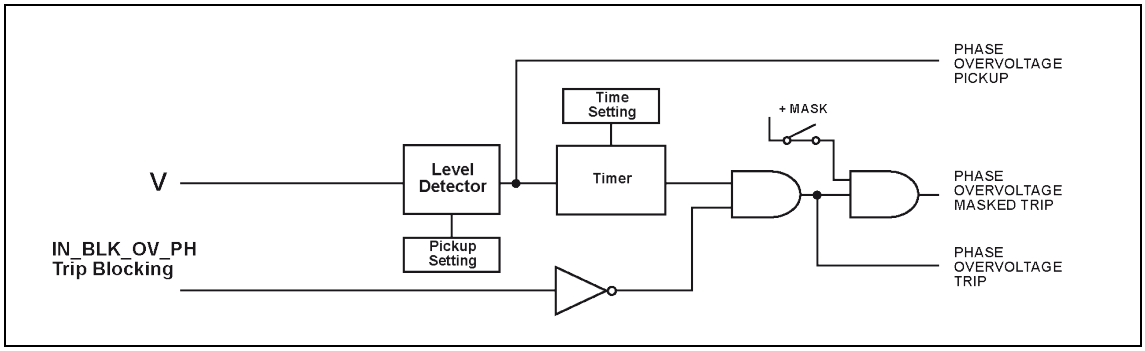


Figure 3.1.1 Block Diagram of the Phase Overvoltage Element.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

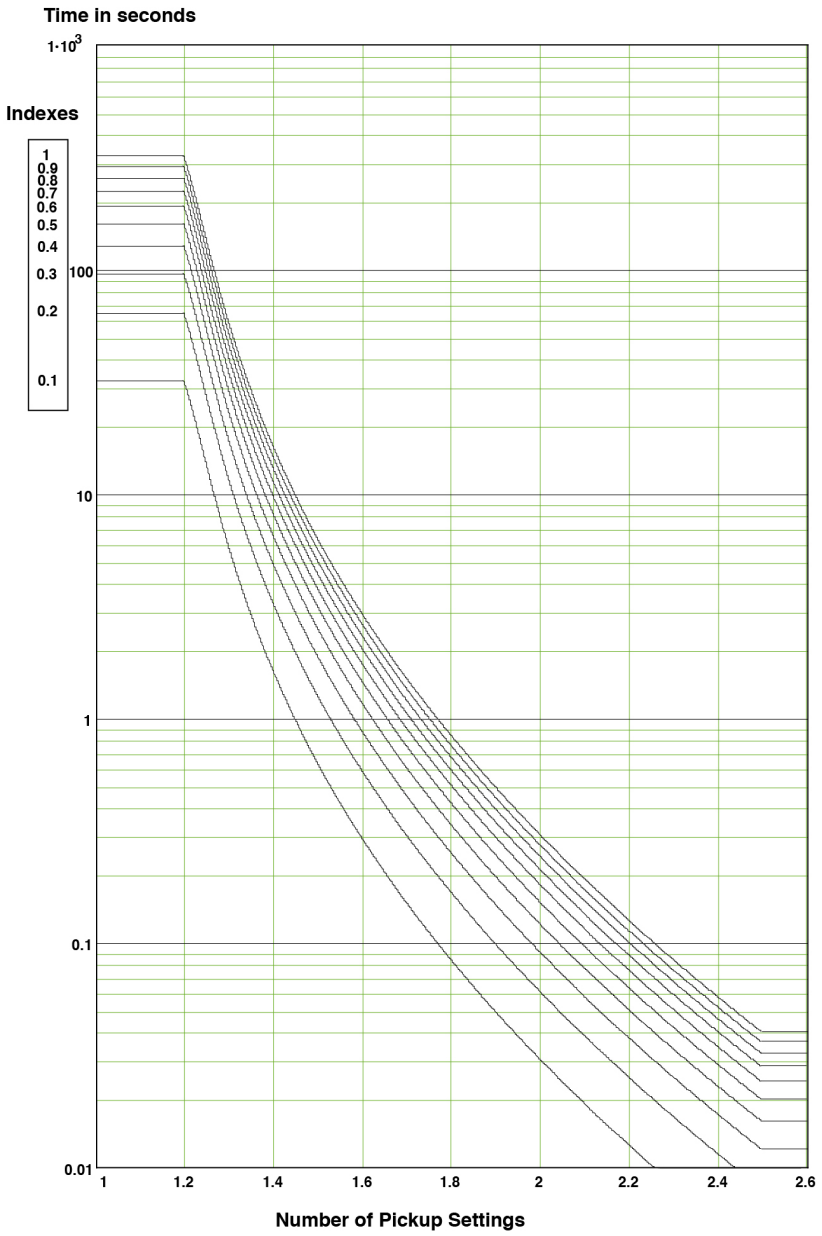


Figure 3.1.2 Inverse Curve with Values Truncated at 1.23 Times.

$$T(s) := \left[\frac{1.372 \cdot 10^{13}}{\left[1.323 \cdot 10^{3} \cdot (x-1) - 0.5\right]^{4.385}} + 0.099 \right] \cdot Dial$$

Where X = Vinjected/Setting

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.1.2.d Application

The Phase Overvoltage Element detects overvoltage conditions in power equipment such as generators, transformers, transmission and distribution lines, motors, etc. that can cause insulation damage in the protected equipment. These overvoltage conditions can be caused by different factors such as:

- Voltage drop not compensated by regulators.
- Bad operation of voltage regulators.
- Phase overvoltage derived from ground faults, even through the system should be designed to support them.
- Sudden voltage drop due to line bay trips.

In this way, the phase overvoltage element can be used to disconnect from the network any equipment that could be damaged when working under high voltage conditions.

3.1.2.e Setting Ranges

Metering / Voltage / Phase Overvoltage					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Phase OV Enable	Ph. OV Enable	PHSPTOV.LNInSvc	NO / YES		NO
Phase OV Pickup	Ph. OV Pickup	PHSPTOV.StrVal	2-300 V	0.01 V	70 V
Phase OV Curve	Ph. OV Curve	PHSPTOV.TmVCrv	Definite Time Inverse		Definite Time
Phase OV Dial	PH. OV Dial	PHSPTOV.TmMult	0.05-1	0.01	1
Phase OV Delay	Ph. OV Delay	PHSPTOV.OpDlTmms	0-300 s	0.01 s	0 s

3.1.2.f Analog Inputs to the Unit

The operating magnitude of the Phase Overvoltage Elements will be VA, VB and VC voltage.

Table 3.1-1: Analog Inputs of the Phase Overvoltage Modules		
Name	**Description**	**IEC 61850**
VCTRL	Wired input voltage	MMXU.VCtrl

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.1.2.g Digital Inputs to the Phase Overvoltage Unit

Table 3.1-2: Digital Inputs to the Phase Overvoltage Modules					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN_BLK_OV1_PH	Logic Inputs to Protection	PHSPTOV1.Mod	Block Phase Overvoltage Unit 1	I	Activation of the input before the trip is generated prevents the element from operating. If activated after the trip, it resets.
ENBL_OV_PH1	Enabling Commands	PHSPTOV1.Mod	Enable Phase Overvoltage Unit 1	I	Activation of this input puts the unit into service. It can be assigned to status contact inputs by level or to a command from the communications protocol or from the HMI. The default value of this logic input signal is a “1.”

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.1.2.h Auxiliary Outputs and Events of the Phase Overvoltage Modules

Table 3.1-3: Auxiliary Outputs and Events of the Phase Overvoltage Modules

Name	Group	IEC 61850	Description	Vis.	Function
PU_OV1_A	Pickup Protection Outputs	PHSPTOV1.Str	Overvoltage Unit 1 Pick Up	I	Pickup of the overvoltage elements and start of the time count.
TRIP_OV1_A	Trip Protection Outputs	PHSPTOV1.Op	Overvoltage Unit 1 Trip	I	Trip of the overvoltage elements.
ENBL_OV_PH1	Units enabled Protection Outputs	PHSPTOV1.Mod	Three Phase Overvoltage Unit 1 enable	I	Indication of enabled or disabled status of the Three Phase Overvoltage elements.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.1.2.i IEC 61850 Logical Node

CLASS PHSPTOV		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
Str	ACD	Pickup
Op	ACT	Trip
Settings		
StrVal	ASG	Start value
TmVCrv	CURVE	Operating Curve characteristic
TmMult	ASG	Time Dial Multiplier
OpDlTmms	ING	Delay time
Extended Data		
LNInSvc	EXT_SPG	In service

3.1.2.j Protection Element Test

IEDs have one phase overvoltage unit (59-1) and it is possible to select between ***Line Voltage*** or ***Phase Voltage*** voltage to set the pickups of the phase units.

- **Pickup and Reset**

The desired pickup values for the relevant unit are set and their activation is checked by operating any output configured for this purpose. This can also be verified by checking the pickup flags of the menu, **Information** - **Status** - **Units**. This verification can also be made by checking that the trip flag of this menu is activated if the unit trips.

Table 3.1-4: Pickup and Reset of the Overvoltage Elements

Setting of the unit	Pickup		Reset	
X	Maximum	Minimum	Maximum	Minimum
	1.03 x X	0.97 x X	(RST setting + 0.03) x X	(RST setting - 0.03) x X

Where the value “RST setting” corresponds to the setting in per unit of the **Unit Reset** for the overvoltage elements.

- **Operating Times**

To verify the operating times use an output configured with the trip signal of the unit.

Fixed Time or Instantaneous

The pickup setting is increased 20%. Operating time should be the selected time setting ±1% or ±32 ms (for 50Hz). A setting of 0 ms will have an operating time between 20 and 32 ms (for 50Hz) or between 15 and 28 ms (for 60Hz).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2 Frequency Elements

3.2.1	Common Principles	3.2-2
3.2.1.a	Frequency Measurement	3.2-2
3.2.1.b	Adaptation of the Sampling Frequency to the Network Frequency	3.2-3
3.2.1.c	Operation and Reset	3.2-3
3.2.1.d	Elements Blocking Logic	3.2-4
3.2.1.e	Enabling and Disabling the Element	3.2-4
3.2.1.f	Undervoltage Element for Blocking	3.2-4
3.2.1.g	Common Settings	3.2-5
3.2.1.h	Setting Ranges	3.2-6
3.2.1.i	IEC 61850 Logical Node	3.2-6
3.2.1.j	Protection Element Test	3.2-7
3.2.1.k	Application	3.2-8
3.2.2	Underfrequency Elements	3.2-10
3.2.2.a	Identification	3.2-10
3.2.2.b	General Block	3.2-10
3.2.2.c	Operation Principles	3.2-10
3.2.2.d	Setting Ranges	3.2-10
3.2.2.e	Analog Inputs to the Unit	3.2-11
3.2.2.f	Digital Inputs to the Underfrequency Modules	3.2-11
3.2.2.g	Auxiliary Outputs and Events of the Underfrequency Modules	3.2-12
3.2.2.h	IEC 61850 Logical Node	3.2-13
3.2.2.i	Protection Element Test	3.2-13

Frequency Protection Elements		
1	Underfrequency Element	**81m1**

3.2.1 Common Principles

3.2.1.a Frequency Measurement

Relays include a frequency measurement module that detects voltage wave zero crossing and computes the time between crossings. This module uses the instantaneous voltage values obtained with a frequency of **4800 Hz**.

In order to prevent the zero crossing detection from being distorted by harmonics voltage magnitude is processed by a digital band pass filter before computing the time between zero crossings.

In order to validate the frequency measurement, the instantaneous value of the voltage must be above the setting ***Inhibit Voltage*** during 6 consecutive zero crossings or the RMS value of the positive sequence voltage must be above this setting also during 6 zero crossings if the setting ***RMS Supervision*** is set to ***Yes***. Similarly, the calculated frequency must be within the range 15 - 80 Hz and the difference between a frequency measurement and the immediately preceding measurement must not exceed a maximum threshold.

When the frequency module changes from measuring a valid frequency value to measuring an invalid value, the module keeps the last valid frequency measured during a period of 2 s. When this time lapses, if the frequency measurement is still valid, the module will consider the rated frequency.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.1.b Adaptation of the Sampling Frequency to the Network Frequency

The devices include a PLL (*Phase Locked Loop*) module that automatically adapts the sampling frequency to the network frequency, varying the time between samples, to ensure that the DFT (*Discrete Fourier Transform*) calculation window comprises exactly one network cycle. If this adaptation should not take place, said window would not comprise one periodic wave, which will result in DFT measurement errors. These errors will be greater as the deviation between the window time and the period of the sampled wave is also greater.

The PLL module controls the resampling made on the A/D converter fixed output wave frequency (4800 Hz) to obtain a variable sampling frequency of 80 samples / cycle. The PLL operation includes a number of checks that allow discerning phase frequency changes produced by faults or sudden load changes.

PLL operation range is 15 to 80 Hz.

The PLL module includes a setting ***Enable*** that is set to **YES** by default.

3.2.1.c Operation and Reset

All the elements have a time module that can be set to instantaneous. It has the following settings: ***Pickup*** and ***Time Delay***.

Associated with the level detection block, there is a setting for the pickup value: if the element is the Overfrequency element, and the value measured exceeds the setting value a given quantity, the element picks up; if it is the Underfrequency element, it picks up whether or not the value measured is less than the setting value a given quantity.

Activation of the pickup enables the timing function. This is done by applying increments on a meter that picks up the element when it times out.

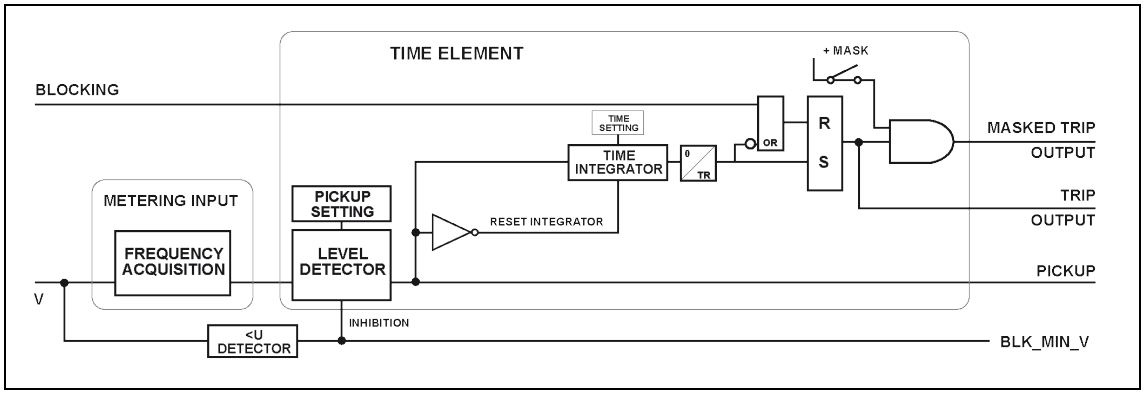


Figure 3.2.1 Block Diagram of a Frequency Element.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.1.d Elements Blocking Logic

Each of the Frequency elements has a **Blocking Logic Input**. Activating this input prevents the activation of the output of the corresponding Frequency element, as shown in Figure 3.2.1.

These logic input signals can be associated to the relay's status contact inputs by configuring the input settings.

3.2.1.e Enabling and Disabling the Element

All the elements have a disabling counter. This counter, of approximately 50 milliseconds, operates when, while the element is tripped, the function is deactivated either by the inhibition voltage, by setting or because the breaker opens.

3.2.1.f Undervoltage Element for Blocking

This element supervises the functioning of the Frequency elements, impeding their operation for measured voltage below the set value.

Voltages compared to the setting ***Inhibit Voltage*** are:

- Instantaneous value of the voltage.
- RMS value of the voltage positive sequence component if the setting ***RMS Supervision*** is set to ***YES***.

Disabling the frequency element operation when the voltage is below a given threshold prevents it from operating in fault situations (as a result of phase changes and frequency measurement errors); also in motor feedback situations when, with absence of network voltage, motors provide voltage because of inertia. This latter voltage will have e decreasing frequency, which could cause the operation of underfrequency elements. As the voltage provided by motors is small, the minimum voltage element will block the operation of frequency elements.

The element picks up when the measured voltage value coincides with or is less than the pickup value (100% of the setting), and resets with a value greater than or equal to 105% of the setting, provided this condition is maintained for at least 6 consecutive half-cycles. These 6 verification half-cycles provide assurance that the voltage is stable.

In any case, the relay cannot measure frequency for voltage less than 4 volts. Therefore, in these conditions, the Frequency and Out-of-Step elements do not work.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Auxiliary Outputs of the Undervoltage Element for Blocking**

Table 3.2-1:Auxiliary Outputs and Events of the Undervoltage Element for Blocking					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
BLK_MIN_V	Generic Outputs of Protection	PFCF1.BlkV	Frequency Disabled by Lack of Voltage.	I	Frequency and Out-of-Step elements blocking.

3.2.1.g Common Settings

The shared settings are:

- ***Inhibition Voltage***. This setting checks that the voltage is above a set value. If so, it allows the frequency elements to meter and to operate. Otherwise, it gives a frequency value of zero and the frequency elements are inhibited.
- ***Pickup Activation Timer***. This is the number of half-waves that must meet the fault conditions for the frequency elements to pick up This time allows filtering transients in frequency measurement, as are produced by phase changes resulting from load changes, faults, etc.
- ***Reset Time***. This is the number of cycles during which there may not exist fault conditions so that the frequency elements already picked up will reset. When the frequency elements have been picked up and have not yet operated, the fault conditions may disappear during a brief instant. This setting indicates how long these conditions may disappear without resetting the element. For example, if the rate of change should be falling below -0.5 Hz/s and during an instant it only goes down to -0.45 Hz/s; it may not be desirable that the protection function reset if the time the fault condition disappears is very short.
- ***RMS Supervision***: allows disabling the frequency elements if the positive sequence voltage RMS value is below the setting ***Inhibit Voltage***.
- ***Time of Differentiation (half-cycles***): gives the time lapse between the frequency values selected for computing the frequency rate of change. It allows reducing the rate of change value when frequency changes are produced that have an oscillatory component.
- ***Frequency Filter Time (half-cycles***): enables computing a mean value of the measured frequency values, filtering frequency measurement oscillations, so avoiding computing excessive rate of changes. No filtering is performed if set to 1.

Note: when the Load Shading type is defined as "Rate of Change", this always has to be with "Negative" rate of change. If it is set to positive, the Load Shading element does not operate.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.1.h Setting Ranges

Metering / Frequency					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Inhibit Voltage	Inhibit Voltage	PFCF1.InhValV	4-150 V	0.01 V	4 V
Pickup Activation Timer	Pick Up Time	PFCF1.StrDlHfCyc	3-30 hc	1	6 hc
Reset Time	Dropout Time	PFCF1.RsDlCyc	0-10 cycles	1	0 cycles
RMS Supervision	RMS supervision	PFCF1.RmsSupEna	NO / YES		NO
Time of differentiation	Differentiation T.	PFCF1.ROCHfCyc	7 - 25 scics	1 scic	7 cicls
Frequency filter time	Freq. filter time	PFCF1.HzFilHfCyc	1 - 25 scics	1 scic	1 cicls

General					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
PLL Enable	PLL Enable	GENTVTR1.PLLEna	NO / YES		NO

3.2.1.i IEC 61850 Logical Node

CLASS PFCF1		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
BlkV	SPS	Frequency Disabled by Lack of Voltage
Settings		
InhValV	ASG	Inhibit Voltage
StrDlHfCyc	ING	Pickup Activation Timer
RsDlCyc	ING	Reset Time
RmsSupEna	SPG	RMS supervision
ROCHfCyc	ING	Time of differentiation
HzFilHfCyc	ING	Frequency filter time

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.1.j Protection Element Test

- **Voltage Reset**

The Frequency elements must reset within the margin indicated in Table 3.2-3 for set voltage value X.

Table 3.2-2: Voltage Reset

Setting	Pickup		Reset	
X	MAX	MIN	MAX	MIN
	1.03 x X	0.97 x X	1.08 x X	1.02 x X

- **Operating Times**

To measure times, the voltage generator must be able to generate an up or down frequency ramp depending on the element to be tested as well as to provide an output to initiate a chronometer when it gets to the pickup frequency.

Operating times must comply with 1.5 cycles + ***Activation Half Cycles*** setting, provided that the frequency variation is not abrupt; in these cases, 2 half cycles should be added to the commented time. If the setting value is 0, the operating time will also be close to 1.5 cycles + ***Activation Half Cycles*** setting.

In operating times, it is important how the frequency ramp is generated and when the chronometer starts. The frequency value of the signal generated should be very close to the threshold to test and generate the broadest step possible.

Without a frequency ramp generator, only the Overfrequency element can be tested. Going from no voltage applied to applying voltage above the disable and the Overfrequency settings will yield a time value somewhat greater than with a frequency ramp.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.1.k Application

The frequency variations are caused by an incorrect balance between generation and load, which is generally due to the following reasons:

- Division of the system into parts.
- Imbalance between load and generation due to lack of foresight or deficient programming.
- Loss of generation, trip of busses or important interconnection lines.

Frequency is a reliable indicator of an overload condition. Any decrease in frequency is caused by an excess load. With this condition, minimum frequency relays must be used to shed load and thus balance generation with consumption and avoid a major collapse of the system. When frequency recovers its rated value and the electricity system stabilizes, the loads that have been shed are restored. This restoration operation is performed by the maximum frequency relay.

A decrease in frequency produces instability in the electricity system and can damage the generators. The greatest danger, however, lies in steam turbines. Variations in the rotational speed of the turbine produce vibrations and consequently the blades suffer mechanical fatigue. Since this is cumulative deterioration, the problem will increase whenever the turbine is in an underfrequency condition.

When the variation in the frequency is small, the imbalance can be corrected by regulating the generators. With large frequency variations, however, the generator cannot correct it. As a result, the frequency starts decreasing, risking a trip of the generation sets. If this frequency drop is not corrected, an irreversible process begins and leads to a general blackout.

In situations of strong generation deficit, the only way to restore balance is to selectively disconnect loads. The loads are usually disconnected when the frequency has fallen below fixed values to give the generation sets time to react to frequency drops with speed regulators. When the frequency drop is very quick, this action is not effective enough. Loads have to be disconnected according to the variation in the frequency in respect of time, that is, by basing calculations and operation on the rate of change in respect of time.

Underfrequency relays are usually installed in substations and industrial plants that require a load shedding system, where the loads are fed exclusively by local generation or by a combination of its own generators and a transmission line derivation. In this second case [part (A) of Figure 3.2.3], if a fault occurs in the transmission line, the system's own generators will be overloaded, and the frequency will drop quickly. This plant needs a fast load shedding system controlled by frequency relays.

If the transmission line supplies more than one plant and is disconnected at a remote end [part (B) of Figure 3.2.3], the plant, with its own generation, is in a situation to supply power to the line while its own frequency is decreasing. This power flow output can be avoided with protection relays against power inversion but, unless the whole overload is eliminated, the frequency relay must disconnect the lower priority local loads.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Independently of generation, frequency protections are also used in distribution substations that require a load shedding system with a disconnection priority scale. Priorities are also taken into account as frequency is recovered while restoring the loads.

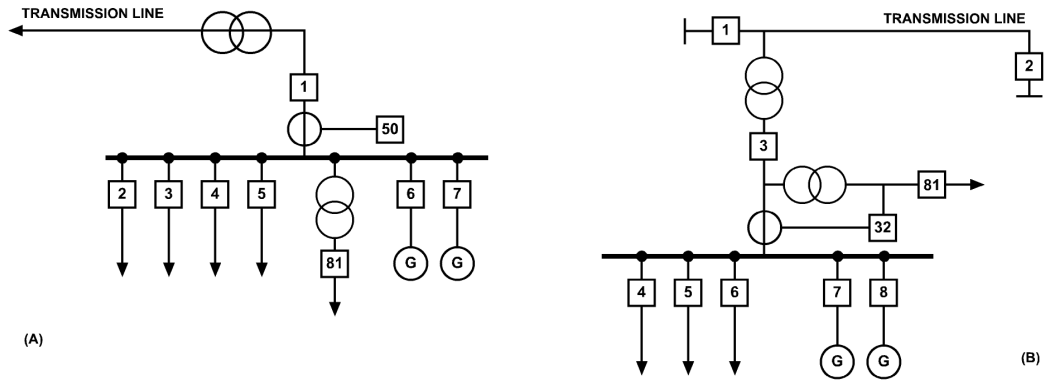


Figure 3.2.2 Load Shedding System in an Industrial Plant.

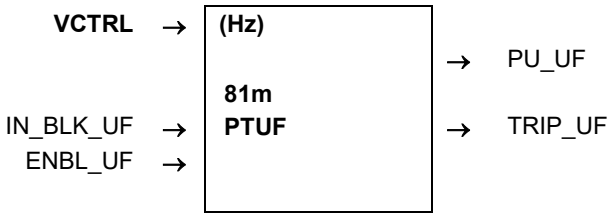
© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.2 Underfrequency Elements

3.2.2.a Identification

Description of the Protection Elements	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Underfrequency Unit 1	PTUF1	f<	81m1

3.2.2.b General Block



3.2.2.c Operation Principles

Pickup occurs when the value measured coincides with or is below the pickup value (100% of the setting) during a number of half-waves equal to or greater than the setting ***Pickup Activation Timer***, and resets when the frequency goes up above 10mHz of this setting for a time equal to or greater than the ***Reset Time*** setting. The same as in the Overfrequency element, this ***Reset Time*** setting indicates how long the fault conditions must disappear after a fault for the trip to reset.

3.2.2.d Setting Ranges

Metering / Frequency / Underfrequency					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Underfrequency Enable	Underfreq. Enable	PTUF.LNInSvc	NO / YES		NO
Underfrequency Pickup	Underfreq. Pickup	PTUF.StrVal	40 - 70 Hz	0.01 Hz	40 - 70 Hz
Underfrequency Delay	Underfreq. Delay	PTUF.OpDlTmms	0-300 s	0.01 s	0-300 s
Reset Time	Dropout Time	PTUF.RsDlTmms	0-300 s	0.01 s	0-300 s

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.2.e Analog Inputs to the Unit

The underfrequency value will be calculated from the input voltage VCTRL.

Table 3.2-3: Analog Inputs to the Underfrequency Modules		
Name	**Description**	**IEC 61850**
FREC	Frequency	MMXU1.Hz (MV)

3.2.2.f Digital Inputs to the Underfrequency Modules

Table 3.2-4: Digital Inputs to the Underfrequency Modules					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN_BLK_UF1	Logic Inputs to Protection	PTUF1.Mod	Block Underfrequency Unit 1	I	Activation of the input before the trip is generated prevents the element from operating. If activated after the trip, it resets.
ENBL_UF1	Enabling Commands	PTUF1.Mod	Enable Underfrequency Unit 1	I	Activation of this input puts the unit into service. It can be assigned to status contact inputs by level or to a command from the communications protocol or from the HMI. The default value of this logic input signal is a “1.”

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.2.g Auxiliary Outputs and Events of the Underfrequency Modules

Table 3.2-5: Auxiliary Outputs and Events of the Underfrequency Modules					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
PU_UF1	Pickup Protection Outputs	PTUF1.Str	Underfrequency Unit 1 Pick Up	I	Pickup of the underfrequency elements and start of the time count.
TRIP_UF1	Trip Protection Outputs	PTUF1.Op	Underfrequency Unit 1 Trip	I	Trip of the underfrequency elements.
UF1_ENBLD	Enabled Units Protection Outputs	PTUF1.Mod	Underfrequency Unit 1 Enabled	I	Enable or disable status indication of the underfrequency elements.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

3.2.2.h IEC 61850 Logical Node

CLASS PTUF		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
Str	ACD	Pickup
Op	ACT	Trip
Settings		
StrVal	ASG	Start value
OpDlTmms	ING	Operate Delay time
RsDlTmms	ING	Reset Delay Time
Extended Data		
LNInSvc	EXT_SPG	In service

3.2.2.i Protection Element Test

Before testing these elements, the voltage elements that are not being tested must be disabled.

- **Pickup and Reset of the Underfrequency Elements**

The pickups and resets must be within the margins indicated in following Table for their rated voltage.

Table 3.2-6: Pickup and Reset of the Underfrequency Elements

Setting	Pickup		Reset	
XHz	ΦA_MIN	ΦA_MAX	ΦR_MIN	ΦR_MAX
	X - 0.005Hz	X + 0.005Hz	(X - 0.01Hz) + 0.005Hz	(X - 0.01Hz) - 0.005Hz

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Chapter 4.

Supervision & Control

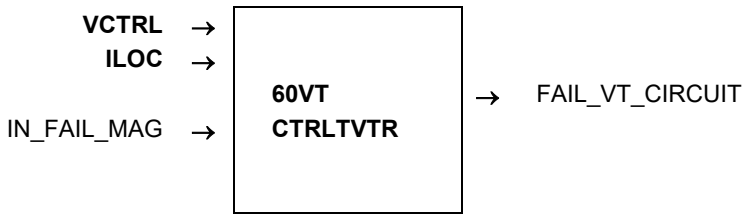
4.1 Voltage Measurement Circuit Supervision

4.1.1 Identification 4.1-2
4.1.2 General Block 4.1-2
4.1.3 Operation Principles and Block Diagram 4.1-2
4.1.4 Aplication of the Unit 4.1-3
4.1.5 Setting Ranges 4.1-3
4.1.6 Analogue Inputs to Voltage Measurement Circuit Supervision Module 4.1-3
4.1.7 Digital Inputs to the Voltage Measurement Circuit Supervision Module 4.1-4
4.1.8 Auxiliary Outputs and Events of the Voltage Measurement Circuit Supervision Module 4.1-4
4.1.9 IEC 61850 Logical Node 4.1-5
4.1.10 Voltage Measurement Circuit Supervision Test 4.1-6

4.1.1 Identification

Description of the Protection Unit	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Voltage Measurement Circuit Supervision	CTRLTVTR1	MCS 3V	60VT

4.1.2 General Block



4.1.3 Operation Principles and Block Diagram

In order to avoid incorrect operations issued by the units that use the voltage measurement, the equipment has a function to check if a drop in the measurement is produced by a failure in the analog voltage measurement reception circuit.

This supervision unit blocks inputs from protection elements when the protection magnetic-thermal circuit breaker of the voltage measuring transformer has previously tripped. The logic related to the detection of the thermal-magnetic circuit breaker trip conditions must be carried out before the functions it blocks. The logic associated to the element is indicated in the following figure.

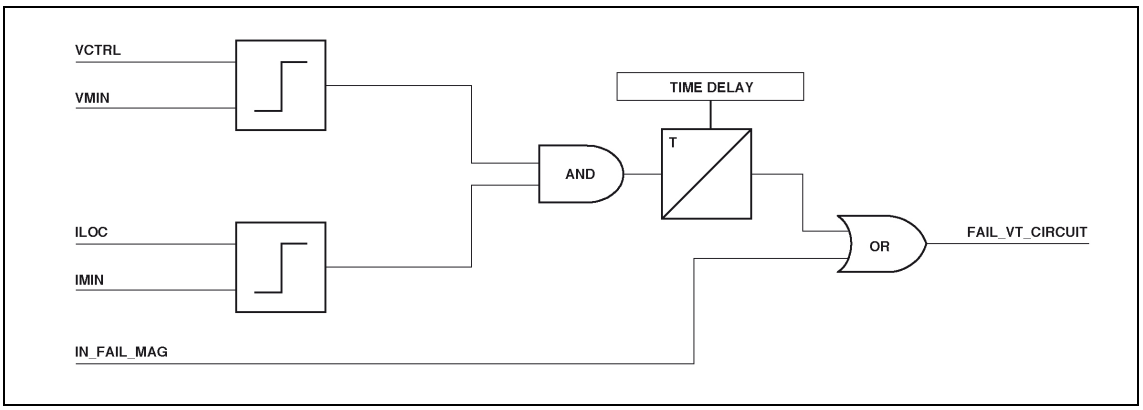


Figure 4.1.1 Voltage Circuit Failure Detection Element Scheme.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Current ILOC is compared with the setting value ***C Min VT Supervision***. If ILOC is higher, the voltage control will be compared with the corresponding setting value ***V Min VT Supervision***. In this case, if the voltage is lower than the set voltage value, the relay will activate the signal **Failure on Voltage Measuring Circuit** after a time delay (***VT Supervision Timer*** setting). The blocking of those protection units affected by the voltage measurement unbalance will have to be duly programmed in the logic module through the communication program ***ZIV e-NET tool***®.

4.1.4 Aplication of the Unit

This Supervision Unit will block, by means of the block inputs of the other protection elements, when the protection magnetothermal circuit breaker of the voltage measuring transformer has previously tripped.

The blocking of those protection units affected by the voltage unbalance will have to be duly programmed in the logic module.

4.1.5 Setting Ranges

Metering / Voltage Transformer Supervision					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
VT Supervision Enable	VT Superv Enable	PHSTVTR1.SupSvc	YES / NO		NO
C Min VT Supervision	C min VT Superv	PHSTVTR1.SupMinA	0.2 - 2 A	0.01A	0.5 A
V Min VT Supervision	V min VT Superv	PHSTVTR1.SupMinV	2 - 100 V	0.01 V	30 V
VT Supervision Timer	VT Superv Time	PHSTVTR1.SupTmms	0.01 - 5 s	0.01 s	0.05 s

4.1.6 Analogue Inputs to Voltage Measurement Circuit Supervision Module

Table 4.1-1:Analogue Inputs to the Voltage Measurement Circuit Supervision Module		
Nombre	**Descripción**	**IEC 61850**
VCTRL	Wired input voltage	MMXU.VCtrl
ILOC	Local current	MMXU.AmpLoc

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.1.7 Digital Inputs to the Voltage Measurement Circuit Supervision Module

Table 4.1-2: Digital Inputs to the Voltage Measurement Circuit Supervision Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN_FAIL_MAG	Logic Inputs to Protection	PHSTVTR1.SupFailIn	Voltage Circuit Supervision Fail Input	I	The activation of this input means direct activation of voltage circuit failure Detector signal.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.1.8 Auxiliary Outputs and Events of the Voltage Measurement Circuit Supervision Module

Table 4.1-3: Auxiliary Outputs and Events of the Voltage Measurement Circuit Supervision Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
FAIL_VT_CIRCUIT	Trip Protection Outputs	PHSTVTR1.SupFail	VT Supervision Unit Active	I	It shows that although voltage measurement does not reach the equipment, there actually is voltage. So that no trip on lack of voltage shall be performed.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.1.9 IEC 61850 Logical Node

CLASS IDFPHSTVTR		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Settings		
VRtg	ASG	Rated Voltage
HzRtg	ASG	Rated Frequency
Rat	ASG	Winding ratio of external voltage transformer
Extended Data		
SupEna	EXT_SPC	TVTR supervision enable command
SupBlk	EXT_SPC	TVTR supervision block command
SupFailIn	EXT_SPS	Supervision failure input
SupFail	EXT_SPS	Supervision failure signal
SupSvc	EXT_SPG	Supervision in service
SupTmms	EXT_ING	Supervision delay time
SupMinA	EXT_ASG	Supervision minimum current
SupMinV	EXT_ASG	Supervision minimum voltage
PLLEna	EXT_SPG	PLL enable

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.1.10 Voltage Measurement Circuit Supervision Test

Without the injection of any magnitude, activate the **Voltage Circuit Supervision Fail Input** signal, which will have been configured in a DI or allocated in a control logic. Check that the **Voltage Circuit Failure** activates without any time delay. Carry out the same check applying voltage above the minimum voltage setting value and current below the minimum current setting, a similar behavior being observed when the **Voltage Circuit Supervision Fail Input** signal is activated.

Beginning with the injection of **ILOC** above the minimum current setting and the voltage above the minimum voltage setting, decrease **VCTRL** value until it is below the setting. Check that the element output activates when **VCTRL** < ***V Min VT Supervision*** and deactivates when **VCTRL** ≥ ***V Min VT Supervision***. Namely, there is no hysteresis between pickup and reset, this value being approximately 50mV.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

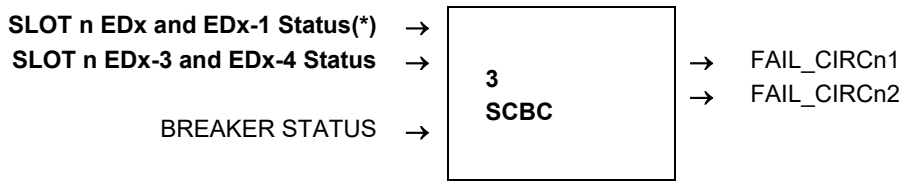
4.2 Trip and Close Coil Circuit Supervision

4.2.1	Identification	4.2-2
4.2.2	General Block	4.2-2
4.2.3	Operation Principles and Block Diagram	4.2-2
4.2.3.a	Circuit 1 Supervision in One State	4.2-5
4.2.3.b	Supervision of Coil Circuit 2	4.2-5
4.2.4	Setting Ranges	4.2-6
4.2.5	Auxiliary Outputs and Events of the Coil Circuit Supervision Module	4.2-7
4.2.6	IEC 61850 Logical Node	4.2-7
4.2.7	Coil Circuit Supervision Test	4.2-8

4.2.1 Identification

Description of the Protection Element	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Trip and Close Coil Circuit Supervision	SCBC1	TCS	3

4.2.2 General Block



(*) Where n goes from "A" to "J", and x is the number of the last digital input on the card.

The slots of digital inputs that have Coil Circuit Supervision inputs always have 2 sets of 3 inputs for the supervision of 2 circuits (coils).

4.2.3 Operation Principles and Block Diagram

This Supervision function permits an alarm when an anomalous situation occurs in the breaker's switching circuits: losses of the auxiliary switching power supply voltage or openings in the open and close circuits themselves.

The number of circuits on which supervision can be carried out depends on the cards selected in the model (see Chapters1.2, Model Selection and 1.9, Schemes and Drawings), being adjustable for each circuit, whether supervision is carried out in both positions of the breaker (open and closed), by means of 3 digital inputs, or only in one of them (by means of 2 digital inputs, the third being free for other applications).

The supervision function generates 2 outputs for each supervised circuit, so that with the 2 possible circuits to be monitored in each slot enabled, the outputs would be the following: **Slot n Circuit 1 Power Failure**, **Slot n Circuit 1 Failure**, **Slot n Circuit 2 Power Failure**, **Slot n Circuit 2 Failure**.

The two supervision circuits, in each slot, are treated as independent functions that can be independently set to enabled by means of a setting.

The coils to be monitored may be trip or closing; therefore, the denomination of the unit is generic. Each of the coils has an associated pair of configurable digital inputs for monitoring. They can be paired to **Supervision in 2 States**, which is explained next, or individually to **Supervision in 1 State**. In any case, both modes can be combined for different coils (for example, to monitor the trip coil in open and closed, and coil two only in open).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 4.2-1 identifies the status contact inputs that must be used to monitor each of the circuits.

Table 4.2-1: Configuration of Digital Inputs for Supervision by SLOTS		
Monitored Circuit	Supervision in 2 states	Supervision in one state
SLOT n Coil 1	IN(x-4)	IN(x-4)
	IN(x-3)	-
SLOT n Coil 2	IN(x-1)	IN(x-1)
	INx	-

Where x is the number of the last digital input on the card.

To monitor the Coil 1, a positive must be entered through terminal IN(x-5) of the SLOT n, and to monitor Coil 2, a positive must be entered through terminal IN(x-2) of the SLOT n. For details, see Chapter 1.9, Schemes and Drawings.

These digital inputs do not need to be configured in advance to perform the coils supervision function. By enabling any of the coils supervision, each pair of digital inputs will be automatically configured as per the table above, this is, the IED needs no physical intervention to be able to assign status contact inputs for the Supervision function; they simply need to be set for this purpose. Each of the coils can be configured as:

1. **No supervision**: The supervision algorithm is not executed and the status contact inputs associated with the supervision of each of the coils are treated as standard status contact inputs.
2. **Supervision in 2 states**: The algorithm is the one indicated by way of example in figure 4.2.1. Basically, an XOR algorithm supervises the state of the switching circuit in open as well as in closed.
3. **Supervision in 1 state**: The algorithm only takes into account the supervision of the coil in the breaker's position configured in the input. It does not monitor in the other position and therefore can never detect a fault in the coil.

For each of the monitored coils, it is possible to set a time after which, if there is discordance, the Failure is activated.

The supervision system of the coil circuits is not very sensitive to the impedance of the circuits as seen from the relay, basing its principle of operation on an injection of current pulses that allow to detect continuity in this circuit. Current pulses of 100ms are injected every second and it is checked whether this current circulates or not. In case of not circulating, the reason could be that it is being supervised by the open auxiliary contact or that the coil is open.

Under the conditions of the following figure (breaker open), current pulses are injected through inputs **IN12** and **IN13**.

Because **IN12** is connected to the 52/b contact that is closed, current flows through it. This current flow implies that the voltage at (+) of **IN12** will be that corresponding to the voltage drop at the coil and therefore insufficient to activate it. Therefore, **IN12** will be deactivated.

There is no current flowing through **IN13** because contact 52/a is open. As a consequence of this, the voltage drop in the (+) of this digital input will be practically the supply voltage of the Opening Circuit. Therefore, **IN13** will be activated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Since the supervision has been programmed for **Supervision in 2 states**, the μController in charge of managing this supervision function will send a logic "0" to the main μProcessor and this will set the **SLOTn_FAIL_CIR1** (**Circuit 1 Failure**) signal to a logical "0". In this situation, it will be detected that digital input **IN12** is deactivated and **IN13** is activated.

If an operating coil is opened, the input that was deactivated (**IN12**) will be activated, remaining **IN13** activated and, after the configured time, the **Circuit 1 Failure** (**SLOTn_FAIL_CIR1**) signal will be activated.

If, with the control circuit in good condition, a closing or reclosing takes place, once the command has been executed, the status of the breaker and its contacts **52/a** and **52/b** changes resulting in that the situation of the **IN12** and **IN13** input activation is reversed and **SLOTn_FAIL_CIR1** output will remain deactivated.

The function of the reset time is to absorb the possible time race between the closure of the **52/a** contact and the opening of the **52/b** contact. In general, the **IN12** and **IN13** digital inputs will not change status simultaneously and, therefore, there will be a discordance between the two contacts. This does not change the **SLOTn_FAIL_CIR1** output status, provided its duration is less than the set time.

If a trip occurs while the breaker is closed and the breaker opens, inverting the state of contacts **52/a** and **52/b**, the **SLOTn_FAIL_CIR1** signal will not be activated, regardless of the duration of the trip command. If the breaker does not execute the command and the opening command persists longer than the adjusted reset time, the **SLOTn_FAIL_CIR1** signal will activate.

If the operating voltage disappears, the energized inputs will deenergize and this will cause the activation of circuit failure outputs (**SLOTn_FAIL_CIR1** and **SLOTn_FAIL_CIR2**).

In order for the supervision function of a trip coil (**SLOTn_FAIL_CIR1**, **SLOTn_FAIL_CIR2**) to avoid the closing of the supervised breaker, this logic must be configured in the programmable logic.

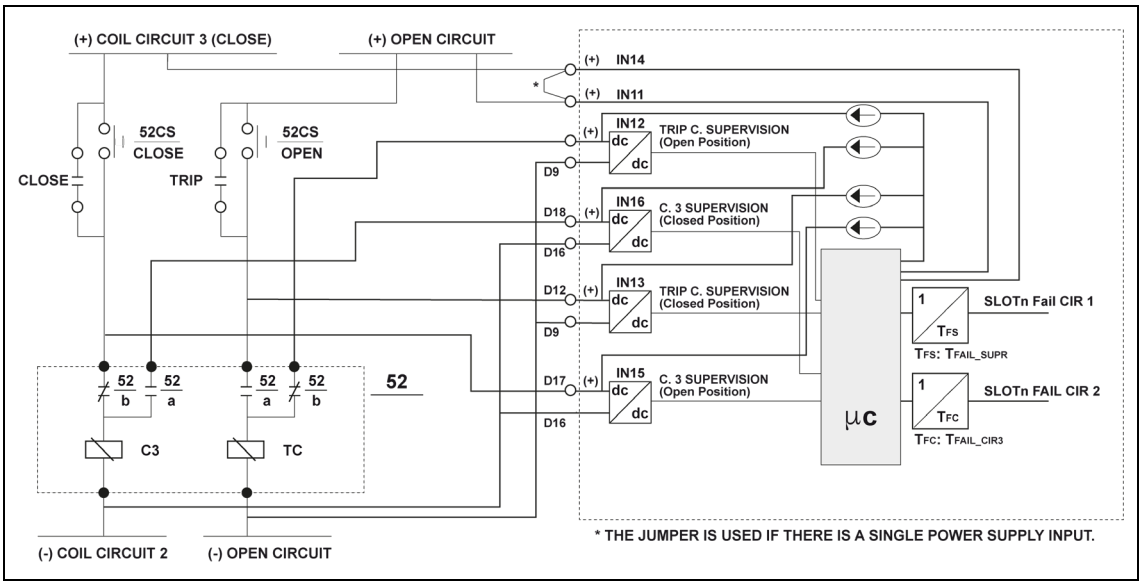


Figure 4.2.1 Trip/Close Coil Circuit Supervision Block Diagram.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.2.3.a Circuit 1 Supervision in One State

Under the conditions in previous Figure (open breaker), when carrying out the supervision in a given status, open or closed breaker supervision must be selected. In any case, the first group input (**IN12** or **IN15**) will be used.

The **IN12** or **IN15** input will therefore be hard wired to the open or closed breaker status, the one to be supervised. In case of Figure 6.8.1, the **IN12** input would be supervising the breaker closed status and therefore the supervision will not be operative since the breaker is open.

With the breaker closed, the **IN12** input is deenergized, because when current is injected into the circuit, the voltage at the positive terminal is below its activation threshold. In this situation, the **Circuit 1 Failure** (**SLOTn_FAIL_CIR1**) output is inactive.

If an operating coil anomaly occurs (breakage), the deactivated input will be activated and once the set timing times out, the **Trip Circuit 1 Failure** (**SLOTn_FAIL_CIR1**) signal will be sent.

4.2.3.b Supervision of Coil Circuit 2

The explanation given for Circuit 1 supervision is valid for the control circuit 2 and for any of the SLOTS, both for the supervision in two states and the supervision in a single status. Also, there must be taken into account that reset times for the activation of the failure output are independent from that of Circuit 1. In this case, the control circuit failure signal is designated as **SLOTn_FAIL_CIR2**.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.2.4 Setting Ranges

Coil Circuit Supervision					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
SLOT n. Circuit 1					
Supervision Mode	Supervision Mode	SCBC1.ColChk1	NO TWO STATES ONE STATE (52 OPEN 1) ONE STATE (52 CLOSE 1) ONE STATE (52 OPEN 2) ONE STATE (52 CLOSE 2) ONE STATE (52 OPEN 3) ONE STATE (52 CLOSE 3) ONE STATE (52 OPEN 4) ONE STATE (52 CLOSE 4)		NO
Failure Delay	Fail Delay	SCBC1.ColAlmTms1	1 - 60 s	1 s	5 s
SLOT n. Circuit 2					
Supervision Mode	Supervision Mode	SCBC1. ColChk2	NO TWO STATES ONE STATE (52 OPEN 1) ONE STATE (52 CLOSE 1) ONE STATE (52 OPEN 2) ONE STATE (52 CLOSE 2) ONE STATE (52 OPEN 3) ONE STATE (52 CLOSE 3) ONE STATE (52 OPEN 4) ONE STATE (52 CLOSE 4)		NO
Failure Delay	Fail Delay	SCBC1.ColAlmTms2	1 - 60 s	1 s	5 s

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.2.5 Auxiliary Outputs and Events of the Coil Circuit Supervision Module

Table 4.2-2: Auxiliary Outputs and Events of the Coil Circuit Supervision Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
SLOTn_FAIL_CIR1	Generic Outputs of Protection	SCBCn.ColAlm1	Coil Circuit 1 Failure Slot n	I	They activate when an anomaly is detected in any of the switching circuits.
SLOTn_FAIL_CIR2		SCBCn.ColAlm2	Coil Circuit 2 Failure Slot n	I	
SLOTA_FAIL_ALMCIR1		SCBCn.ColPwrAlm1	Coil Circuit 1 Power Failure Slot n	I	Alarm signals that indicate an anomaly of the internal supervision circuit power supply.
SLOTA_FAIL_ALMCIR2		SCBCn.ColPwrAlm2	Coil Circuit 2 Power Failure Slot n	I	

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.2.6 IEC 61850 Logical Node

CLASS IRLSCBCn		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
ColAlm1	SPS	Slotn_Circuit 1 alarm indication
ColAlm2	SPS	Slotn_Circuit 2 alarm indication
ColPwrAlm1	SPS	Slotn_Circuit 1 internal supply failure indication
ColPwrAlm2	SPS	Slotn_Circuit 2 internal supply failure indication
Settings		
ColChk1	ENG	Slotn_Circuit 1 supervision mode
ColAlmTmms1	ING	Slotn_Circuit 1 time delay
ColChk2	ENG	Slotn_Circuit 2 supervision mode
ColAlmTmms2	ING	Slotn_Circuit 2 time delay

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.2.7 Coil Circuit Supervision Test

Hard wire the relay with the **IN12** and **IN13**, **IN15** and **IN16** inputs, corresponding to Slot A, connected to a resistor simulating a breaker coil, with a contact in series that can be opened and closed (simulating the breaker status contact) to close the ground connection circuit.

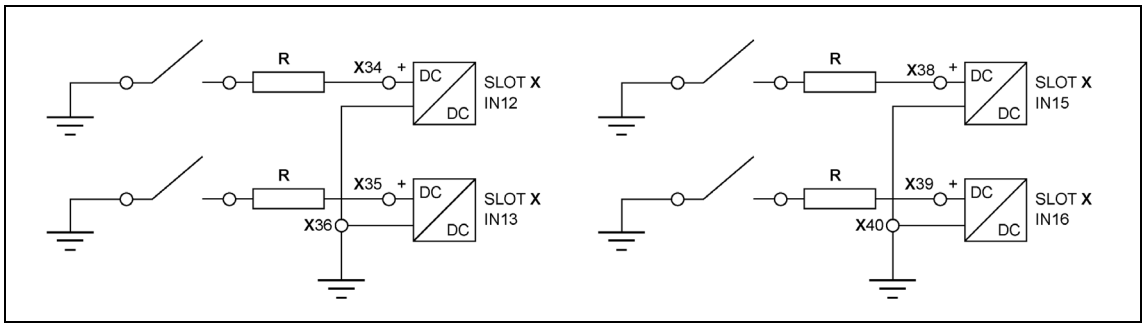


Figure 4.2.2 Hard Wiring for the Control Circuit Supervision Test of the SLOT X (A and/or B).

Set the circuit 1 and 2 element to **Double Status** checking that:

- Circuit anomaly signal is generated when both contacts simulating the breaker status are open or both closed.
- The alarm of each of the supervision circuits disappears when one and only one contact is in closed status, whereas the other remains open (always referring to the pairs of contacts relative to the supervision circuit inputs, **IN12**-**IN13** and **IN15**-**IN16**).

Set the element to close breaker status, such that the inputs used for supervision will be **IN12** (Circuit 1) and **IN15** (Circuit 2).

- In the closed breaker status, leave the contact simulating open breaker and check that alarms are generated.
- In the closed breaker status, close the contact simulating the breaker and check that alarms disappear.
- In the open breaker status, check that no alarms are ever generated regardless the status of the contact simulating the breaker status.

Set the element to open breaker status, such that the inputs used for supervision will be **IN12** (Circuit 1) and **IN15** (Circuit 2).

- In the open breaker status, leave the contact simulating open breaker and check that alarms are generated.
- In the open breaker status, close the contact simulating the breaker and check that alarms disappear.
- In the close breaker status, check that no alarms are ever generated regardless the status of the contact simulating the breaker status.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.3 General Settings

4.3.1	Description	4.3-2
4.3.1.a	Unit In Service	4.3-2
4.3.1.b	Transformer Ratios	4.3-2
4.3.1.c	Angle Reference	4.3-3
4.3.1.d	Digital PLL	4.3-3
4.3.1.e	Simultaneous Commands	4.3-3
4.3.1.f	Description Settings	4.3-4
4.3.2	Setting Ranges	4.3-4

4.3.1 Description

The following settings are included within the General Settings group:

Unit In Service.
CT / VT Ratios.
Angle Reference.
PLL Enable.
Simultaneous Commands.
Description Settings.

4.3.1.a Unit In Service

Relay enabled (**YES**), means that all relay functions work normally (dependent on function settings).

If relay is disabled (**NO**), all functions are restricted to measurement operations only. Measurements are visualized on display and through local and remote communications.

4.3.1.b Transformer Ratios

Transformer Ratio defines how analog values are displayed on the protection display. If Transformer Ratio is set to 1, secondary values are displayed. If, on the other hand, the Transformer Ratio corresponding to analog input adapter transformer is selected, primary values are displayed. Settable turn ratios are:

- Local Current.
- Parallel Transformer Current.
- Voltage.

In all cases, all overcurrent and overvoltage protection element settings are referred to secondary values. Programmable logic analog settings could refer both to secondary and primary values.

Note: all Event Record and Metering History Log magnitudes are stored in secondary values; except for energy magnitudes that are always recorded in primary values.

***ZivercomPlus*® status screen may display all the measurements in primary or secondary values depending on the button (), being pushed or not respectively. Energy measurements are an exception as will always be displayed on primary values.**

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.3.1.c Angle Reference

The angle reference can be the measurement carried out by the VCTRL voltage analog channel or the measurement carried out by the ILOC local current analog channel, depending on the regulation variable to be controlled (VCTRL or external).

Likewise, the minimum values of current or voltage required to carry out the calculation of the angles can be adjusted.

When there is no angle reference magnitude, all angles will be displayed in the relay with an invalid value (***) and the oscillogram will display them at 0˚.

4.3.1.d Digital PLL

The equipments include an algorithm that automatically adapts the sampling frequency to the network frequency, varying the time between samples, to ensure that the DFT calculation window comprises exactly one network cycle. If this adaptation should not take place, said window would not comprise one periodic wave, which will result in DFT measurement errors. These errors will be greater as the deviation between the window time and the period of the sampled wave is also greater.

The algorithm of sampling frequency adaptation is disabled by default. It can only be enabled through the HMI or Configuration Program, which is only recommended in those cases in which large variations in the frequency are likely to be produced.

4.3.1.e Simultaneous Commands

The setting ***Simultaneous Commands*** allows setting the behavior of command acceptance. When this setting is set to **NO**, the relay will allow running a single command at a time, namely, once a command is received, any other command will be rejected until completing the preceding command already in progress, whether satisfactorily or not. Namely, new commands are not admitted when there is one in progress.

With the setting set to **YES**, the relay allows concurrent commands except if they are on the same logic element, in which case they will be rejected. Commands will start running once the operation of preceding command has started, and a maximum of 32 concurrent commands may be queued or carried out.

At the time of running the commands, the concurrent conditions are checked 2 times to give more security over the change of conditions from the time it is received to the time it is finally going to be run. The command is deemed to be in progress only if there are no running problems and the blocking is only checked once since it depends on the status and this changes from instant to instant. In this way, a command running process will be:

1. Assessment of concurrent conditions. Progress continues anyway.
2. Blocking conditions are assessed, an error being returned if there is blocking.
3. If the above concurrent conditions are not complied with, a concurrent error is returned.
4. A non-interrupt zone is entered in real time.
5. The concurrent conditions are assessed again, an error being returned if they are not complied with.
6. Activation of the command being run (this prevents new commands from entering).
7. Return to interrupt zone.
8. Activation of the command pulse if the process above has been satisfactory.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.3.1.f Description Settings

The device has 6 settings to be able to describe the device by a maximum of 64 characters per setting.

Name.
Breaker.
Division.
Zone.
Description1.
Description2.

4.3.2 Setting Ranges

General				
Communications Program	**IEC 61850**	**Range**	**Step**	**By Default**
Name	LPHD1.Name	Max Charac=20		""
Breaker	LPHD1.Breaker	Max Charac=5		""
Division	LPHD1.Division	Max Charac=64		""
Zone	LPHD1.Zone	Max Charac=64		""
Description1	LPHD1.Desc1	Max Charac=64		""
Description2	LPHD1.Desc2	Max Charac=64		""
Unit In Service	LPHD1.UnitInSvc	YES / NO		YES
Local CT Ratio	LOCTCTR1.Rat	1 - 100000	0.01	1
Parallel CT Ratio	PARTCTR2.Rat	1 - 100000	0.01	1
VT Ratio	CTRLTVTR1.Rat	1 - 100000	0.01	1
PLL Enable	CTRTVTR1.PLLEna	YES / NO		YES
Simultaneous Commands	LPHD1.LmtCmdEna	YES / NO		YES
Angle Reference				
Minimum Voltage Value	LPHD1.AngRefMinV	0.5 - 110 V	0.001 V	0.5 V
Minimum Current Value	LPHD1.AngRefMinA	0.02 - 5 A	0.001 A	0.02 A

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.4 Configuration Settings

4.4.1	Description	4.4-2
4.4.1.a	Nominal Values	4.4-2
4.4.1.b	Access Passwords	4.4-2
4.4.1.c	Communications	4.4-2
4.4.1.d	Date and Time	4.4-3
4.4.1.e	Contrast Adjustment	4.4-3
4.4.1.f	Autodimming Function	4.4-3
4.4.1.g	Return Time	4.4-4
4.4.2	Setting Ranges	4.4-4

4.4.1 Description

The following setting groups are included into the Configuration group:

Nominal Values.
Passwords.
Communications.
Operation Enable (when there are commands in the control logic configured to be carried out from HMI).
Date and Time.
Image.
Autodimming.

4.4.1.a Nominal Values

Nominal operating values are selected through these settings, both for current and voltage. Following parameters can be selected:

- **Nominal I Local**: local transformer nominal current.
- **Nominal I Parallel**: parallel transformer nominal current.
- **Nominal VCTRL**: nominal phase-to-phase voltage setting is the reference value for all settings expressed in times or % nominal voltage. Applied both to phase and synchronism voltage.
- **Nominal Frequency**: to select system nominal frequency, regardless whether the frequency adaptation system is later capable of adjusting to changes produced in this magnitude.

After modification of any of the settings above, only accessible from HMI display, relay resets the same as if it were switched off and then switched on; no setting or information is lost.

4.4.1.b Access Passwords

The Passwords option allows changing access passwords for options: Configuration, Operations and Settings.

Select the Configuration option to change access password for configuration group options. Also, different passwords can be configured for operations and settings modification options.

These settings are only available through HMI and the passwords are numerical consisting of four digits.

4.4.1.c Communications

See paragraph 1.5.6 on Communications.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.4.1.d Date and Time

Selecting date and time in the configuration menu displays this setting to configure relay date and time.

- **Local Time Zone Setting**

Setting ***Local Time Zone*** allows putting UTC time forward or back as required.

- **Summer Time / Winter Time Change**

Relay allows configuring the dates when summer time / winter time change takes place. In the first case the relay clock is put one hour forward (+1 Hour). In the second case the relay clock is put one hour back (-1 Hour) for the winter season. To configure a change of season the following must be specified:

- **Begin Time**: time when change of season takes place. Range 0 to 23 h.
- **Begin Day Type**: type of day when change of season takes place. It can take the following values **First Sunday**, **Second Sunday**, **Third Sunday**, **Fourth Sunday**, **Last Sunday** of the month and **Specific Day**.
- **Begin Day**: in case **Specific Day** is selected, state in which specific day of the month the change of season takes place.
- **Begin Month**: state the month in which the change of season takes place.

These settings are independent for the summer and winter seasons.

Note: if the Begin Day setting value is higher than the number of days of a given month, the last valid day of said month is taken as the day for the change of season.

The change of season function can be activated or deactivated through ***Summer / Winter Change Enable*** setting.

4.4.1.e Contrast Adjustment

This setting modifies the display contrast value (high value = more contrast).

4.4.1.f Autodimming Function

Autodimming function keeps the display background light off when not in use during an adjustable time. The display lights on when:

- A key is pressed.
- The relay trips.
- Activation of an internal alarm.

Being the display off, any key pressed will activate the display showing the as-default information under normal conditions for a period of time previously configured as long as no more keys are pressed. On that sense, pressing any key will always initiate the timer for the auto-dimming of the display.

If the relay is displaying a screen other than the default screen, the autodimming timer will not be initiated. Once the set ***Return Time*** times out, when the screen returns to the default screen, this autodimming function will begin.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Any protection trip or internal alarm within the relay will immediately switch-on the display to show the relevant information. The display will keep on until that trip or alarm is reset / acknowledged by the operator.

The screen will never be permanently switched off through setting.

4.4.1.g Return Time

If the relay displays a screen other than the default screen, it will not return to this state until the set ***Return Time*** times out.

If the ***Return Time*** is less than the ***Autodimming*** time, the latter is used as return time.

4.4.2 Setting Ranges

Communications Program	IEC 61850	Range	Step	Default
Nominal Values				
Nominal for I LOCAL	LOCTCTR1.ARtg	1 A / 5 A		5 A
Nominal for I PARAL	PARTCTR2.ARtg	1 A / 5 A		5 A
Nominal VCTRL	CTRITVTR1.VRtg	50 - 230 V		110 V
Nominal Freq.	CTRLTVTR1.HzRtg	50 Hz / 60 Hz		50 Hz
Autodimming				
Autodimming Enable	LPHD1.AutoDimEna	YES / NO		NO
Time Delay	LPHD1.AutoDimTmm	1 - 100 min	1 min	2 min
Communications				
See 1.4.6				
Passwords				
The factory-specified access password (full access) is 2140. Nevertheless, you can change the password to access the following options with the keypad: **Configuration**, **Operations** and **Settings**.				
Image				
No available	-	-01 to +04		-01
T RETURN				
Not available	-	1 - 100 min	1	2 min

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.5 Change Settings Groups

4.5.1 Description 4.5-2
4.5.2 Digital Inputs to Change Settings Groups 4.5-3
4.5.3 Auxiliary Outputs and Events to Change Settings Groups 4.5-4

4.5.1 Description

The Protection, Logic and Recloser settings include four alternative groups (GROUP 1, GROUP 2, GROUP 3, GROUP 4, GROUP 5, GROUP 6, GROUP 7 and GROUP 8), which can be activated or deactivated from the keypad, through the communication ports, by using digital inputs or with signals generated in the programmable logic.

This function permits modifying the active setting groups and, thereby, the response of the protection. This way, the behavior of the IED can adapt to changes in the external circumstances.

Two logic input signals can block changes in the active group from the HMI as well as via communications. When **Settings Group Change by Communications Disable (INH_CGRP_COM)** and **Settings Group Change by HMI Disable (INH_CGRP_MMI**) digital inputs are active, groups cannot be changed with commands via communications nor through the HMI.

If the digital inputs are used to change groups, up to four digital inputs may need to be configured through the programmable digital inputs:

- Command to activate Settings Group 1 by digital input (**Settings Group 1 Activation by Digital Input**, **CMD_GRP1_DI**).
- Command to activate Settings Group 2 by digital input (**Settings Group 2 Activation by Digital Input**, **CMD_GRP2_DI**).
- Command to activate Settings Group 3 by digital input (**Settings Group 3 Activation by Digital Input**, **CMD_GRP3_DI**).
- Command to activate Settings Group 4 by digital input (**Settings Group 4 Activation by Digital Input**, **CMD_GRP4_DI**).
- Command to activate Settings Group 1 by digital input (**Settings Group 5 Activation by Digital Input**, **CMD_GRP5_DI**).
- Command to activate Settings Group 2 by digital input (**Settings Group 6 Activation by Digital Input**, **CMD_GRP6_DI**).
- Command to activate Settings Group 3 by digital input (**Settings Group 7 Activation by Digital Input**, **CMD_GRP7_DI**).
- Command to activate Settings Group 4 by digital input (**Settings Group 8 Activation by Digital Input**, **CMD_GRP8_DI**).

Activation of said inputs will result in the activation of GROUP 1, GROUP 2, GROUP 3, GROUP 4, GROUP 5, GROUP 6, GROUP 7 and GROUP 8 respectively.

If, while one of the inputs is active, either of the other three or several of them are activated, no group change will take place. The status contact settings group control logic will recognize a single input only. If all four inputs are deactivated, however, the IED will remain in the last active settings group.

Note: Groups can be changed by activating T1, T2, T3, T4, T5, T6, T7 and T8 only if the display is in the default screen.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.5.2 Digital Inputs to Change Settings Groups

Table 4.5-1: Digital Inputs to Change Settings Groups					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
INH_CGRP_COM	Tables of Settings	-	Settings Group Change by Communications Disable		It blocks any change of the active group by the PROCOME procedure.
INH_CGRP_HMI		-	Settings Group Change by HMI Disable		It blocks any change of the active group through the HMI menu.
CMD_GRP1_COM	Commands	-	Settings Group 1 Activation by Communications		Commands to change the active group.
CMD_GRP1_DI		-	Settings Group 1 Activation by Digital Input		
CMD_GRP1_HMI		-	Settings Group 1 Activation by HMI		
CMD_GRP2_COM		-	Settings Group 2 Activation by Communications		
CMD_GRP2_DI		-	Settings Group 2 Activation by Digital Input		
CMD_GRP2_HMI		-	Settings Group 2 Activation by HMI		
CMD_GRP3_COM		-	Settings Group 3 Activation by Communications		
CMD_GRP3_DI		-	Settings Group 3 Activation by Digital Input		
CMD_GRP3_HMI		-	Settings Group 3 Activation by HMI		
CMD_GRP4_COM		-	Settings Group 4 Activation by Communications		
CMD_GRP4_DI		-	Settings Group 4 Activation by Digital Input		
CMD_GRP4_HMI		-	Settings Group 4 Activation by HMI		
CMD_GRP5_COM		-	Settings Group 5 Activation by Communications		
CMD_GRP5_DI		-	Settings Group 5 Activation by Digital Input		
CMD_GRP5_HMI		-	Settings Group 5 Activation by HMI		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 4.5-1: Digital Inputs to Change Settings Groups					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
CMD_GRP6_COM	Commands	-	Settings Group 6 Activation by Communications		Commands to change the active group.
CMD_GRP6_DI		-	Settings Group 6 Activation by Digital Input		
CMD_GRP6_HMI		-	Settings Group 6 Activation by HMI		
CMD_GRP7_COM		-	Settings Group 7 Activation by Communications		
CMD_GRP7_DI		-	Settings Group 7 Activation by Digital Input		
CMD_GRP7_HMI		-	Settings Group 7 Activation by HMI		
CMD_GRP8_COM		-	Settings Group 8 Activation by Communications		
CMD_GRP8_DI		-	Settings Group 8 Activation by Digital Input		
CMD_GRP8_HMI		-	Settings Group 8 Activation by HMI		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.5.3 Auxiliary Outputs and Events to Change Settings Groups

Table 4.5-2: Auxiliary Outputs and Events to Change Settings Groups					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
T1_ACTIVATED	Tables of Settings	-	Settings Group 1 In Service		Indication of the active group.
T2_ACTIVATED		-	Settings Group 2 In Service		
T3_ACTIVATED		-	Settings Group 3 In Service		
T4_ACTIVATED		-	Settings Group 4 In Service		
T5_ACTIVATED		-	Settings Group 5 In Service		
T6_ACTIVATED		-	Settings Group 6 In Service		
T7_ACTIVATED		-	Settings Group 7 In Service		
T8_ACTIVATED		-	Settings Group 8 In Service		

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

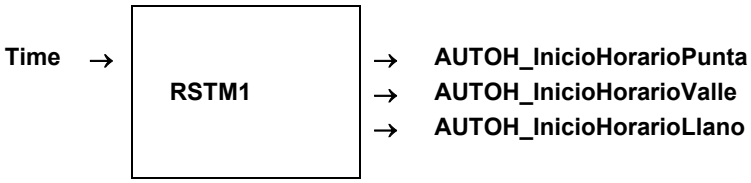
4.6 Time Zone Calendar

4.6.1 Identification 4.6-2
4.6.2 General Block 4.6-2
4.6.3 Description 4.6-2
4.6.4 Setting Ranges 4.6-2
4.6.5 Auxiliary Outputs of the Time Zone Calendar 4.6-3
4.6.6 IEC 61850 Logical Node 4.6-3

4.6.1 Identification

Description of the Protection Element	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Time Zone Calendar	RSTM1		

4.6.2 General Block



4.6.3 Description

Time Zone Calendar function allows carrying out applications dependent on time zones defined by relay protection settings. Three time zones can be set, namely, peak time, valley time and flat time, with access to time zone indication signals in the control part, such that can be used, for instance, to change settings tables, blocking protection elements or starting automatic controls. The time zones defined will be common to the 7 days of the week, discerning between working days, Saturdays or holidays not being possible.

4.6.4 Setting Ranges

Schedule of Time					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Enable	Enable	RSTM1.LNInSvc	YES / NO		NO
Start Peak Schedule	Start Peak Sched	RSTM1.StrTmm1	00:00 - 24:00	00:01	00:00
Start Valley Schedule	Start Valley Sched	RSTM1.StrTmm2	00:00 - 24:00	00:01	00:00
Start Flat Schedule	Start Flat Sched	RSTM1.StrTmm3	00:00 - 24:00	00:01	00:00

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.6.5 Auxiliary Outputs of the Time Zone Calendar

Table 4.6-1: Auxiliary Outputs of the Time Zone Calendar					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
AUTOH_InicioHorarioPunta	Automatons	RSTM1.StrInd1	Peak Schedule		Indicates that the current time is within the time zone defined as Peak
AUTOH_InicioHorarioValle		RSTM1.StrInd2	Valley Schedule		Indicates that the current time is within the time zone defined as Valley
AUTOH_InicioHorarioLlano		RSTM1.StrInd3	Flat Schedule		Indicates that the current time is within the time zone defined as Flat

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.6.6 IEC 61850 Logical Node

CLASS IRLRSTM		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
StrInd1	SPS	Peak Time zone
StrInd2	SPS	Off-peak time zone
StrInd1	SPS	Plain time zone
Settings		
LnInSvc	SPG	In Service
StrTmm1	ING	Time zone definition for peak time
StrTmm2	ING	Time zone definition for off-peak time
StrTmm3	ING	Time zone definition for plain time

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7 Programmable Logic

4.7.1	Description	4.7-2
4.7.2	Functional Characteristics	4.7-2
4.7.3	Control Commands	4.7-4
4.7.3.a	Command or Source Hierarchy	4.7-4
4.7.3.b	Successful and Failed Command Signals	4.7-5
4.7.3.c	Running simultaneous Commands	4.7-5
4.7.3.d	Command Treatment	4.7-5
4.7.3.e	Command Blocking as a Function of the Hierarchy	4.7-6
4.7.4	Description of Logic Operations	4.7-7
4.7.4.a	Boolean Operations (Booleans)	4.7-7
4.7.4.b	Move Instructions	4.7-8
4.7.4.c	Pulse Activation Operations (Triggers)	4.7-10
4.7.4.d	Counters	4.7-13
4.7.4.e	Arithmetic Operations	4.7-14
4.7.4.f	Special Operations	4.7-17

4.7.1 Description

One of the functions of the devices is a fully configurable one called Programmable Logic. The user can freely interconnect this logic digitally and analogically by using the ***ZIV e-NET tool***® program.

All the signals generated by the equipment will be available to the events, oscillograph records, digital inputs and outputs, HMI and communications according to how their programmable logic has been configured.

From the signals or readings generated by any of the functions of the relay (Protection units, Digital inputs, Communications, Command functions and Analog inputs), the user can define a logical operation using primitive logic functions (AND, OR, XOR, NOT, etc.), bistable circuits (latched or not), timers, comparators, constants, values, etc.

The programming function allows definition of the trip logic, control logic, interlocks, functional modules, local and remote states and control hierarchy required for complete protection and operation of a bay.

Priorities may also be selected in the programmable logic. There are three run cycles, of 2, 10 and 20 milliseconds, and priorities may be allocated placing the logics in either cycle. In this way, control logic can be carried out and use them as protection functions as they can be run with a priority similar to the functions implemented into the equipment firmware itself. For more information, please refer to the ***ZIV e-NET tool***® manual.

The processing of the input signals produces logical outputs that can be assigned to existing connections between the IED and the exterior: auxiliary output contacts, display, LEDs, communications, HMI, etc.

Maximum size for the programmable logic will be 64kb; i.e. around 1000 primitive logic gates.

4.7.2 Functional Characteristics

The IEDs can execute local programmable control functions associated with the bay as well as the logic associated with internal and external interlockings, treatment and generation of alarms and processing of signals. They are all programmable.

The execution of interlockings towards the external circuits implies being able to execute continuously active outputs depending on the combination of the state of various input signals through logic gates. These interlocking outputs are used for interrupting / continuing an exterior command circuit. These interlockings are the consequence of the logic capacity pointed out in the following sections.

The execution of internal interlockings implies being able to obtain logic outputs of permission / blocking of commands towards the external circuits according to the combination of the state of various input signals through logic gates. These processed logic signals affect the permissions / lockouts of commands generated both from the unit's local control module and from the Central Unit originating in the control display, central programmable control functions and/or remote.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Logical alarms can be generated with data from the combination of the state of various input signals through logic gates as well as from "timers" of presence / absence of a given signal, either physical or logic.

The processing of analog signals offers the possibility of comparing analog inputs with set points and of generating digital ON/OFF signals as a result of this comparison as well as the possibility of adding and multiplying analog signals. Analog values can be used in primary or secondary values.

Logic configurations can also generate user defined values such as counters. These values are the result of the user defined logic algorithms. User defined values can be displayed on the HMI, sent via communications and retrieved using ***ZIV e-NET tool***®.

Likewise, it is also possible to define new user settings in the IED associated with the logic. These settings can be consulted afterwards from the HMI or communications.

In addition, the logic configurations can disable protection elements of the IED. The disabling of an element allows it to be replaced by another that operates under user-defined algorithms.

Basically, the system takes input signals from various sources, both external to the IED (communications or HMI) and internal; processes these signals according to the configuration that has been loaded and the pre-established settings and activates certain output signals that will be used for sending information messages or measurements to the central unit as well as commands to relays, LEDs and protection or logic units.

The **Programmable Logic** and its **Configuration** comprise the engine of this whole system. The logic has a set of *blocks* that encompass a series of logic operations. Each of these blocks determines an *outcome* (state of one or more signals) depending on the state of the inputs of that *block*. The **Configuration** determines the use of one or another *block*.

If the required input signals are signals that arrive through communications, they arrive encoded according to the PROCOME, MODBUS or DNP 3.0 communications protocol, which forces associating each necessary signal with its corresponding protocol. This process is performed in **Input Tagging** and the associations are made in one form or another according to the configuration. The same happens with the signals sent through communications; the software process is carried out in **Output Tagging** and is also determined by the Configuration.

New logic-generated values can be redirected to the IED's different communication protocols as well as to the HMI.

The **Programmable Logic** can be used to generate events with any available digital signal that the IED can capture with the PROCOME communications protocol and the program. It doesn't matter if this signal is a digital input or a signal received via communications from the central unit or, on the contrary, is the outcome of internal operations included in the programmed algorithm itself. Moreover, there is the option of recording the event by the rising edge of the chosen signal, by the falling edge or by both.

Once the event is generated, it can be captured the same as the rest of the events generated by the IED (as, for example, trip events) with the ***ZIV e-NET tool***® communications program.

There is an exclusive option to simplify the task of configuring the Digital Inputs, Digital Outputs and LEDs. This voids the need to work with complex algorithms that would make the task unnecessarily difficult.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.3 Control Commands

The system uses **ON** / **OFF** action groups. In this way, when a command is configured through the configuration program, action groups are defined, also called logic actions (ON, OFF…) and then, for each action group, as many physical actions as the user requires, up to a maximum of 256. For the rest of the configuration, when an actual action is to be run, the action group is selected (not the action linked to the pulse signal, but the logic action).

Every command element has an operating time setting (*opertimeout*). One setting may not be allocated to several different commands.

4.7.3.a Command or Source Hierarchy

For protocol configuration, the user must select the source from which the group action is run. By default, this value is Station-Control (2) or HMI.

In this way, the relay will be able to manage the source knowing the source of each command with no need to configure it in the logic.

This new configuration mechanism is intended to use only one ON action (and other OFF action) with all possible sources. However, for non-IEC61850 protocols, command sources cannot be discerned, since only one signal is activated when the single ON (and OFF) action to be configured is run. Therefore, as many ON (and OFF) actions must be configured as sources to be discerned, if required, assigning different signals to activate. Specific cases are analyzed:

- Sources 1 and 4 made from the logic through the COMMAND opcode can be controlled through logic.
- Source 1 from HMI can be controlled by logic looking at the simultaneity of signals ControlLocal = 1 and the Signal to be Activated.
- Source 7 can be controlled by logic looking at the simultaneity of signals ControlMaintenance = 1 and the Signal to be Activated.
- Source 2 can be controlled by logic looking at the simultaneity of signals ControlPanel = 1 and the Signal to be Activated.
- Source 3 can be controlled by logic looking at the simultaneity of signals Remote Control = 1 and the Signal to be Activated.
- Sources 5 and 6 can be framed the same as sources 2 and 3, respectively, otherwise they must be discerned (the first will be HMI and the second, remote control). If it must be discerned whether it is a control function or not, specific actions must be defined for sources 5 and 6 (it seems the latter has not been used until now).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.3.b Successful and Failed Command Signals

For single and dual commands, the relay will automatically allocate a value to the success and failure signals configured through the ***ZIV e-NET tool***®. This will be arranged by the relay as a function of the command and action group (**ON / OFF**) status signal. Once the command has been run, whether successfully or not, a pulse will be generated in the corresponding **Success signal** / **Failure signal** allocated through the configuration program of long enough duration to be detected by all the possible clients (logic, LEDs, protocols…). The duration will be 22ms.

These signals, designated **Successful signal** / **Failure signal**, will be marked as used and may only be designated as **Successful signal** / **Failure signal** in the same command group (**ON / OFF**), for the same or different actions. The same signal can be used for success and failure.

4.7.3.c Running simultaneous Commands

The relay has a setting, ***Simultaneous commands*** (General Settings), to allow or not to allow running simultaneous commands. The relay operation as a function of the new setting is as follows:

- **NO**: the relay will allow running a single command at a time. Once the command is received, any other command received will be rejected until the command in progress is completed, whether satisfactorily or not. Namely, when there is a command in progress, new commands are not allowed.
- **YES**: the relay allows concurrent commands, except if they are over the same logic element, in which case they will be rejected. The command will start running once the action of the previous command has been initiated, and may be queued or run up to a maximum of 32 concurrent commands.

4.7.3.d Command Treatment

When commands are run, concurrent conditions are checked 2 times. This is intended to provide greater reliability upon changing conditions since the command is received until the moment when it is finally to be run. The command is deemed to have progressed only if no running problems occur. Blocking is only checked once, since it is a function of the status and this changes all the time. In this way, the command running process is as follows:

1. Assessment of concurrent conditions. Progress goes on in any case.
2. Blocking conditions are examined. If blocking occurs, an error is issued.
3. If the above concurrent conditions are not met, a concurrent error is issued.
4. A non-interruptible area is entered in real time.
5. Concurrent conditions are reassessed. If they are not met, an error is issued.
6. Activation of the command being run (which will prevent new commands from entering).
7. An interruptible area is entered again.
8. Command pulse activation (if the complete process above has been satisfactory).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

In this way, always:

- Concurrent conditions are checked 2 times. First, before the command. Then, in a no longer interruptible area, to verify that it has not changed and that the command can still execute.
- The command is deemed to have progressed only if no running problems occur.
- Blocking is only checked once, in concurrent conditions. The reason is that the block depends on the status and this changes all the time. If evaluated at the beginning, when executing the command later there could already be a blocking.

In either case, a new signal indicating, at all times, that a Command is running is available (either an analog or digital Command). With the ***Simultaneous Commands*** to YES, this signal could be added by setting to blocking all the commands.

4.7.3.e Command Blocking as a Function of the Hierarchy

Local-Control	Maintenance-Control	Panel-Control	Remote-Control	Bay-control (1)	Station-control (2)	Remote-control (3)	Automatic-bay (4)	Automatic-station (5)	Automatic-remote(6)	Maintenance (7)	Process (8)
0	0	0	0	BLOCKED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
0	0	0	1	BLOCKED	BLOCKED	ALLOWED	ALLOWED	BLOCKED	ALLOWED	BLOCKED	ALLOWED
0	0	1	0	BLOCKED	ALLOWED	BLOCKED	ALLOWED	ALLOWED	BLOCKED	BLOCKED	ALLOWED
0	0	1	1	BLOCKED	ALLOWED	ALLOWED	ALLOWED	ALLOWED	ALLOWED	BLOCKED	ALLOWED
0	1	0	0	BLOCKED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	ALLOWED	ALLOWED
0	1	0	1	BLOCKED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	ALLOWED	ALLOWED
0	1	1	0	BLOCKED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	ALLOWED	ALLOWED
0	1	1	1	BLOCKED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	ALLOWED	ALLOWED
1	0	0	0	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	0	0	1	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	0	1	0	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	0	1	1	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	1	0	0	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	1	0	1	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	1	1	0	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED
1	1	1	1	ALLOWED	BLOCKED	BLOCKED	ALLOWED	BLOCKED	BLOCKED	BLOCKED	ALLOWED

PanelControl signals (these will be mapped through configuration to the command that LLN0.LocSta in IEC 61850 is finally linked to) and **Remote Control** can be both 0 or both 1.

LocalControl has full priority, then **MaintenanceControl** and, finally, the other two with the same priority (**LocalControl** and **Remote Control**).

The table has two exceptions to be dealt with when the commands are sent through communications:

1) When **LocalControl** ("LLN0.Loc" in IEC 61850) is set to **TRUE**, all commands sent through communications will be rejected, indicating in *IEC 61850 AddCause=Blocked-by-switching-hierarchy*, regardless the source (including source 1).
2) Source 4 (Automatic-Bay) will never be allowed from communications. It will always be rejected. These are always commands made in the relay logic, namely, always with source in the relay. Therefore, they are not allowed through communications.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.4 Description of Logic Operations

For each configuration, only the logic functions indicated in the profile of the model being configured will be available. This section describes the logic functions defined for the different **ZIV** models.

The value of a signal or variable can be allocated directly to another variable of the same type by connecting the two variables with no need for using intermediate logic operators. The value of a variable can be allocated to several variables.

4.7.4.a Boolean Operations (Booleans)

AND: AND operation between digital inputs.

Operands	From 2 up to a maximum of 16 digital inputs.			
Results	1 digital output.			
Truth table for two inputs	In0	In1	Q	
	0	0	0	
	0	1	0	
	1	0	0	
	1	1	1	

OR: OR operation between digital inputs.

Operands	From 2 up to a maximum of 16 digital inputs.			
Results	1 digital output.			
Truth table for two inputs	In0	In1	Q	
	0	0	0	
	0	1	1	
	1	0	1	
	1	1	1	

XOR: OR operation-exclusive between two digital inputs.

Operands	2 digital inputs.			
Results	1 digital output.			
Truth table for two inputs	In0	In1	Q	
	0	0	0	
	0	1	1	
	1	0	1	
	1	1	0	

NOT: moves the digital input negation result to the digital output.

Operands	1 digital input.		
Results	1 digital output.		
Truth table for two inputs	In	Q	
	0	1	
	1	0	

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.4.b Move Instructions

BCD_TO_DINT: BCD to integer.

This opcode sets up the value of an integer analog output from a number of digital inputs.

Operands	Up to 16 digital inputs (I0..I15).
Results	1 Integer type Analog Output resulting from the operation: Q=(I0+(I1<<1)+(I2<<2)+(I2<<3))+ (I3+(I4<<1)+(I5<<2)+(I6<<3))*10+...

BCD_TO_REAL: BCD to real.

This opcode sets up the value of a floating type analog output from a number of digital inputs.

Operands	Up to 16 digital inputs (I0..I15).
Results	1 Floating type Analog Output resulting from the operation: Q=(I0+(I1<<1)+(I2<<2)+(I2<<3))+ (I3+(I4<<1)+(I5<<2)+(I6<<3))*10+...

BIN_TO_DINT: Binary to integer.

This opcode sets up the value of an integer analog output from a number of digital inputs.

Operands	Up to 16 digital inputs (I0..I15).
Results	1 Integer type Analog Output resulting from the operation: Q=I0+(I1<<1)+(I2<<2)+...(IN<<N+1)

BIN_TO_REAL: Binary to real.

This opcode sets up the value of a floating type analog output from a number of digital inputs.

Operands	Up to 16 digital inputs (I0..I15).
Results	1 Floating type Analog Output resulting from the operation: Q=I0+(I1<<1)+(I2<<2)+...(IN<<N+1)

BOOL_TO_DINT: Boolean to integer.

This opcode converts a boolean value into an integer (0 or 1).

Operands	1 boolean input.
Results	1 Integer type Analog Output.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

BOOL_TO_REAL: Boolean to real.

This opcode converts a boolean value into a real number (0 or 1).

Operands	1 boolean input.
Results	1 Real type Analog Output.

DINT_TO_BCD: Integer to BCD.

This opcode, from an integer type analog input, sets up the value of a number of digital outputs representing the integer value of the magnitude in BCD format.

Operands	An integer type analog input.
Results	From 1 up to 16 digital outputs (Q0, Q1,...,Q15).

DINT_TO_Bin: Integer to binary.

This opcode, from an integer type analog input, sets up the value of a number of digital outputs representing the integer value of the magnitude in Binary format.

Operands	An integer type analog input.
Results	From 1 up to 16 digital outputs (Q0, Q1,...,Q15).

MUX: multiplexor.

Based on a selector, sets up the output value with the value of one of both inputs. Input type (no selector) must match the output type.

Operands	1 digital input acting as selector (SEL). 2 inputs (I0, I1).		
Results	Q = 1 Output.		
Truth table for two inputs	***Sel***	Q	
	0	***E0***	
	1	***E1***	

REAL_TO_BCD: Real to BCD

This opcode, sets up, from a real type analog input, the value of a number of digital outputs representing the integer value of the magnitude in BCD format.

Operands	Integer type analog input
Results	From 1 up to 16 digital outputs (Q0, Q1,...,Q15).

REAL_TO_Bin: Binary to real.

This opcode, sets up, from a real type analog input, the value of a number of digital outputs representing the integer value of the input.

Operands	A real type analog input.
Results	From 1 up to 16 digital outputs (Q0, Q1,...,Q15).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

VALID:

The digital output is set to 1 whenever the input has a valid value. Otherwise, the output is set to 0.

Operands	IN = analog input (measure, setting or analog constant).
Results	Q = Digital output (1, if valid input; 0, otherwise).

4.7.4.c Pulse Activation Operations (Triggers)

FFD: D type latch.

Every time a rising edge is produced in the digital input displayed as a clock, the latch takes the input value.

Operands	1 clock digital input. Digital input.				
Results	1 digital output.				
Truth table		**E**	**CLK**	Q	
		0	↑	0	
		1	↑	1	

FFDmem:

Same parameters and operation as for the FFD logic operation. The only difference resides in that, in this case, the value is memorized.

FFRS: RS type latch.

While the S digital input is activated, the latch takes the input value. When the R input is activated, the latch takes the value 0.

Operands	1 digital input R. 1 digital input S..				
Results	1 digital output				
Truth table		**R**	**S**	Qt+ Δt	
		0	0	Qt	
		0	1	1	
		1	0	0	
		1	1	1	

FFRSmem:

Same parameters and operation as for the FFRS logic operation. The only difference resides in that, in this case, the value is memorized.

PLSTRAIN : Pulse train.

This opcode is a logic block that produces a pulse train while the digital input is active.

Operands	1 digital input for pulse train activation. 1 analog input indicating the time of the active pulse in seconds (TM1). 1 analog input indicating the time of inactive pulse in seconds (TM0).
Results	1 digital output.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

PLSTRAINmem: pulse train memorized.

Same parameters and operation as for PLSTRAIN logic operation. The only difference resides in that, in this case, the value is memorized.

PULSE:

When the digital input switches from 0 to 1, the output activates during the time specified as parameter.

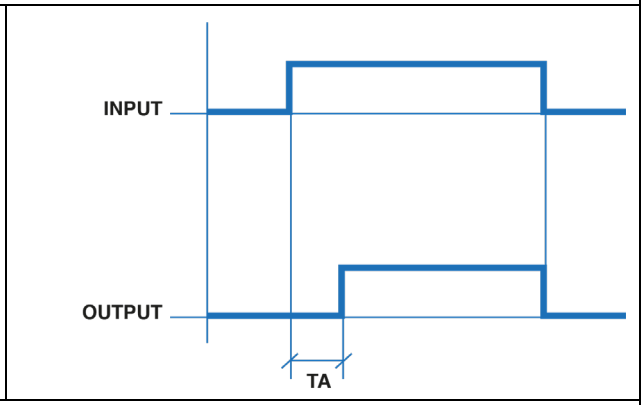
Operands	1 digital input. 1 analog setting or pulse time constant in seconds (TM).
Results	1 digital output.
Limits	The maximum time must be set between 0.0 and 2147483.648 seconds (24 days).

PULSEmem:

Same parameters and operation as for PULSE logic operation. The only difference resides in that, in this case, the value is memorized.

TMA: A- Timer.

When the setting value of the time elapsed since the digital input switches from 0 to 1 times out, the output sets to 1 provided the input is not reset.

Operands	1 digital input 1 setting or delay time constant in seconds
Results	1 digital output
Operating diagram	
Limits	The maximum time must be set between 0.0 and 2147483.648 seconds (24 days).

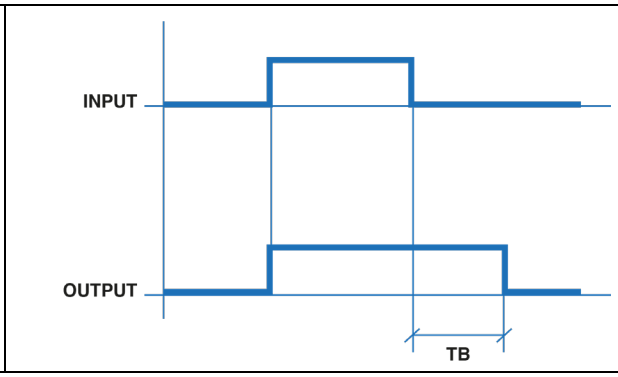
TMAmem:

Same parameters and operation as for TMA logic operation. The only difference resides in that, in this case, the value is memorized.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

TMB: B- Timer.

When the setting value of the time elapsed since the digital input switches from 1 to 0 times out, the output sets to 0 provided the input is not reset.

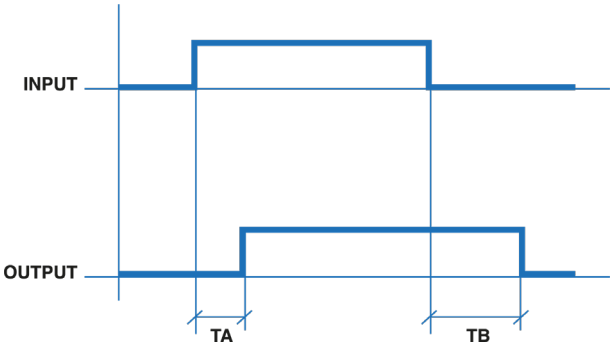
Operands	1 digital input. 1 setting or delay time constant in seconds.
Results	1 digital output.
Operating diagram	
Limits	The maximum time must be set between 0.0 and 2147483.648 seconds (24 days).

TMBmem:

Same parameters and operation as for TMB logic operation. The only difference resides in that, in this case, the value is memorized.

TEMPOR:

Timer to configure both the start of output activation and deactivation time.

Operands	IN: 1 digital input. TA: 1 setting or delay time constant in seconds. TB: 1 setting or reset time constant in seconds.
Results	Q: 1 digital output
Operating diagram	

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

R_TRIG: Rising edge:

This opcode activates the digital output when detecting the switching of the digital input from 0 to 1.

Operands	1 digital input.
Results	1 digital output.

4.7.4.d Counters

COUNT_I: Counter (integer).

This opcode handles a counter that increments with each rising edge of the digital input displayed as a clock. When the reset input activates, the counter resets to 0. The output is an integer type analog signal.

Operands	1 reset digital input (RST). 1 clock digital input (CLK).
Results	1 Integer type Analog Output.
Limits	The counter saturates at 65535. Later increments do not change the counter output value.

COUNTmem_I: Counter (integer - memorized).

This opcode handles a counter that increments with each rising edge of the digital input displayed as a clock. When the reset input activates, the counter resets to 0. The difference with the COUNT_I opcode resides in that, in this case, the output is memorized.

COUNT_R: Counter (real).

This opcode handles a counter that increments with each rising edge of the digital input displayed as a clock. When the reset input activates, the counter resets to 0. The output is a floating (= real) type analog signal.

Operands	1 reset digital input (RST). 1 clock digital input (CLK).
Results	1 Float Analog Output.
Limits	The counter saturates at 65535. Later increments do not change the counter output value.

COUNTmem_R: Counter (real - memorized).

This opcode handles a counter that increments with each rising edge of the digital input displayed as a clock. When the reset input activates, the counter resets to 0. The difference with the COUNT_R opcode resides in that, in this case, the output is memorized. The same as for the case above, the analog output is floating (= real) type.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.4.e Arithmetic Operations

+ : Addition.

This opcode sets up the value of the analog output with the result of the sum of analog inputs.

Operands	2 Analog inputs.
Results	1 Analog output.

- : Subtraction.

This opcode sets up the value of the analog output with the result of the subtraction of analog inputs.

Operands	2 Analog inputs (minuend IN1 and subtrahend IN2).
Results	1 Analog output.

* : Multiply.

This opcode sets up the value of the analog output with the result of the product of analog inputs.

Operands	2 Analog inputs.
Results	1 Analog output.

/ : Divide.

This opcode sets up the value of the analog output with the result of the division between analog inputs.

Operands	2 Analog inputs.
Results	1 Analog output.

- **Comparison Operations**

< : Less Than.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is less than IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

<= : Less or Equal.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is less than IN2, or IN1 is equal to IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

<> : Is not equal.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is not equal to IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

= : Is Equal.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is equal to IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

> : Greater than.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is greater than IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

>= : Greater or equal.

This opcode compares two analog inputs IN1 and IN2, and sets up the value of the digital output based on the result of the comparison. If IN1 is equal to or greater than IN2, the digital output activates. Otherwise, the output sets to 0.

Operands	2 Analog inputs.
Results	1 digital output.

CMPCONT: Counter Comparator.

Compares the value of the counter CON input with the value defined in the Vc input. If the comparison is greater or equal, the output activates. Otherwise, the output deactivates.

Operands	1 DINT (CON) type counter input. 1 input Vc.
Results	1 digital output Q.
Operating logic	If CON >= Vc Q activates. If CON<Vc Q deactivates.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

DNIVEL: Range evaluator.

It works as follows: takes the value of the field measurement (represented in MEA input), and compares it with the inputs Vc (equal), Vmin (less than) and Vmax (greater than), such that:

If [MEA] >= Vmax => the GT output signal activates.
If [MEA] = Vc => the EQ output signal activates.
If [MEA] <= Vmin => the LT output signal activates.

Operands	1 measurement type input (REAL) (MEA). 1 REAL input Vmax. 1 REAL input Vc. 1 REAL input Vmin.
Results	1 digital output GT. 1 digital output EQ. 1 digital output LT.
Operating logic	If [MEA] >= Vmax => output signal activates GT. If [MEA] = Vc => the EQ output signal activates. If [MEA] <= Vmin => the LT output signal activates.

LVCOMP: Level comparator.

This opcode compares the analog input with respect to a minimum and maximum reference value with respect to a minimum and maximum reference value, and sets up the digital output based on the same. Thus:

The output sets to 1 if the input is greater than the maximum reference value.
The output sets to 0 if the input is less than the minimum reference value.
Otherwise, the output remains with the same value.

Operands	1 Analog input IN. One analog input as minimum reference value (Min). One analog input as maximum reference value (Max).
Results	1 digital output1 digital output LT.

LVCOMPmem: Level comparator (memorized).

Same as for LVCOMP with the only difference that, in this case, the output is memorized.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.7.4.f Special Operations

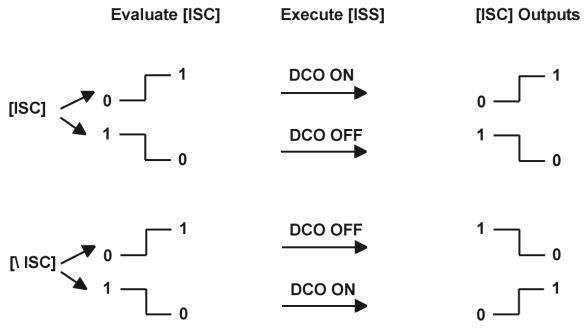
DEACT:

This function activates the digital output if and only if there is only a single active input. Otherwise, the output deactivates.

Operands	Up to 16 possible digital inputs (IN0..IN15).				
Results	1 digital output.				
Truth table (specific case with 3 inputs)	**IN0**	**IN1**	**IN2**	Q	
	0	0	0	0	
	0	0	1	1	
	0	1	0	1	
	0	1	1	0	
	1	0	0	1	
	1	0	1	0	
	1	1	0	0	
	1	1	1	0	

ESC:

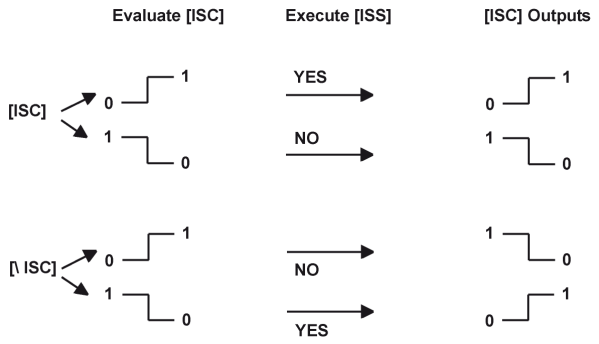
This logic function writes ISS outputs with the DCO_ON if the ISC signal is active and writes ISS outputs with the DCO_OFF if the ISC input signal is inactive. Also, the value of the ISC input is allocated to the outputs.

Operands	1 ISC digital input to activate / deactivate the ISS output writing. 1 digital input that represents the ISS or output writing over which the command is run. 1 setting or integer constant that sets the value of the DCO_ON with which the command is run, if the input ISC is active. 1 setting or integer constant that sets the value of the DCO_OFF with which the command is run, if the input ISC is inactive.
Results	Up to 32 possible digital outputs. When the command is run, these outputs take the value of the input ISC.
Operating diagram	

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

COMMAND:

This logic function (FB)runs the ISE input command with the DCO specified, and the value of the input ISC is allocated to the outputs, every time the ISC input is activated (namely, switches from 0 to 1) or deactivated in case the input is negated. For the ISE input, only commands (or ISEs signals) of the central unit database not belonging to the “LOGICA” logic equipment are allowed, since it makes no sense that an equipment issues a command on itself.

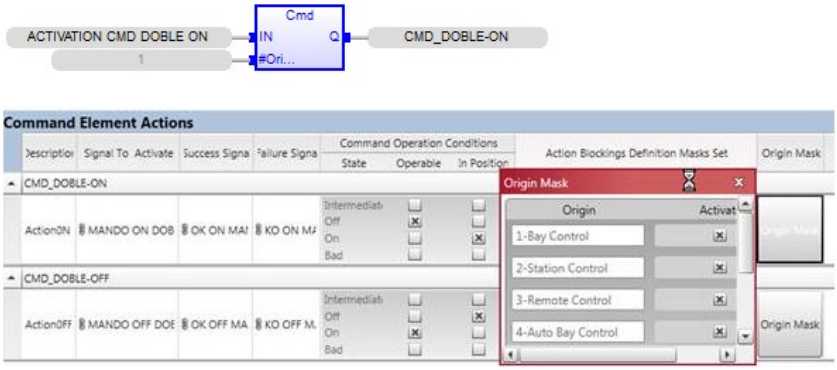
Operands	1 ISC digital input to activate the command. 1 digital input representing the ISE or signal on which the command is issued. 1 setting or integer constant that defines the DCO with which the command is run.
Results	Up to 32 possible digital outputs. When the command is run, these outputs take the value of the input ISC.
Operating diagram	

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **Command Operations**

Cmd:

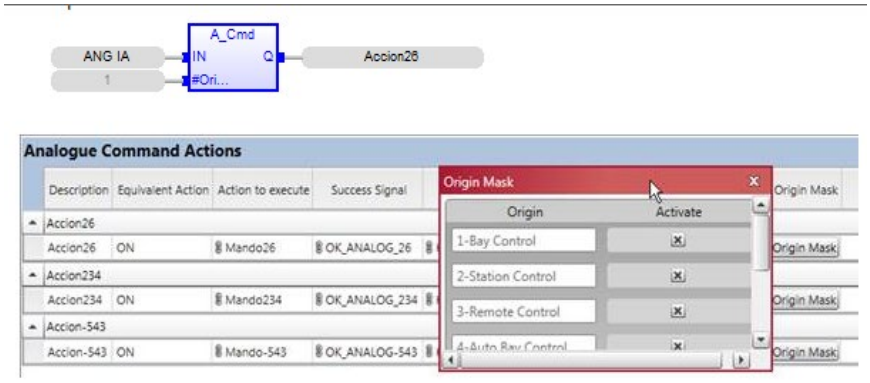
This function block tries to execute a command action whenever the input is activated.

Operands	Two Inputs: Digital input used to trigger the command. Integer input which represents the origin for the execution of the command. It is a numeric identifier which corresponds to the identifier used in IEC-61850. When returning from the Logic Editor, the application will reject any value which is not considered as a valid origin within the equipment.
Results	A single output which corresponds to the "Action Group" of the digital command which wants to be executed.
Operation logic	When there is activation of the input signal IN (by rising edge) the function block triggers the "digital command action group" indicated in output Q. This results in the generation of a pulse in the signal configured as "Signal to activate" which corresponds to the first action with the origin indicated in input '#Origin' set from all of the actions in the group action indicated in the output Q. (Note: The pulse will be generated, provided the action is not blocked and the state of the command allows the action to take place). Example:  When signal "Activation CMD Doble ON" is activated, group action "CMD_DOBLE-ON" with origin = 1 is triggered. That means that the equipment will look for the action, in group action "CMD_DOBLE-ON", which has the origin "1 (Bay control)" set in the origin mask. Once the action is located, the equipment will try to generate a pulse in the signal configured in "Signal to activate". In the example, the equipment will try to generate a pulse over signal "Mando ON Doble". Should there be more than one action with #Origin set in the origin mask, only the first action found with that origin will be executed. Should there be no action with #Origin set in the origin mask, no action will be executed.

M0RTFA1902I
RTF: Automatic Voltage Regulator
© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

A-Cmd:

This function attempts to execute an analog command action when the analog input value changes.

Operands	Two Inputs: Analogue input which triggers the command. Integer input which represents the origin for the execution of the command. It is a numeric identifier which corresponds to the identifier used in IEC-61850. When returning from the Logic Editor, the application will reject any value which is not considered as a valid origin within the equipment.
Results	A single output which corresponds to the "Action Group" of the analogue command which wants to be executed.
Operation logic	When the value of the analogue input signal IN (by rising edge) changes, the function block triggers the "analogue command action group" indicated in output Q. This results in the signal configured as "Signal to activate", which corresponds to the first action with the origin indicated in input '#Origin' set from all of the actions in the group action indicated in the output Q, to take the same value as the one in input IN. (Note: The value will be assigned to the analogue signal provided the action is not blocked and the state of the command allows the action to take place). Example:  When the value of "Ang IA" is modiifed, group action "Accion26" is triggered with origin 1 (Bay Control). The equipment will look for the first action with the origin 1 set in its origin mask. If found, the value of the input IN, in this case the value of "Ang IA" will be copied into "Mando26" which is the "Action to execute" configured for action "Accion26". Should there be more than one action with #Origin set in the origin mask, only the first action found with that origin will be executed. Should there be no action with #Origin set in the origin mask, no action will be executed.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

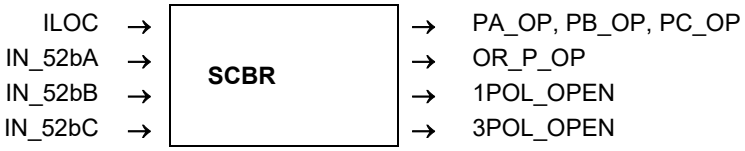
4.8 Open Pole Detector

4.8.1 Identification 4.8-2
4.8.2 General Block 4.8-2
4.8.3 Operation Principles and Block Diagram 4.8-2
4.8.4 Setting Ranges 4.8-4
4.8.5 Analog Inputs to the Unit 4.8-4
4.8.6 Digital Inputs to the Open Pole Module 4.8-4
4.8.7 Auxiliary Outputs and Events of the Open Pole Module 4.8-5
4.8.8 IEC 61850 Logical Node 4.8-5

4.8.1 Identification

Description of the Protection Element	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Open Pole Detector	SCBR1		

4.8.2 General Block



4.8.3 Operation Principles and Block Diagram

This unit detects the opening of any pole of the breaker, generating the corresponding outputs (**Pole A Open**, **Pole B Open** and **Pole C Open**), based not only on the condition of the breaker position contacts but also on the output of the undercurrent detector, whose level is given by the ***Pole Open Current*** setting. With the aperture indication outputs of each pole, the open pole detector also generates the following outputs: **One Pole Open**, **Three Poles Open** or **Any Pole Open**.

The outputs of this unit are used by other units which carry out modifications in the operating logic to adapt to the new situation which causes the opening of any pole of the breaker.

The Open Pole Detector can operate based on two operating logics, exclusive within themselves, each of which can be selected through the ***Num Brk Pos Inputs*** setting. If this setting takes the value **3 Inputs**, the operating logic will be the following:

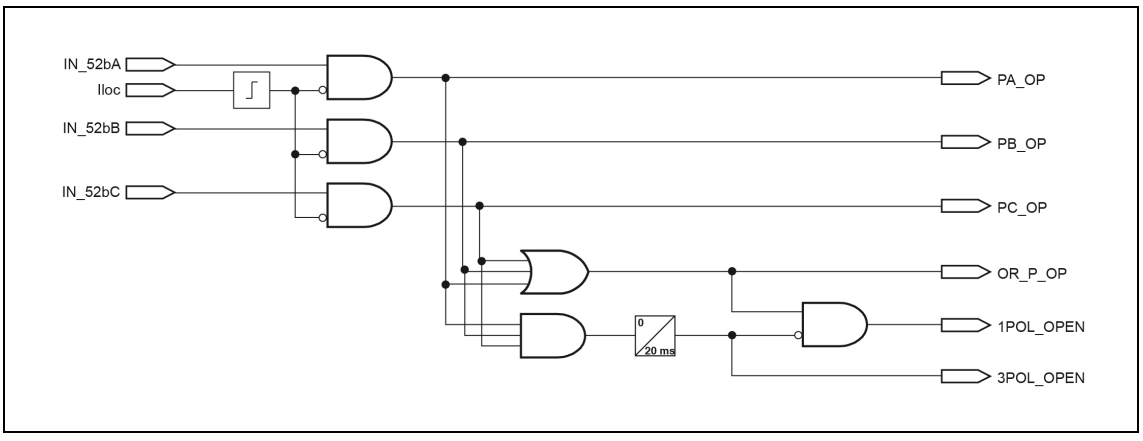


Figure 4.8.1 Logic Diagram of the Open Pole Detector with 3 Inputs.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Legend	
IN_52bX: Open X Pole Position Input.	1POL_OPEN: One Pole Open.
PX_OP: Pole X Open.	3POL_OPEN: Three Poles Open.
OR_P_OP: Any Pole Open.	

IN_52bA, **IN_52bB** e **IN_52bC** inputs are designed to receive breaker **52b** normally closed contact state. However, using programmable logic, said logic inputs could receive breaker 52a contact (use operator NOT) or both **52b** and **52a** contacts (use operators NOT and AND) state.

The reset time of 20 ms associated with the **Three Poles Open** (**3POL_OPEN**) signal will be used to avoid transient activation of the **One Pole Open** (**1POL_OPEN**) signal in case of imbalances which arise in a three-phase reclose.

If the ***Num Brk Pos Inputs*** setting takes the value **2 Inputs**, the operating logic used becomes the following:

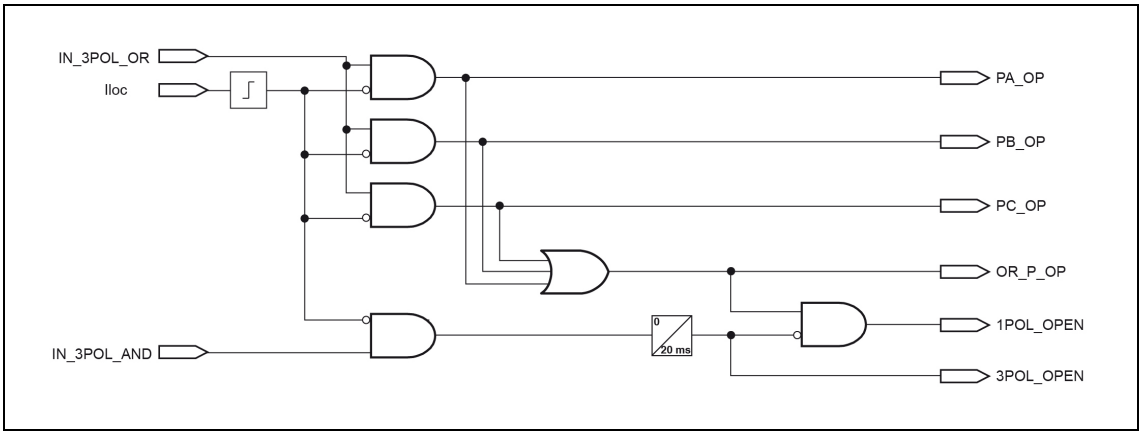


Figure 4.8.2 Logic Diagram of the Open Pole Detector with 2 Inputs.

Legend	
IN_3POL_OR: One Pole Open Input.	OR_P_OP: Any Pole Open.
IN_3POL_AND: Three Poles Open Input.	1POL_OPEN: One Pole Open.
PX_OP: Pole X Open.	3POL_OPEN: Three Poles Open.

This logic allows using one less input than the logic above. Inputs **IN_3POL_OR** and **IN_3POL_AND** are designed to receive one **OR** and one **AND,** respectively, from the breaker **52b** normally closed contacts. However, using programmable logic, one OR and one AND from the **52 a** normally open contacts or both **52b** and **52a** contacts can also be assigned.

The reset time of 20 ms associated with the **Three Poles Open** (**3POL_OPEN**) signal is used, as in the previous logic, to avoid transient activation of the **One Pole Open** (**1POL_OPEN**) signal in case of imbalances which occur in a three-phase reclose.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.8.4 Setting Ranges

Metering / Open Pole Logic					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Num Brk Pos Inputs	Open Pole Selection	SCBR1.NumIn	3 INPUTS 2 INPUTS		3 INP.
Pole Open Current	Pole Open Current	SCBR1.OpnA	0,04 - 0,8 A	0,01 A	0,04

4.8.5 Analog Inputs to the Unit

Table 4.8-1: Analog Inputs to the Open Pole Module		
Name	**Description**	**IEC 61850**
ILOC	Local current	MMXU.AmpLoc

4.8.6 Digital Inputs to the Open Pole Module

Table 4.8-2: Digital Inputs to the Open Pole Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
IN_52bA	Breaker Control	SCBR1.CBInA	Pole A Open Input	I	Activation of this input indicates that the 52b contact of (A/B/C) pole position of the breaker is closed.
IN_52bB		SCBR1.CBInB	Pole B Open Input	I	
IN_52bC		SCBR1.CBInC	Pole C Open Input	I	
IN_3POL_AND		SCBR1.CBInAND	Three Poles Open Input	I	The activation of this input indicates that the three 52b contacts of the pole position of the breaker are closed.
IN_3POL_OR		SCBR1.CBInOR	Any Pole Open Input	I	The activation of this input indicates that any 52b contact of the pole position of the breaker is closed.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.8.7 Auxiliary Outputs and Events of the Open Pole Module

Table 4.8-3: Auxiliary Outputs and Events of the Open Pole Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
PA_OP	Breaker Control	SCBR1.AnyPoleOpn	Pole A Open	I	Open (A / B / C) pole indication.
PB_OP		SCBR1.AnyPoleOpn	Pole B Open	I	
PC_OP		SCBR1.AnyPoleOpn	Pole C Open	I	
OR_P_OP		SCBR1.AnyPoleOpn	Any Pole Open	I	Any pole open indication.
1POL_OPEN		SCBR1.OnePoleOpn	One Pole Open	I	One pole open indication. It is also activated when 2 poles open.
3POL_OPEN		SCBR1.AllPoleOpn	Three Poles Open	I	Three poles open indication.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.8.8 IEC 61850 Logical Node

CLASS IRLSCBR		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status information		
CBInA	SPS	Breaker pole A open input
CBInB	SPS	Breaker pole B open input
CBInC	SPS	Breaker pole C open input
CBInOR	SPS	Breaker any pole open input
CBInAND	SPS	Breaker all pole open input
AnyPoleOpn	ACT	Breaker any pole open
OnePoleOpn	SPS	Breaker one pole open
AllPoleOpn	SPS	Breaker all pole open
Settings		
NumIn	ENG	Open Pole number of breaker inputs
OpnA	ASG	Open Pole current

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.9 Pole Discordance Detector

4.9.1 Identification 4.9-2
4.9.2 General Block 4.9-2
4.9.3 Operating Principles and Block Diagram 4.9-2
4.9.4 Setting Ranges 4.9-3
4.9.5 Digital Inputs to the Pole Discordance Detector Module 4.9-3
4.9.6 Auxiliary Outputs and Events of the Pole Discordance Detector Module 4.9-4
4.9.7 IEC 61850 Logical Node 4.9-4
4.9.8 Protection Element Test 4.9-5

4.9.1 Identification

Description of the Protection Element	Node IEC 61850	IEC 60617	ANSI/IEEE C37.2
Pole Discordance Detector	PPDS1		2

4.9.2 General Block



4.9.3 Operating Principles and Block Diagram

This unit is for the purpose of detecting a discordance in the position of the three breaker poles. If this condition is maintained during the **T_PD** (***Pole Discrep Delay***) time setting, the **TRIP_PD** (**Pole Discordance Detector Trip**) trip signal is generated. Given that the single-phase reclose cycles will produce a pole discordance condition, the **T_PD** time setting should be longer than the single-phase reclose time.

Figure 4.9.1 shows the operation diagram of the Pole Discordance Detector.

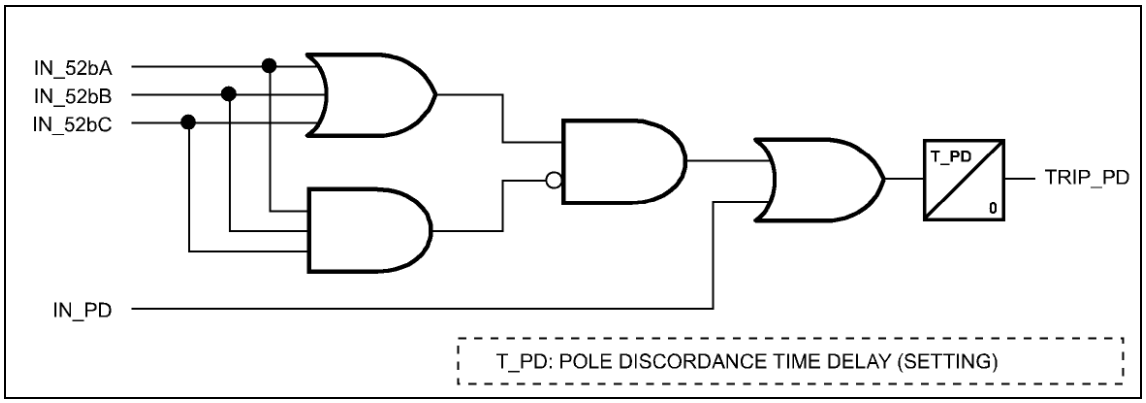


Figure 4.9.1 Diagram of the Pole Discordance Detector.

It will be possible to detect the existence of pole discordance from the status of the three digital inputs associated with the status of the three poles of the breaker (activated if the corresponding pole is open). Notwithstanding, many breakers incorporate a wiring logic in their control cabinets, which detects the pole discordance (based on the status of the **52aA/B/C** and **52bA/B/C** contacts), generating a signal in this case. For this reason, the IED incorporates a digital input, **IN_PD** (Pole Discordance Input), to receive this signal, which will directly activate the **TRIP_PD** output.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.9.4 Setting Ranges

Metering / Pole Discrepancy					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Enable Pole Discrep	Pole Discr Enable	PPDS1.LNInSvc	NO / YES		NO
Pole Discrep Delay	Pole discrep. Delay	PPDS1.OpDlTmms	0-50 s	0.01 s	2 s

4.9.5 Digital Inputs to the Pole Discordance Detector Module

Table 4.9-1: Digital Inputs to the Pole Discordance Detector Module

Name	Group	IEC 61850	Description	Vis.	Function
IN_52bA	Breaker Control	SCBR1.CBInA	Pole A Open Input	I	Activation of this input indicates that the 52b contact of (A/B/C) pole position of the breaker is closed.
IN_52bB		SCBR1.CBInB	Pole B Open Input	I	
IN_52bC		SCBR1.CBInC	Pole C Open Input	I	
IN_PD		PPDS1.PoleDscIn	Pole Discordance Input	I	Activation of this input directly generates the startup of the timer associated with the pole discordance detector.
ENBL_PD	Enabling Commands	PPDS1.Mod	Pole Discrepancy Enable Input	I	Activation of this input puts the unit into service. It can be assigned to status contact inputs by level or to a command from the communications protocol or from the HMI. The default value of this logic input signal is a “1.”

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.9.6 Auxiliary Outputs and Events of the Pole Discordance Detector Module

Table 4.9-2: Auxiliary Outputs and Events of the Pole Discordance Detector Module					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
TRIP_PD	Breaker Control	PPDS1.Op	Pole Discrepancy Trip	I, F	Trip of the Unit.
PD_ENBLD		PPDS1.Mod	Pole Discrepancy Enabled	I	Indication of enabled or disabled status of the unit.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

4.9.7 IEC 61850 Logical Node

CLASS IRLPPSD		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Status		
Op	ACT	Operation
PoleDscIn	SPS	Pole Discrepancy Input
Settings		
LnInSvc	SPG	In service
OpDlTmms	ING	Time delay

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

4.9.8 Protection Element Test

The following indicators will be monitored during the test:

In the display on the **Information** - **Status** - **Measuring elements** - **Pole Discordance** screen, or on the status screen of the ***ZIV e-NET tool***® (**Status** - **Elements** - **Pole Discordance**).

The Pole Discordance Detector will be enabled and the remaining elements disabled.

Adjust the timing to 10 s.

Activate the **Pole A Open Input**, without the **Pole B Open Input** and **Pole C Open Input** inputs being active. Verify that a three-phase trip due to pole discordance is produced after 10 s.

Repeat the test with the **Pole A Open Input** and **Pole B Open Input** active without the **Pole C Open Input** active. Verify that a three-phase trip due to pole discordance is produced after 10 s.

Activate the **Pole Discordance Input** and verify that a three-phase trip due to pole discordance is produced after 10 s.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Chapter 5.

Records

5.1 Oscillographic Recording

5.1.1 Operation Principles 5.1-2
5.1.2 Capture Function 5.1-2
5.1.3 Stored Data 5.1-2
5.1.4 Number of Channels and Digital Signals 5.1-2
5.1.5 Start Function 5.1-3
5.1.6 Oscillograph Deletion Function 5.1-3
5.1.7 Pre-Fault Time 5.1-3
5.1.8 Length of the Oscillograph 5.1-4
5.1.9 Setting Ranges 5.1-4
5.1.10 Digital Inputs of the Oscillographic Recording 5.1-5
5.1.11 Auxiliary Outputs and Events of the Oscillographic Recording 5.1-6
5.1.12 IEC 61850 Logical Node 5.1-6

5.1.1 Operation Principles

The Oscillography function is composed of two different sub functions: **Capture** and **Display**. The first captures and stores protection data inside the IED and is part of the relay's software; the second retrieves and presents the stored data graphically with one or more programs running on a PC connected to the protection.

For 50Kz, sampling and storage frequency is 4800Hz (96 samples per cycle) with 15 seconds of maximum storage per oscillo (14.5 seconds of fault and 0.5 seconds of pre-fault, both adjustable times) and 100 seconds of total memory storage and 64 files. Permanence of the information, with the IED disconnected from the power supply, is guaranteed since the IED stores the information in non-volatile Flash memory with cache in RAM.

The IEDs come with a display and analysis program, because the waveform records are in binary COMTRADE format according to IEEE standard C37.111-1999. The COMTRADE file generated considers the changes in frequency that can occur in the system, so that the analog magnitudes are stored with complete fidelity to how they have evolved on the system.

5.1.2 Capture Function

It is possible to record measured analog values, *User Defined Magnitudes*, digital inputs to the IED, internal logic signals generated by the protection and the programmable logic up to a total of 64 oscillographs in cyclical memory.

5.1.3 Stored Data

The following data are stored with a resolution time equal to the sampling rate:

- Value of the samples of the selected parameters (measured and *User Defined*) and of the digital and analogical signals programmed for this purpose.
- Time stamp of the Oscillography startup.

When there is no angle reference magnitude, all angles will be displayed in the relay with an invalid value (***) and the oscillogram will display them at 0˚.

5.1.4 Number of Channels and Digital Signals

It is possible to record all the analog inputs, eight (8). In addition, up to a maximum of 16 additional *User Defined Magnitudes* can be added.

User magnitudes are those selected from the magnitudes calculated by the relay, including the ones calculated under the programmable logic through ***ZIV e-NET tool***®.

Models with Power Supply Voltage Monitoring measure the voltage via a transducer input. This value is considered an *User Defined* value.

User Defined values include any type of parameters. If sine waves are recorded the Oscillography records the changes of the RMS value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Values are stored in the COMTRADE oscillography format with the label assigned in the programmable logic. The power supply voltage is stored with the label VDC.

It is also possible to assign direct metering from the analog channels as a *User Defined* value. Being waveforms the RMS value is stored. COMTRADE label is VALUE_u (ie. VA_u).

The maximum number of digital signals that can be registered is 160.

5.1.5 Start Function

The Start Function is determined by a programmable mask applied to certain internal signals (element pickups, open command, etc.) and to an External Pickup signal (which, if it is to be used, must be connected to any of the physical status contact inputs, to a programmable button of the HMI, to a command via communications or to a signal configured for this purpose in the programmable logic).

If the start function mask setting is **YES**, this signal activates the Oscillography startup. This signal will not start the Oscillography function if its mask setting is **NO**.

5.1.6 Oscillograph Deletion Function

Since the Oscillograph records are stored in non-volatile memory, there is a mechanism that allows deleting all the content of this memory externally.

The Oscillograph Deletion Function can operate by activating the **Deletion of Oscillographs** signal, which can be assigned by the programmable logic to any of the physical inputs, to a programmable button of the HMI, to a command via communications, etc.).

5.1.7 Pre-Fault Time

This is the length of pre-fault data that must be stored before the start function initiates a record. The setting range is from 0 to 0.5 seconds of pre-fault.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.1.8 Length of the Oscillograph

It is the duration time of the storage window. The number of records stored in memory varies and depends on the number of channels recorded and the length of the fault records. Once the recording memory is full, the next event will overwrite the oldest one stored.

The maximum number of oscillos is 64, the maximum length per oscillo is 15 seconds and the maximum memory 100 seconds. Depending on the length selected, the maximum number varies.

Set lenght in seconds	Max. number of oscillographs
15	6
10	10
7	14
...	...
3	33
1.56	64

5.1.9 Setting Ranges

Oscillography					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
PreStartup Length Seconds	`Pretrig. Length Seconds`	RDRE1.PreTmms	0 - 0.5 s	0.01 s	0.1 s
Length	`Postfault Length Seconds`	RDRE1.PstTmms	0.1 - 14.5 s	0.01 s	0.1 s

Trigger Mask			
Setting	**Step**	**Default**	**IEC 61850**
Phase Overvoltage	YES / NO	NO	RDRE1.PHTOVTrg
Underfrequency	YES / NO	NO	RDRE1.PTUFTrg
External Trigger	YES / NO	YES	RDRE1.ExTrg
Pole Discrepancy	YES / NO	YES	RDRE1.PPDSTrg
Voltage supervision overvoltage	YES / NO	NO	RDRE1.VDCOVTrg
Voltage supervision undervoltage	YES / NO	NO	RDRE1.VDCUVTrg

Analog Channel Mask			
Setting	**Step**	**Default**	**IEC 61850**
VCTRL	YES / NO	YES	RDRE1.AnChgMsk1
ILOC	YES / NO	YES	RDRE1.AnChgMsk2
IPAR	YES / NO	YES	RDRE1.AnChgMsk3

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

User Defined Values (Up to 16 values)					
ACT TIME	CMAXLOC	SMAX	HARM2 VCTRL	ANG ILOC	FREQ PLL
ACTGRP	CMAXPAR	SMIN	HARM3 VCTRL	ANG IPAR	MREF A
FAULTT	PMIN	VCTRLMAX	HARM4 VCTRL	ARM2_ILOC	ICIRC12
IM IC S	QMAX	VCTRLMIN	HARM5 VCTRL	ARM5_ILOC	ICIRC13
ISH_PI	QMIN	P	HARM6 VCTRL	ILOC	ICIRC14
ISH_PR		ALARMS	HARM7 VCTRL	IPAR	ICIRC15
N.A.ENGY		COLDSTARTS	HARM8 VCTRL		ICIRC
N.R.ENGY		NTRAPS	HARM9 VCTRL		
P.Active Energy		WARMSTARTS	ANG VCTRL		
P.React. Energy		HARM10 VCTRL	VCTRL		
FREQ					
ROC FREQ					

Digital Channel Selection (maximum 160)
Selectable from all configurable Digital Inputs and Digital Signals

5.1.10 Digital Inputs of the Oscillographic Recording

Table 5.1-1: Digital Inputs of the Oscillographic Recording

Name	Group	IEC 61850	Description	Vis.	Function
TRIG_EXT_OSC	Logic Inputs to Protection	RDRE1.RcdTrg	Oscillography External Trigger	I	Input intended for external triggering.
DEL_OSC	Reposition Commands	RDRE1.MemClr	Delete Oscillography Command	I	The activation of this input deletes all the oscillographs stored.
ENBL_OSC	Enabling Commands	RDRE1.Mod	Oscillography Enable Input		Activation of this input puts the element into service. The default value of this logic input signal is a “1.”

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.1.11 Auxiliary Outputs and Events of the Oscillographic Recording

Table 5.1-2: Auxiliary Outputs and Events of the Oscillographic Recording					
Name	**Group**	**IEC 61850**	**Description**	**Vis.**	**Function**
PU_OSC	Others	RDRE1.RcdStr	Oscillography Triggered	I	Indicates that a oscillographic recording is on process.
OSC_ENBLD	Enabled Units Protection Outputs	RDRE1.Mod	Oscillography Enable	I	Indication of enabled or disabled status of the element.

Note: The Visualization column (Vis.) indicates whether the signal is shown as indication in the relay status (I) through the communications program and in the Fault Report (F).

5.1.12 IEC 61850 Logical Node

CLASS IRLRDRE		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Controls		
MemClr	SPC	Clear memory
Status Information		
RcdMade	SPS	Recording made
FltNum	INS	Fault Number
RcdStr	SPS	Recording started
Settings		
PreTmms	ING	Pre-trigger time
PstTmms	ING	Post-trigger time
ReTrgMod	ING	Retrigger mode
ExclTmms	ING	Exclusion time
Extended Data		
RcdTrg	EXT_SPC	External trigger
PHTOVTrg	EXT_SPG	Trigger mask
PTUFTrg	EXT_SPG	Trigger mask
ExTrg	EXT_SPG	Trigger mask
PPDSTrg	EXT_SPG	Trigger mask
VDCOVTrg	EXT_SPG	Trigger mask
VDCUVTrg	EXT_SPG	Trigger mask

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.2 Event Record

5.2.1 Introduction 5.2-2
5.2.2 Protection Event Record 5.2-2
5.2.2.a Operation Principles 5.2-2
5.2.2.b Organization of the Event Record 5.2-3
5.2.2.c Event Mask 5.2-4
5.2.2.d Consulting the Record 5.2-4
5.2.2.e Event Record Settings (Only via Communications) 5.2-4
5.2.2.f SYSLOGSOE Event Record 5.2-5
5.2.3 IEC 61850 Based SYSLOGSOE Event Record 5.2-8
5.2.3.a SYSLOG Event Format 5.2-11
5.2.3.b SYSLOGSOE File Format 5.2-12

5.2.1 Introduction

Depending on the model there are up to two different event record systems in the equipment, one based on internal resources and one based on resources from IEC 61850 data model (SYSLOGSOE event recorder). The first one is described as follows while the second one is described in Section 5.2.3.

5.2.2 Protection Event Record

5.2.2.a Operation Principles

The capacity of the IED is 2000 records in non-volatile memory where each record stores all events that have been generated at the same time up to a maximum of 16 activation or deactivation events per record. The signals that generate the events are user-selectable and are recorded with a resolution of 1 ms together with a maximum of 12 values also selectable from all the available metering values measured or calculated by the IED (*User Defined Values*, including VDC in models with Power Supply Voltage Monitoring).

Each of the functions that the system uses records an event in the Event Record when any of the situations listed in the tables nested in the description of each function occur. Moreover, the events listed in Table 5.2-1 -the IED's general services- are also recorded. The tables mentioned above only list the events available with the default configuration. The list of signals can be expanded with those that the user configures in the programmable logic (any signal existing in the programmable logic can be configured to generate an event with the description that the user defines).

Table 5.2-1: Event Record

Name	Description
Equipment Cold Start Up	It activates each time the relay is power-supplied.
Equipment Warm Start Up	It activates after a relay reset (configuration loading, manual reset…) but with the relay power supply on.
Digital Inputs Power Failure	It activates when no voltage is present at the digital input selected for the ED supervision.
Summer Time	It activates when the relay is in summer time mode.
Local Control	Digital signal indicating relay local control enable. See paragraph 5.16.3, relative to the commands.
Panel-controlled	Digital signal indicating relay control from control panel or HMI enable. See paragraph 5.16.3, relative to the commands.
Remote	Digital signal indicating operations enabled on the equipment from remote control. See paragraph 5.16.3, relative to the commands.
Maintenance Control	Digital signal indicating operations enabled on the equipment from maintenance. See paragraph 5.16.3, relative to the commands.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 5.2-1: Event Record	
Name	**Description**
System Non Critical Error	They write down that a technical issue in the relay has occurred.
System Critical Error	
System Event	It indicates that a relay SW reset has taken place.
Change of Settings Initialization	It is shown when a setting is changed.
HMI Access	It activates every time the HMI is accessed from the relay home screen and deactivates when returning to the home screen.
SNTP Sync	The relay is receiving SNTP synchronization.
Clock Synchronization	The relay is synchronized.
Communication Failure Local Port	They activate when no communications activity through the ports is present for a time set for each of them.
Communication Failure Remote Port 1	
LAN1 / Communication Failure PROCOME Protocol	
LAN1 / Communication Failure Protocol 1	
LAN1 / Communication Failure Protocol 2	
LAN1 / Communication Failure Protocol 3	
LAN1 / Communication Failure Protocol 4	

All the configured events as well as the pre-existing ones in the default configuration can be masked.

The text indicated in the events tables is expanded with the message **Activation of...** when the event is generated by activation of any of the signals or **Deactivation of...** when the event is generated by deactivation of the signal.

5.2.2.b Organization of the Event Record

The Event Record reaches the last 2000 events generated, in a circular pile form, so that event writing above this capacity will result in erasing the events written at the beginning of the pile. The following information is stored in each event register:

- Values of the 12 magnitudes selected at the time the event is generated.
- Event date and time.

Event recorder management is optimized so that simultaneous operations generated by the same event occupy a single position in the event memory. For example, the simultaneous occurrence of the phase A and neutral time overcurrent pickups are recorded in the same memory position. However, if the occurrences are not simultaneous, two separate events are generated. Simultaneous events are those operations occurring within a 1 ms interval, the resolution time of the recorder. Each pile register can store a maximum of 16 activation or deactivation events per register so that the actual maximum capacity will be 32000 events when 16 different events are generated in every millisecond.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.2.2.c Event Mask

There is the possibility of masking events that are not necessary, or are not useful, when studying the behavior of the equipment. This possibility can only be made via communications.

Important: Events that can be generated in excess should be masked since they could fill the memory and erase more important previous events.

5.2.2.d Consulting the Record

The communications and remote management program, ***ZIV e-NET tool***®, has a completely decoded system for consulting the Event Record.

5.2.2.e Event Record Settings (Only via Communications)

Events Mask
IED events may be masked separately

User Defined Magnitudes (Up to 16 magnitudes)					
ACT TIME	CMAXLOC	SMAX	HARM2 VCTRL	ANG ILOC	FREQ PLL
ACTGRP	CMAXPAR	SMIN	HARM3 VCTRL	ANG IPAR	MREF A
FAULTT	PMIN	VCTRLMAX	HARM4 VCTRL	ARM2_ILOC	ICIRC12
IM IC S	QMAX	VCTRLMIN	HARM5 VCTRL	ARM5_ILOC	ICIRC13
ISH_PI	QMIN	P	HARM6 VCTRL	ILOC	ICIRC14
ISH_PR		ALARMS	HARM7 VCTRL	IPAR	ICIRC15
N.A.ENGY		COLDSTARTS	HARM8 VCTRL		ICIRC
N.R.ENGY		NTRAPS	HARM9 VCTRL		
P.Active Energy		WARMSTARTS	ANG VCTRL		
P.React. Energy		HARM10 VCTRL	VCTRL		
FREQ					
ROC FREQ					

Note: all magnitudes for each event are stored in secondary values; therefore not affected by any primary-to-secondary ratio except for energy magnitudes that are always recorded in primary values.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.2.2.f SYSLOGSOE Event Record

In addition to the protection Event Log, the user can configure the protection events to be stored in a second log called SYSLOGSOE in Flash memory (non-volatile). All events stored in this log are automatically sent through the equipment's **Syslog** protocol (see Syslog Protocol Annex).

The SYSLOGSOE event file (.*soe* extension) will be available in the /SYSLOGSOE directory (at the same level as the COMTRADE, COMFEDE, and SCL directories, and with the same access security level as these, i.e. with the same permissions) so that the user can download it through the FTP or SFTP client-server service.

The configuration of the events to be sent via the Syslog protocol is done by activation of the corresponding settings (event masks) located in **Settings\Communications\Protocols\Syslog\Soe Events\Events Mask** (see ***ZIV e-NET tool***® / ***ZIVercomPlus***®).

It is important to note that for an event to be assigned to the SYSLOGSOE log, it must also be assigned to the Event Log, i.e. the user must enable both the Syslog event mask (**Settings\Communications\Protocols\Syslog\Soe Events\Events Mask**) and the main Event Log mask (***Settings\Records\Events\Events Mask***).

User events generated in the logic through the ***ZIV e-NET tool***® (defined as Procome events) will be automatically available to be configured within both the Event Log (***Settings\Records\Events\Events Mask***) and the SYSLOGSOE log (**Settings\Communications\Protocols\Syslog\Soe Events\Events Mask**).

Once the event masks have been enabled, each event can be configured (with the corresponding setting) with a "***Facility***" and "**Severity**" as defined by the protocol.

The ***Facility*** setting options available are as follows:

- 13 log audit.
- 16 local use 0 (local0).
- 17 local use 1 (local1).
- 18 local use 2 (local2).

Regarding the ***Severity*** setting options, the equipment supports the following:

- 2 Critical: critical conditions.
- 4 Warning: warning conditions.
- 6 Informational: informational messages.
- 7 Debug: debug-level messages.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The default settings for the different groups of settings are described in the following table:

Events / Events Group	***Facility***	***Severity***
Digital Inputs/Output/LEDs/Buttons	18	6
Protection	18	6
Recloser	18	6
Control	18	6
User Events (Programmable Logic)	17	6
Oscillography	18	6
Breaker Supervision	18	6
Coil Circuit Supervision	18	6
Energy Counters Reset & Pick value Reset	18	6
Schedule	18	6
System		
System\Equipment Cold Start Up	16	4
System\Equipment Warm Start Up	16	4
System\Alarms\System Critical Error	16	2
System\Alarms\System Non Critical Error	16	4
System\Alarms\System Event	16	4
System\Date and Time	16	6
System\Control State	18	6
System\Settings	18	6
System\HMI	18	6
System\Synchronization	16	6
Communications	18	6

- **SYSLOG Event Format**

The format (see below) is described in detail in the Syslog Protocol Annex.

```
HEADER SP STRUCTURED-DATA [SP MSG]
```

Example of SYSLOG events:

```
<110>1 2020-04-29T12:25:35.231Z 192.168.1.81 IRF1Q11F01 – IEC62351-14:1-nocyb
[62351-14@41912 ID=”7446544” Text=”On Phase A Instantaneous unit 1
Trip|On|Good” SOE=”1234567890”]
[VA63.1VVB34VVC63.41VVG26.87VIA13.81AIB24AIC13.41AIG23.87AIGS4.75ª]
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **SYSLOGSOE File Format**

The SYSLOGSOE file format is as follows:

TIMESTAMP – EventId – PRI (only Severity description) - MSG

Example:

```
2000:01:01_00:03:19.716 - 3705006 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Digital Inputs
Enabled|Off|Good
2000:01:01_00:03:19.716 - 3702630 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Frequency Disabled by
Lack of Voltage|On|Good
2000:01:01_00:03:19.716 - 3702211 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Protection in
Service|On|Good
2000:01:01_00:03:19.716 - 3702207 - warning - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Equipment Warm Start
Up|On|Good
2000:01:01_00:03:19.716 - 3702821 - warning - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - System Event|On|Good
2000:01:01_00:03:19.716 - 3716911 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Communication Failure
PROCOME Protocol|On|Good
2000:01:01_00:03:19.716 - 3716912 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Communication Failure
Protocol 1|On|Good
2000:01:01_00:03:19.716 - 3716913 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Communication Failure
Protocol 2|On|Good
2000:01:01_00:03:19.716 - 3716914 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Communication Failure
Protocol 3|On|Good
2000:01:01_00:03:19.716 - 3716915 - debug - VA0.000V VB0.000V VC0.000V
VG0.000V IA0.000A IB0.000A IC0.000A IG0.000A IGS0.000A - Communication Failure
Protocol 4|On|Good
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.2.3 IEC 61850 Based SYSLOGSOE Event Record

In addition to the protection Event Log, the user can configure events to be stored and/or sent in a second log called SYSLOGSOE in Flash memory (non-volatile). In this event recorder, only data from IEC 61850 data model is considered. Specifically, only changes on states and measurements, and their associated qualities, can produce events. These events can be sent through the Syslog protocol (see Syslog Protocol Annex), stored in a file or both. Two different types of files can be used to store events: Txt and XML.

The SYSLOGSOE event file will be available in the /SoE directory (at the same level as the COMTRADE, COMFEDE, and SCL directories, and with the same access security level as these, i.e. with the same permissions) so that the user can download it using an FTP/SFTP client. It is possible to download this event record file through the ***ZIV e-NET tool***® clicking on Tools/Device Access/Retrieval of Files.

The *Facility* and *Severity* of each event can be configured individually. All *Facility* and *Severity* options defined in the RFC 5424 are available.

Each event can be associated with a group of predefined magnitudes or measurements. These measurements must also be data from IEC 61850 data model. There is a limit of 20 measurement groups and each event can be associated to up to 32 measurements.

It is possible to configure if the quality changes of signals or measurements trigger events or not.

The events must be configured using the software ***ZIV e-NET tool***® though several configuration sheets: General, Syslog, Measure groups and Signals. Because signal sheet could have hundreds of signals, it is possible to copy and paste data to/from an excel spreadsheet considering the structure indicated in the Signals sheet.

It is possible to use predefined wildcards for some of the configurable fields. Wildcards are identified because they are between curly brackets, for example, {IEDName}. Additionally, it is possible to combine wildcards and free text. The following wildcards are possible:

- **{clientCode}**: It is the configuration parameter *clientCode* defined for each signal (e.g., INT502).
- **{phyLabel}**: It is the configuration parameter *phyLabel* defined for each signal (e.g., DI-2).
- **{desc}**: It is the configuration parameter *desc* defined in each signal (e.g., BREAKER 52 CLOSED).
- **{61850Desc}**: It is the description of the signal from the field d of the IEC 61850 data.
- **{acronym}**: It corresponds with the acronym of the value of the signal set in the Acronyms section, for example ON, when the event is triggered. If there is no acronym set, then the value will be empty.
- **{quality}**: It corresponds with the quality (validity of the q attribute) IEC 61850 when the event is triggered, for example GOOD. The admitted values are the one described in the IEC 61850 standard (good, invalid, reserved, questionable).
- **{goCBRef}**: It indicates the Goose Control Block path (complete GOOSE Control Block reference including the IEDName).
- **{FirstLAN}**: It is the IP address of the first enabled LAN port.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **{LAN1}**: It is the IP address of the first LAN port.
- **{LAN2}**: It is the IP address of the second LAN port.
- **{LAN3}**: It is the IP address of the third LAN port.
- **{LAN4}**: It is the IP address of the fourth LAN port.
- **{IEDName}**: It is the IEC 61850 IEDName of the equipment.
- **{intId}**: It is the internal identifier of the IEC 61850 signal.
- **{facility}**: It is the configuration parameter *facility* defined for each event.
- **{severity}**: It is the configuration parameter *severity* defined for each event.
- **{internalDesc}**: It is the internal description of the measure.

The following parameters related with SYSLOGSOE event recorder can be configured through the ***ZIV e-NET tool***®.

Events (SoE) and Fault reports - General				
Parameter	**Type**	**Range**	**Default**	**Description**
Event (SoE) file format	Selectable	Txt XML	Txt	Select the output file format of events recorder.
Quality changes generate events	Selectable	No Yes	Yes	Select whether a quality change generates events.

Events (SoE) and Fault reports - Syslog				
Parameter	**Type**	**Range**	**Default**	**Description**
VERSION (HEADER)	Integer	1-255	1	Value of the VERSION field of the HEADER of Syslog.
HOSTNAME (HEADER)	Text (up to 255 char.)	{FirstLAN} {LAN1} {LAN2} {LAN3} {LAN4} {IEDName} Free text	{FirstLAN}	Value of the HOSTNAME field of the HEADER of Syslog. It can be an IP of the equipment IEDName or a free text.
APP-NAME (HEADER)	Text (up to 48 char.)	{IEDName} Free text	{IEDName}	Value of the APP-NAME field of the HEADER of Syslog. It can be the IEDName of the equipment or a free text.
MSGID (HEADER)	Text (up to 32 char.)	Free text	IEC62351 - 14:1-nocyb	Value of the MSGID field of the HEADER of Syslog.
SD-ID (STRUCTURED-DATA)	Text (up to 32 char.)	Free text	62351 - 14@41912	Value of the SD-ID field of the STRUCTURED-DATA of Syslog.
Send additional information (measures)	Selectable	No Yes	Yes	It indicates if measurement information is included in the Syslog event or not.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Events (SoE) and Fault reports - Measure groups				
Parameter	**Type**	**Range**	**Default**	**Description**
Description (*)	Text			Description text of the measurement group.
IEC 61850 reference (**)	Non editable text			Select the IEC 61850 reference for the required measurement.
Description for Syslog (**)	Text	{61850Desc} Free text	{61850Desc}	Description of the measurement.

(*) For each measurement group.
(**) For each measurement.

Events (SoE) and Fault reports - Signals				
Parameter	**Type**	**Range**	**Default**	**Description**
IEC 61850 reference (*)	Non editable text			Select the IEC 61850 reference for the required data object.
Client code (*)	Text (up to 32 char.)			Customer defined code for the event.
Physical label (*)	Text (up to 32 char.)			Normally used for indicating if the signal is a digital input, digital output or LED.
Description (*)	Text (up to 128 char.)	{61850Desc} Free text	{61850Desc}	Text description of the event.
Facility (*)	Selectable	List according to RFC 5424		Category of the event according to RFC 5424.
Severity (*)	Selectable	List according to RFC 5424		Severity of the event according to RFC 5424.
Send by Syslog (*)	Checkbox	No Yes	Yes	It defines if the event should be sent by the Syslog protocol.
Save to file (*)	Checkbox	No Yes	Yes	It defines if the event should be stored in file.
ID (STRUCTURED-DATA Syslog) (*)	Text (up to 32 char.)	{intId} {clientCode} Free text	{IntId}	Value of the ID field of the STRUCTURED-DATA of Syslog. It can take the internal ID of the signal, the client code or another text.
A**X** (**)	Text (up to 48 char.)	Free text	Boolean: (0 - OFF; 1 - ON) Dbpos: (0 - INTERMEDIATE-STATE; 1 - OFF; 2 - ON; 3 - BAD-STATE) Enum: Value of (“ord” EnumVal IEC 61850) - Text of (“desc” EnumVal IEC 61850)	The description of the event state. For example: ON, OFF, OPEN, CLOSE, etc.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Events (SoE) and Fault reports - Signals				
Parameter	**Type**	**Range**	**Default**	**Description**
E**X** (**)	Checkbox	No Yes	Yes	It defines if the event state generates events or not.
Text for Syslog (*)	Text (up to 128 char.)	{clientCode} {phyLabel} {desc} {acronym} {quality} {goCBRef} {IEDName} {facility} {severity} Free text	{desc}|{acronym}|{quality}	The text field for the event on Syslog protocol. It can be free text, wildcard or wildcards or a combination of wildcards and free text.
Text for file (*)	Text (up to 128 char.)	{clientCode} {phyLabel} {desc} {acronym} {quality} {goCBRef} {IEDName} {facility} {severity} Free text	{desc}|{acronym}|{quality}	The text field for the event on file. It can be free text, wildcard or wildcards or a combination of wildcards and free text.
Associated measures (*)	Selectable	(***)		It is used to indicate which measure groups come along with the event.

(*) For each event.
(**) There can exist several pairs of acronym and event for each event: for example, A0E0, A1E1 for an ON / OFF event.
(***) It depends on the already generated measure groups.

5.2.3.a SYSLOG Event Format

The format (see below) is described in detail in the Syslog Protocol Annex (Syslog format for protection events).

```
HEADER SP STRUCTURED-DATA [SP MSG]
```

Example of SYSLOG events:

```
<110>1 2020-04-29T12:25:35.231Z 192.168.1.81 IRF1Q11F01 - IEC62351-14:1-nocyb
[62351-14@41912 SOE=”1234567890” ID=”e8ca5212bec076cc” Text=”INT502|ED-
2|BREAKER 52 CLOSED|ON|good”] VA=0.000V,0.000° VB=0.000V,0.000°
VC=0.000V,0.000° VG=0.000V,0.000° IA=0.000A,0.000° IB=0.000A,0.000°
IC=0.000A,0.000° IG=0.000A,0.000° IGS=0.000A,0.000°
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.2.3.b SYSLOGSOE File Format

There are two available file formats: Txt and XML. Only one type of file is generated depending on the selected value for the parameter **Event (SoE) File Format** in the ***ZIV e-NET tool***®. This parameter can be found in **Protocols/IEC 61850/Events (SoE) and Fault reports/General**.

Note that the change of the file format from Txt to XML and vice versa will delete the previous event file.

- **Text File Format**

This file will be generated when the parameter **Event (SoE) File Format** takes the Txt value.

The Txt file has a size limit of 2Mbytes. After reaching this file size limit, old event data will be discarded to allow the recording of new events. The SYSLOGSOE Txt file format is as follows:

TIMESTAMP – **EventId** – **PRI** (only **Severity** description) – **MSG**

Example:

```
2022:04:25 14:05:04.268 - e8ca5212bec076cc - informational - INT502|ED-
2|BREAKER 52 CLOSED|ON|good - VA=0.000V,0.000° VB=0.000V,0.000°
VC=0.000V,0.000° VG=0.000V,0.000° IA=0.000A,0.000° IB=0.000A,0.000°
IC=0.000A,0.000° IG=0.000A,0.000° IGS=0.000A,0.000°
```

- **XML File Format**

This file will be generated when the parameter **Event (SoE) File Format** takes the XML value. The SYSLOGSOE XML file format is as follows:

The XML file has a size limit of 2Mbytes. After reaching this file size limit, old event data will be discarded to allow the recording of new events. The structure of the XML events file is the following one:

Node	Description	Children	Attributes
resource	Root node	source	**idRes**: It indicates that it is a fault report. It always takes the value **events**.
source	Unique section which indicates the events producer IED	event	**ip**: IP of the events producer IED. It equals to the field HOSTNAME of the HEADER of Syslog. E.g.: 192.168.1.1 **iedName**: Name of the events producer IED (IEC 61850). E.g.: L45GISDB. **man**: Name of the manufacturer. It takes the fixed value **ZIV**. **sn**: Serial number of the IED which generates the event. E.g.: 154988. **mod**: IED full model name which generates the event. E.g.: IRFA-1A24322A000000XXXX-3332873.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Node	Description	Children	Attributes
event	Section which indicates the data of a single event	evtDatST, evtMeas	**sqNum**: Sequence number of the event. It equals to the field SOE of the STRUCTURED-DATA of Syslog. **date**: Timestamp of the event. It equals to the field TIMESTAMP of the HEADER of Syslog. **q**: Quality of the timestamp. It is an OR of the *ClockFailure* and *ClockNotSynchronized* bits of IEC 61850, this is, a 1 indicates synchronization failure. E.g.: *0*.
evtDatST	Section for the event itself	-	**propId**: Customer identifier. It equals to the configuration parameter *clientCode*. **stdrId**: Internal manufacturer identifier. **val**: Acronym corresponding to the value of the signal when the event is produced. If the acronym does not exist, then the value of the signal is used. **desc**: Description of the signal. It equals to the configuration parameter *Description*. **q**: Quality of the signal (considering only the two most significant bits of IEC 61850 quality) when the event has been triggered. The possible values are **good** (00), **invalid** (01), **reserved** (10) or **questionable** (11).
evtMeas	Section of measurements associated to the event	m	**origin**: It indicates if the measurement values are taken in **primary** or **secondary** winding of the CT. It only can take the fixed value of **primary**. E.g.: *primary*.
m	Measurement associated to the event (1)	-	**propId**: It can take the following values: **voltage**, **voltArg**, **current**, **curArg**, **difCurrent**, **biasCurrent**, **brkCurrent**, **frequency**, **difCheckZoneCurrent** and **biasCheckZoneCurrent**. **stdrId**: Same value as **propId**. **unit**: Unit of the measurement. It can take the values: **A**, **V**, **kV**, **s**, **deg** and **Hz**. **I1**: Phase A current measurement (mag. and angle). **I2**: Phase B current measurement (mag. and angle). **I3**: Phase C current measurement (mag. and angle). **I4**: It is the 4th current channel which could be the sensitive neutral current measurement (mag. and angle). **IN**: Neutral current measurement (mag. and angle). **V1**: Phase A voltage measurement (mag. and angle). **V2**: Phase B voltage measurement (mag. and angle). **V3**: Phase C voltage measurement (mag. and angle). **V4**: VSYN voltage measurement (mag. and angle). **VN**: Neutral voltage measurement (mag. and angle). **F**: Frequency measurement (mag. and angle).

(1) Available measurements within the event depends on the IED type. For IEDs with several windings, I1, I2, I3 and IN will correspond to the ones designed as reference winding. For busbar differential IEDs, I1, I2 and I3 will correspond to the ones designed as angle reference and the difCurrent and the biasCurrent will correspond to the busbar which has tripped. If several busbars have tripped, then they will correspond to the busbar with lowest index of them.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Example:

```
<resource idRes="events">
 <source ip="192.168.1.81" iedName="BUS03" man="ZIV" sn="154988" mod="IRFA-
1A24322A000000XXXX-3332873">
  <event sqNum="1" date="2023-09-06T09:47:24.600Z" q="0">
   <evtDatST propId="FPR200" stdrId="cdf6ef6169a58d3d" val="ON" desc="DISTURBANCE
RECORD START" q="good"/>
   <evtMeas origin="primary">
    <m propId="current" stdrId="current" unit="A" I1="12.25" I2="0.16" I3="0.18" I4="0.00"
IN="12.40"/>
    <m propId="curArg" stdrId="curArg" unit="deg" I1="0.0" I2="0.0" I3="0.0" I4="0.0" IN="0.0"/>
    <m propId="voltage" stdrId="voltage" unit="kV" V1="0.00" V2="0.00" V3="0.00" V4="0.61"
VN="0.00"/>
    <m propId="voltArg" stdrId="voltArg" unit="deg" V1="0.0" V2="0.0" V3="0.0" V4="0.0"
VN="0.0"/>
    <m propId="frequency" stdrId="frequency" unit="Hz" F="0.00"/>
    <m propId="brkCurrent" stdrId="brkCurrent" unit="A" I1="0.00" I2="0.00" I3="0.00"/>
   </evtMeas>
  </event>
 </source>
</resource>
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.3 Metering History Log

5.3.1 Operation Principles 5.3-2
5.3.2 Setting Ranges 5.3-3
5.3.3 IEC61850 Logical Node 5.3-5

5.3.1 Operation Principles

This function records the evolution of the values monitored at the point where the IED is installed. Each second, it samples each of the values programmed for this purpose and calculates their average over the interval defined as ***Sampling Interval***. This time interval is adjustable between 1 and 15 minutes.

The ***Recording Interval*** is an adjustable period of time between 1 minute and 24 hours. The maximum and minimum averages recorded in the whole interval are recorded with their final time stamp. Figure 5.3.1 shows how the Metering History Log works.

-**SI**: Sampling Interval; the figure shows an SI value of one minute.

-**RI**: Recording Interval; the figure shows a RI of 15 minutes.

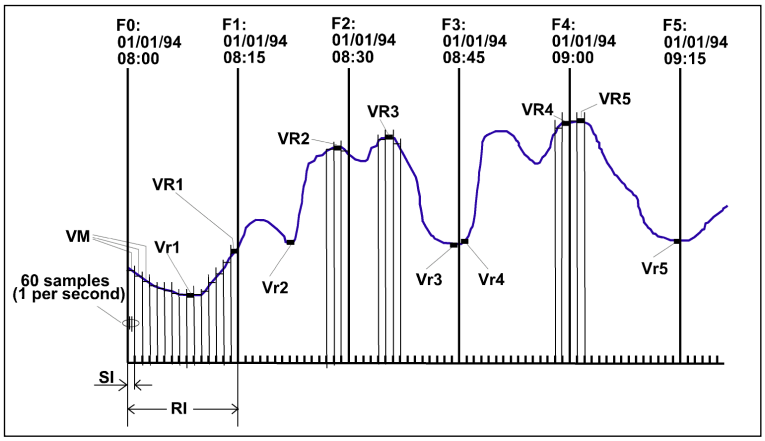


Figure 5.3.1 Explanatory Diagram of the Metering Log.

There are 12 History Log Groups. For each of those 12 values, up to **4 different metering** values can be selected.

Each **SI** window yields two **VM** values that correspond to the maximum and minimum averages of configured group magnitudes. If only one group magnitude is configured, the average value coincides with the maximum and minimum values (see Figure 5.3.1). Maximum and minimum value of all maximum and minimum group **VMs** computed are stored and shown in each **RI** interval. The profile of Figure 5.3.1 yields the following values: VR1 - Vr1; VR2 - Vr2; VR3 - Vr3; VR4 - Vr4 and VR5 - Vr5.

Note: if any of the overcurrent elements pick up during the Sampling Interval, the average of the measurements made while the elements were not picked up is recorded. Otherwise, if the elements remain picked up throughout the SI, the value recorded is: 0A / 0V.

As already indicated, twelve (12) values can be configured among all the direct or calculated metering values (*User Defined* values, including VDC in models with Power Supply Voltage Monitoring) available in the IED (M_i). For each group, up to four different magnitudes can be selected, an average value being obtained for each magnitude along the **Window for Average Calculation**. See figure 5.3.2.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Thus, for every group (up to 12 groups), maximum and minimum measurements of the different magnitudes (up to 4 magnitudes) in each average interval are calculated. Maximum and minimum values of all maximum and minimum measurements obtained along said interval for each group are recorded in each recording interval.

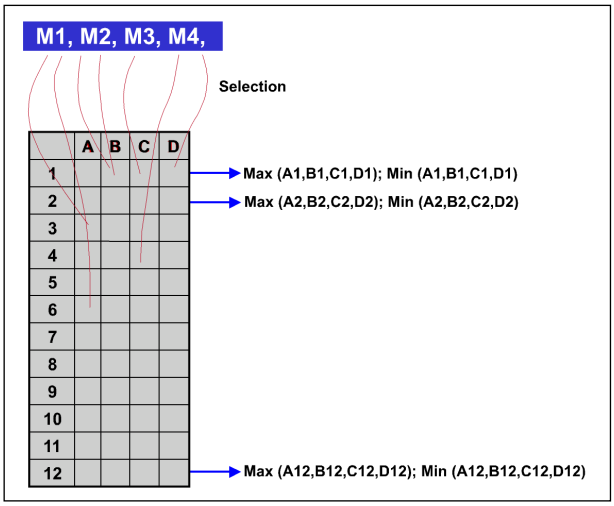


Figure 5.3.2 Metering History Log Logic.

The memory available for the Metering Log is RAM, large enough for 168. The memory can be customized by defining an hour range and ***Week Mask*** (the same hour range for all the days). No values outside the mask will be recorded.

Likewise, the phase currents and voltages as well as the powers are constantly sampled. The sampled values are compared with those already stored. This keeps a maximum/minimum demand metering of the phase currents and voltages and of the active, reactive and apparent powers up to date.

These maximum and minimum values are stored in non-volatile memory, so they are reset by the logic input signal, **Maximum Demand Element Reset**.

All this information is only available via communications through the communications and remote management program ***ZIV e-NET tool***®.

5.3.2 Setting Ranges

Records / History					
Communications Program	**HMI**	**IEC 61850**	**Range**	**Step**	**Default**
Sampling Interval	Sample Interval	HISMSTA1.EvTmms	1 - 15 min		1 min
Recording Interval	Log Rec. Interval	HISMSTA1.RcdLenTmm	from 00:01 to 24:00 (hh:mm)		1 min
Week Mask		HISMSTA1.WeekMaskX X: 1 to 7	Monday to Sunday	YES/NO	YES
Recording Start Time	Hist. Start Time	HISMSTA1.RcdStrTmm	from 00:00 to 24:00 (hh:mm)		0 min
Recording End Time	Hist. End Time	HISMSTA1.RcdStopTmm	from 00:00 to 24:00 (hh:mm)		24:00 min

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Log Groups (Magnitudes)					
There are 12 Log Groups. Up to 4 different magnitudes may be defined within each group for historical record calculations. Said magnitudes are:					
ACT TIME	CMAXLOC	SMAX	HARM2 VCTRL	ANG ILOC	FREQ PLL
ACTGRP	CMAXPAR	SMIN	HARM3 VCTRL	ANG IPAR	MREF A
FAULTT	PMIN	VCTRLMAX	HARM4 VCTRL	ARM2_ILOC	ICIRC12
IM IC S	QMAX	VCTRLMIN	HARM5 VCTRL	ARM5_ILOC	ICIRC13
ISH_PI	QMIN	P	HARM6 VCTRL	ILOC	ICIRC14
ISH_PR		ALARMS	HARM7 VCTRL	IPAR	ICIRC15
N.A.ENGY		COLDSTARTS	HARM8 VCTRL		ICIRC
N.R.ENGY		NTRAPS	HARM9 VCTRL		
P.Active Energy		WARMSTARTS	ANG VCTRL		
P.React. Energy		HARM10 VCTRL	VCTRL		
FREQ					
ROC FREQ					

Note: all the magnitudes shown in historical records are referred to the secondary and are not affected by Transformation Ratios. However, Energy is a special case and is always referred to the primary.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

5.3.3 IEC61850 Logical Node

CLASS IRLHISMSTA		
Data Object Name	**Common Data Class**	**Explanation**
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2, Clause 22
Data Objects		
Settings		
EvTmms	ASG	Window time to calculate samples
RcdLenTmm	ING	Time interval
WeekMask1	SPG	Weekly mask
WeekMask2	SPG	Weekly mask
WeekMask3	SPG	Weekly mask
WeekMask4	SPG	Weekly mask
WeekMask5	SPG	Weekly mask
WeekMask6	SPG	Weekly mask
WeekMask7	SPG	Weekly mask
RcdStrTmm	ING	Start time
RcdStopTmm	ING	Stop time
Gr01Mag1	ING	Magnitude 1 of group 1
Gr01Mag2	ING	Magnitude 2 of group 1
Gr01Mag3	ING	Magnitude 3 of group 1
Gr01Mag4	ING	Magnitude 4 of group 1
Gr02Mag1	ING	Magnitude 1 of group 2
Gr02Mag2	ING	Magnitude 2 of group 2
Gr02Mag3	ING	Magnitude 3 of group 2
Gr02Mag4	ING	Magnitude 4 of group 2
Gr03Mag1	ING	Magnitude 1 of group 3
Gr03Mag2	ING	Magnitude 2 of group 3
Gr03Mag3	ING	Magnitude 3 of group 3
Gr03Mag4	ING	Magnitude 4 of group 3
Gr04Mag1	ING	Magnitude 1 of group 4
Gr04Mag2	ING	Magnitude 2 of group 4
Gr04Mag3	ING	Magnitude 3 of group 4
Gr04Mag4	ING	Magnitude 4 of group 4
Gr05Mag1	ING	Magnitude 1 of group 5
Gr05Mag2	ING	Magnitude 2 of group 5
Gr05Mag3	ING	Magnitude 3 of group 5
Gr05Mag4	ING	Magnitude 4 of group 5
Gr06Mag1	ING	Magnitude 1 of group 6
Gr06Mag2	ING	Magnitude 2 of group 6
Gr06Mag3	ING	Magnitude 3 of group 6
Gr06Mag4	ING	Magnitude 4 of group 6
Gr07Mag1	ING	Magnitude 1 of group 7
Gr07Mag2	ING	Magnitude 2 of group 7
Gr07Mag3	ING	Magnitude 3 of group 7
Gr07Mag4	ING	Magnitude 4 of group 7

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Settings (Cont.)		
Gr08Mag1	ING	Magnitude 1 of group 8
Gr08Mag2	ING	Magnitude 2 of group 8
Gr08Mag3	ING	Magnitude 3 of group 8
Gr08Mag4	ING	Magnitude 4 of group 8
Gr09Mag1	ING	Magnitude 1 of group 9
Gr09Mag2	ING	Magnitude 2 of group 9
Gr09Mag3	ING	Magnitude 3 of group 9
Gr09Mag4	ING	Magnitude 4 of group 9
Gr10Mag1	ING	Magnitude 1 of group 10
Gr10Mag2	ING	Magnitude 2 of group 10
Gr10Mag3	ING	Magnitude 3 of group 10
Gr10Mag4	ING	Magnitude 4 of group 10
Gr11Mag1	ING	Magnitude 1 of group 11
Gr11Mag2	ING	Magnitude 2 of group 11
Gr11Mag3	ING	Magnitude 3 of group 11
Gr11Mag4	ING	Magnitude 4 of group 11
Gr12Mag1	ING	Magnitude 1 of group 12
Gr12Mag2	ING	Magnitude 2 of group 12
Gr12Mag3	ING	Magnitude 3 of group 12
Gr12Mag4	ING	Magnitude 4 of group 12

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

A. PROCOME 3.0 Communications Protocol

A.1 Control Application Layer A-2
A.2 Control Data A-3

A.1 Control Application Layer

- **Application Functions**

☑ **Initialization of the secondary station**
☑ **Clock synchronization**
☑ **Control functions**
  ☑ Control interrogation
  ☑ Refreshing of digital control signals
  ☑ Write outputs
  ☑ Enabling and disabling of inputs
  ☑ *Overflow*
  ☑ Force Single Coil

- **Compatible ASDUs in Secondary-to-Primary Direction**

☑ **<5> Identification**
☑ **<6> Clock synchronization**
☑ **<100> Transmission of metering values and digital control signal changes**
☑ **<101> Transmission of counters**
☑ **<103> Transmission of digital control states**
☑ **<110> Write binary outputs**
☑ **<121> Force Single Coil**

- **Compatible ASDUs in Primary to Secondary Direction**

☑ **<6> Clock synchronization**
☑ **<100> Control data request (Metering values and control changes INF=200)**
☑ **<100> Control data request (Capture of counters INF=202)**
☑ **<100> Control data request (Request for counters INF=201)**
☑ **<103> Request for digital control states**
☑ **<110> Write binary outputs**
☑ **<112> Enable/disable binary inputs**
☑ **<121> Force single coil**

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

A.2 Control Data

- **Control Metering (MEA-s)**

Configurable through the ***ZIV e-NET tool***®: any value measured or calculated by the protection or generated by the programmable logic. It is possible to select between primary and secondary values, taking into account the corresponding transformation ratios.

All the full scale values of the magnitudes are definable, and these magnitudes can be used to create *User Defined Values*. Some typical values are:

- Phase and sequence currents and harmonics: **Rated value I_{PHASE} + 20**% sends 4095 counts.
- Ground and synchronization currents: **Rated value I_{GROUND} + 20%** sends 4095 counts.
- Sensitive ground and directional ungrounded currents: **1.2 A** sends 4095 counts.
- Phase voltages, sequence and harmonics voltages: **(Rated value V / √3) + 20%** sends 4095 counts.
- Line and polarization voltages: **Rated value V + 20%** sends 4095 counts.
- Powers: 3 x 1.4 x Rated value I_{PHASE} x Rated value / √3 sends 4095 counts.
- Power factor: from **–1** to **1** sends from –4095 to 4095 counts.
- Frequency: from **0 Hz** to **1.2 x Frequency$_{RATED}$** (50Hz / 60Hz) sends 4095 counts.
- Thermal value: **240%** sends 4095 counts
- Distance to the fault:
  - Percentage value: **±100%** sends ±4095 counts (range from -100% to 100%).
  - Value in kilometers: with the ***Length*** of the line, it sends ±4095 counts (range from 0 km to the length of the line set in km. It can also send negative values).
  - Value in miles: with the ***Length*** of the line, it sends ±4095 counts (range from 0 km to the length of the line set in miles. It can also send negative values).

With the ***ZIV e-NET tool***® program, it is possible to define the full-scale value to be used to transmit this magnitude in counts, the unit that all the protocols use. There are three definable parameters that determine the range of distance covered:

- **Offset value**: the minimum value of the magnitude for which 0 counts are sent.
- **Limit**: the length of the range of the magnitude on which it is interpolated to calculate the number of counts to send. If the offset value is 0, it coincides with the value of the magnitude for which the defined maximum of counts (4095) is sent.
- **Nominal flag**: this flag allows determining whether the limit set is proportional to the rated value of the magnitude or not. The rated value of the new magnitudes defined by the user in the programmable logic can be configured, while the rest of the existing magnitudes are fixed.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The expression that allows defining this full-scale value is the following:

- When the Nominal flag is enabled,

$$CommunicationsMeasurement = \frac{Measurement - Offset}{Nominal} \times \frac{4095}{Limit}$$

- When the Nominal flag is NOT enabled,

$$CommunicationsMeasurement = (Measurement - Offset) \times \frac{4095}{Limit}$$

- **Counters**

Configurable through the ***ZIV e-NET tool***®: Counters can be created with any signal configured in the programmable logic or from the protection modules. The default counters are those of the real energies (positive and negative) and the reactive energies (capacitive and inductive).

The metering range of energies in primary values is from 100wh/varh to 99999 MWh/Mvarh. The magnitude transmitted via communications is this same primary value; that is, one (1) count represents 100 wh/varh.

- **Force Single Coil (ISE-s)**

Configurable through the ***ZIV e-NET tool***®: A command can be made on any input from the protection modules and on any signal configured in the programmable logic.

- **Write Control Outputs (ISS-s)**

Configurable through the ***ZIV e-NET tool***®: A writing can be made on any input from the protection modules and on any signal configured in the programmable logic.

- **Digital Control Signals (ISC-s)**

Configurable through the ***ZIV e-NET tool***®: Any input or output logic signal from the protection modules or generated by the programmable logic.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

B. DNP V3.00 Device Profiles Document

Dnp3 Basic Profile

(Version 02.44.00 is the last Software Version that supports this Profile)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP V3.00 Basic Profile

DEVICE PROFILE DOCUMENT

This document must be accompanied by: **Implementation Table** and **Point List**.

Vendor Name: **ZIV Aplicaciones y Tecnología S.A.**

Device Name: **RTF**

Highest DNP Level Supported:	Device Function:
For Requests 2 For Responses 2	☐ Master ☒ Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

1) Supports Enable/Disable Unsolicited Responses (FC=20 and 21), for classes 1 and 2.
2) Supports Write operations (FC=2) on Time and Date objects.
3) Supports Delay measurement Fine (FC=23).
4) Supports Warm Start command (FC=14).
5) Supports **Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998)**
6) Supports selection of DNP3 Revision.
7) Supports indication of no **synchronization in time.**
8) Supports simultaneous communications with two different Master devices

Maximum Data Link Frame Size (octets):	Maximum Application Fragment Size (octets):
Transmitted 292 Received 292	Transmitted 2048 (if >2048, must be configurable) Received 249 (must be <= 249)

Maximum Data Link Re-tries:	Maximum Application Layer Re-tries:
☒ None ☐ Fixed at _____ ☐ Configurable, range ___ to ___	☐ None ☒ Configurable, range 0 to 3 (Fixed is not permitted)

Requires Data Link Layer Confirmation:

☒ Never
☐ Always
☐ Sometimes. If 'Sometimes', when?
_____
☐ Configurable. If 'Configurable', how?
_____

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always (not recommended)
- ☒ When reporting Event Data (Slave devices only) For unsolicited, Class 1 and Class 2 responses that contain Event Data. (If there is no Event Data reported into a Class 1 or 2 response, Application Layer Confirmation is not requested)
- ☐ When sending multi-fragment responses (Slave devices only)
- ☐ Sometimes. If 'Sometimes', when?
- ☐ Configurable. If 'Configurable', how?

Timeouts while waiting for:

Data Link Confirm	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Complete Appl. Fragment	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Application Confirm	☐ None	☐ Fixed at ____	☐ Variable	☒ Configurable
Complete Appl. Response	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable

Others

_____

Attach explanation if 'Variable' or 'Configurable' was checked for any timeout

Application Confirm timeout setting (***MMI***): Range 50 ms. 65.535 ms.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Sends/Executes Control Operations:

- Maximum number of CROB (obj. 12, var. 1) objects supported in a single message 1
- Maximum number of Analog Output (obj. 41, any var.) supported in a single message 0

☐ Pattern Control Block and Pattern Mask (obj. 12, var. 2 and 3 respectively) supported.

☐ CROB (obj. 12) and Analog Output (obj. 41) permitted together in a single message.

WRITE Binary Outputs	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
SELECT (3) / OPERATE (4)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE (5)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE - NO ACK (6)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Count > 1	☐ Never	☐ Always	☒ Sometimes	☐ Configurable
Pulse On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Pulse Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
Clear Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable

Attach explanation:

- All points support the same Function Codes: (3) Select, (4) Operate, (5) Direct Operate and (6) Direct Operate - No ACK.
- Maximum Select/Operate Delay Time: 60 seconds.
- Count can be >1 only for PULSE ON and PULSE OFF

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

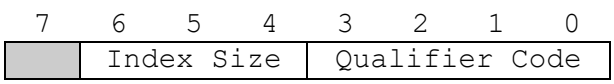
FILL OUT THE FOLLOWING ITEMS FOR SLAVE DEVICES ONLY:	
Reports Binary Input Change Events when no specific variation requested: ☐ Never ☒ Only time-tagged ☐ Only non-time-tagged ☐ Configurable to send both, one or the other (attach explanation)	Reports time-tagged Binary Input Change Events when no specific variation requested: ☐ Never ☒ Binary Input Change With Time ☐ Binary Input Change With Relative Time ☐ Configurable (attach explanation)
Sends Unsolicited Responses: ☐ Never ☒ Configurable (See Note D) ☒ Only certain objects (Class 1 and 2) ☐ Sometimes (attach explanation) ☒ ENABLE/DISABLE UNSOLICITED Function codes supported	Sends Static Data in Unsolicited Responses: ☒ Never ☐ When Device Restarts ☐ When Status Flags Change No other options are permitted.
Default Counter Object/Variation: ☐ No Counters Reported ☐ Configurable (attach explanation) ☒ Default Object 20,21 Default Variation 1 ☐ Point-by-point list attached	Counters Roll Over at: ☐ No Counters Reported ☐ Configurable (attach explanation) ☐ 16 Bits ☐ 32 Bits ☒ Other Value 31 Bits ☐ Point-by-point list attached
Sends Multi-Fragment Responses: ☒ Yes ☐ No	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

QUICK REFERENCE FOR DNP3.0 LEVEL 2 FUNCTION CODES & QUALIFIERS

Function Codes

1	Read
2	Write
3	Select
4	Operate
5	Direct Operate
6	Direct Operate-No ACK
7	Immediate Freeze
8	Immediate Freeze no ACK
13	Cold Start
14	Warm Start
20	Enable Unsol. Messages
21	Disable Unsol. Messages
23	Delay Measurement
129	Response
130	Unsolicited Message



Index Size

0- No Index, Packed
1- 1 byte Index
2- 2 byte Index
3- 4 byte Index
4- 1 byte Object Size
5- 2 byte Object Size
6- 4 byte Object Size

Qualifier Code

0- 8-Bit Start and Stop Indices
1- 16-Bit Start and Stop Indices
2- 32-Bit Start and Stop Indices
3- 8-Bit Absolute address Ident.
4- 16-Bit Absolute address Ident.
5- 32-Bit Absolute address Ident.
6- No Range Field (all)
7- 8-Bit Quantity
8- 16-Bit Quantity
9- 32-Bit Quantity
11-(0xB) Variable array

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

IMPLEMENTATION TABLE

OBJECT			REQUEST (RTF will parse)		RESPONSE (RTF will respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
1	0	Binary Input – All variations	1	6			
1	1	Binary Input			129	1	Assigned to Class 0.
2	0	Binary Input Change – All variations	1	6,7,8			
2	1	Binary Input Change without Time	1	6,7,8	129		B
2	2	Binary Input Change with Time	1	6,7,8	129,130	28	Assigned to Class 1.
2	3	Binary Input Change with Relative Time	1	6,7,8	129		B
10	0	Binary Outputs – All variations	1	6	129		A
12	1	Control Relay Output Block	3,4,5,6	17,28	129	17,28	
20	0	Binary Counter – All variations	1	6	129		~~A~~
20	1	32 Bits Binary Counter			129	1	
21	0	Frozen Counter – All variations	1	6	129		~~A~~
21	1	32 Bits Frozen Counter			129	1	
22	0	Counter Change Event – All variations	1	6,7,8	129		B
30	0	Analog Input – All variations	1	6			
30	2	16-Bit Analog Input			129	1	Assigned to Class 0.
32	0	Analog Change Event – All variations	1	6,7,8			
32	4	16-Bit Analog Change Event with Time			129,130	28	Assigned to Class 2.
40	0	Analog Output Status – All variations	1	6	129		A
41	2	16-Bit Analog Output Block	3,4,5,6	17,28	129		A
50	1	Time and Date	2	7 count=1	129		C
52	2	Time Delay Fine	23		129	1	F,G

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

OBJECT			REQUEST (RTF will parse)		RESPONSE (RTF will respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
60	1	Class 0 Data	1	6	129	1	
60	2	Class 1 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	3	Class 2 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	4	Class 3 Data	1	6,7,8	N/A		B
			20,21	6			
80	1	Internal Indications	2	0 index=7			E
--	--	No Object (Cold Start)	13				F
--	--	No Object (Warm Start)	14				F
--	--	No Object (Delay Measurement)	23				G

NOTES

A: Device implementation level does not support this group and variation of object or, for static objects, it has no objects with this group and variation. **OBJECT UNKNOWN** response (IIN2 bit 1 set).

B: No point range was specified, and device has no objects of this type. **NULL response** (no IIN bits set, but no objects of the specified type returned).

C: Device supports write operations on Time and Date objects. Time Synchronization-Required Internal Indication bit (IIN1-4) will be cleared on the response.

D: The device can be configured to send or not, unsolicited responses depending on a configuration option by means of ***MMI*** (Man-Machine Interface or front-panel user interface). Then, the Master can Enable or Disable Unsolicited messages (for Classes 1 and 2) by means of requests (FC 20 and 21).
If the unsolicited response mode is configured "on", then upon device restart, the device will transmit an initial Null unsolicited response, requesting an application layer confirmation. While waiting for that application layer confirmation, the device will respond to all function requests, including READ requests.

E: Restart Internal Indication bit (IIN1-7) can be cleared explicitly by the master.

F: The outstation, upon receiving a ***Cold or Warm Start*** request, will respond sending a Time Delay Fine object message (which specifies a time interval until the outstation will be ready for further communications), restarting the DNP process, clearing events stored in its local buffers and setting IIN1-7 bit (Device Restart).

G: Device supports Delay Measurement requests (FC = 23). It responds with the Time Delay Fine object (52-2). This object states the number of milliseconds elapsed between Outstation receiving the first bit of the first byte of the request and the time of transmission of the first bit of the first byte of the response.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DEVICE SPECIFIC FEATURES

- Internal Indication IIN1-6 (Device trouble): **Set to indicate a change in the current DNP configuration in the outstation. Cleared in the next response. Used to let the master station know that DNP settings have changed at the outstation. Note that some erroneous configurations could make impossible to communicate this condition to a master station.**

  This document also states the DNP3.0 settings currently available in the device. If the user changes whatever of these settings, it will set the *Device Trouble Internal Indication* bit on the next response sent.
- Event buffers**: device can hold as much as** 50 Binary Input Changes **and** 50 Analog Input Changes**. If these limits are reached the device will set the *Event Buffers Overflow Internal Indication* bit on the next response sent. It will be cleared when the master reads the changes, making room for new ones.**
- Configuration ➔ Operation Enable **menu: the device can enable or disable** permissions **for the operations over al Control Relay Output Block. In case permissions are configured off (disabled) the response to a command (issued as Control Relay Output Block) will have the Status code NOT_AUTHORIZED. In case the equipment is** blocked **the commands allowed are the configured when permitted. While blocked, the relay will accept commands over the configured signal. If the equipment is in** operation inhibited state**, the response to all commands over the configured signal will have the Status code NOT_AUTHORIZED.**
- Configuration ➔ Binary Inputs/Outputs **menu: contains the default configuration (as shipped from factory or after a reset by means of F4 key), but customers can configure Inputs/Outputs to suit their needs, by means of** *ZIVercomPlus*® **software.**

Atención © ***ZIV Aplicaciones y Tecnología, S.A.*** **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

POINT LIST

BINARY INPUT (OBJECT 1) -> Assigned to Class 0. BINARY INPUT CHANGE (OBJECT 2) -> Assigned to Class 1.		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 2048 points**	
1	***Configure by ZIVercomPlus®* 2048 points**	
2	***Configure by ZIVercomPlus®* 2048 points**	
3	***Configure by ZIVercomPlus®* 2048 points**	
4	***Configure by ZIVercomPlus®* 2048 points**	
5	***Configure by ZIVercomPlus®* 2048 points**	
6	***Configure by ZIVercomPlus®* 2048 points**	
7	***Configure by ZIVercomPlus®* 2048 points**	
8	***Configure by ZIVercomPlus®* 2048 points**	
9	***Configure by ZIVercomPlus®* 2048 points**	
10	***Configure by ZIVercomPlus®* 2048 points**	
11	***Configure by ZIVercomPlus®* 2048 points**	
12	***Configure by ZIVercomPlus®* 2048 points**	
13	***Configure by ZIVercomPlus®* 2048 points**	
14	***Configure by ZIVercomPlus®* 2048 points**	
15	***Configure by ZIVercomPlus®* 2048 points**	
16	***Configure by ZIVercomPlus®* 2048 points**	
17	***Configure by ZIVercomPlus®* 2048 points**	
...	***Configure by ZIVercomPlus®* 2048 points**	
253	***Configure by ZIVercomPlus®* 2048 points**	
254	***Configure by ZIVercomPlus®* 2048 points**	
255	***Configure by ZIVercomPlus®* 2048 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
0	***Configure by ZIVercomPlus*® 256 points**	
1	***Configure by ZIVercomPlus*® 256 points**	
2	***Configure by ZIVercomPlus*® 256 points**	
3	***Configure by ZIVercomPlus*® 256 points**	
4	***Configure by ZIVercomPlus*® 256 points**	
5	***Configure by ZIVercomPlus*® 256 points**	
6	***Configure by ZIVercomPlus*® 256 points**	
7	***Configure by ZIVercomPlus*® 256 points**	
8	***Configure by ZIVercomPlus*® 256 points**	
9	***Configure by ZIVercomPlus*® 256 points**	
10	***Configure by ZIVercomPlus*® 256 points**	
11	***Configure by ZIVercomPlus*® 256 points**	
12	***Configure by ZIVercomPlus*® 256 points**	
13	***Configure by ZIVercomPlus*® 256 points**	
14	***Configure by ZIVercomPlus*® 256 points**	
15	***Configure by ZIVercomPlus*® 256 points**	
16	***Configure by ZIVercomPlus*® 256 points**	
17	***Configure by ZIVercomPlus*® 256 points**	
...	***Configure by ZIVercomPlus*® 256 points**	
253	***Configure by ZIVercomPlus*® 256 points**	
254	***Configure by ZIVercomPlus*® 256 points**	
255	***Configure by ZIVercomPlus*® 256 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0. ANALOG INPUT CHANGE (OBJECT 32) -> Assigned to Class 2.		
Index	**Description**	**Deadband**
0	*Configure by ZIVercomPlus*® 512 points	Deadband_1.
1	*Configure by ZIVercomPlus*® 512 points	Deadband_2.
2	*Configure by ZIVercomPlus*® 512 points	Deadband_3.
3	*Configure by ZIVercomPlus*® 512 points	Deadband_4.
4	*Configure by ZIVercomPlus*® 512 points	Deadband_5.
5	*Configure by ZIVercomPlus*® 512 points	Deadband_6.
6	*Configure by ZIVercomPlus*® 512 points	Deadband_7.
7	*Configure by ZIVercomPlus*® 512 points	Deadband_8.
8	*Configure by ZIVercomPlus*® 512 points	Deadband_9.
9	*Configure by ZIVercomPlus*® 512 points	Deadband_10.
10	*Configure by ZIVercomPlus*® 512 points	Deadband_11.
11	*Configure by ZIVercomPlus*® 512 points	Deadband_12.
12	*Configure by ZIVercomPlus*® 512 points	Deadband_13.
13	*Configure by ZIVercomPlus*® 512 points	Deadband_14.
14	*Configure by ZIVercomPlus*® 512 points	Deadband_15.
15	*Configure by ZIVercomPlus*® 512 points	Deadband_16.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Additional assign with *ZIVercomPlus*®:

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0.	
Index	**Description**
16	***Configure by ZIVercomPlus® 512 points***
17	***Configure by ZIVercomPlus® 512 points***
18	***Configure by ZIVercomPlus® 512 points***
19	***Configure by ZIVercomPlus® 512 points***
20	***Configure by ZIVercomPlus® 512 points***
21	***Configure by ZIVercomPlus® 512 points***
22	***Configure by ZIVercomPlus® 512 points***
23	***Configure by ZIVercomPlus® 512 points***
24	***Configure by ZIVercomPlus® 512 points***
25	***Configure by ZIVercomPlus® 512 points***
26	***Configure by ZIVercomPlus® 512 points***
27	***Configure by ZIVercomPlus® 512 points***
....	***Configure by ZIVercomPlus® 512 points***
254	***Configure by ZIVercomPlus® 512 points***
255	***Configure by ZIVercomPlus® 512 points***

The full scale ranges are adjustable and user's magnitudes can be created. It's possible to choose between primary and secondary values, considering CT and PT ratios. Typical ranges in secondary values are:

Description	**Full Scale Range**		
	Engineering units	**Counts**	
Currents (Phases, sequences, harmonics)	0 to 1,2 x In_{PHASE} A	0 to 32767	**Deadband**
Currents (Ground, polarizing)	0 to 1,2 x In_{GROUND} A	0 to 32767	**Deadband**
Currents (Ground sensitive, isolated neutral)	0 to 1,2 A	0 to 32767	**Deadband**
Voltages (Phase to ground, sequences, harmonics)	0 to 1,2 x Vn/√3 V	0 to 32767	**Deadband**
Voltages(Phase to phase, synchronizing)	0 to 1,2 x Vn V	0 to 32767	**Deadband**
Power (Real, reactive, apparent)	0 to 3 x 1,4 x In_{PHASE} x Vn/√3 W	-32768 to 32767	**Deadband**
Power factor	-1 to 1	-32768 to 32767	**Deadband**
Frequency	0 to 1,2 x Rated frequency (50/60 Hz)	0 to 32767	**Deadband**
Thermal value	0 to 200%	0 to 32767	**Deadband**
Distance to Fault - **Percentage of line length:** 100% sends 32767 counts (range from -100% to 100%) - **Distance in kilometers:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in km) - **Distance in miles:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in miles)		-32768 to 32767	**Deadband**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

With ***ZIVercomPlus®*** program it's possible to define the ***Full Scale Range*** that is desired to transmit each magnitude in *counts*, which is the unit used by the protocol. There are three parameters to determine the distance range covered:

- **Offset:** minimum value of each magnitude to transmit 0 counts.
- **Limit:** it's the length of the magnitude range used to calculate the number of counts to transmit. If **offset** is 0, it's the same as the value of the magnitude for which the maximum number of counts defined by the protocol is sent (32767 counts).
- **Nominal Flag:** this *flag* defines if the **limit** is proportional to the rated value of the magnitude or not. The rated value of the new magnitudes defined by the user is a setting, while for the pre-defined magnitudes is a fix value.

Mathematical expression to describe the ***Full Scale Range*** is:

- When **Nominal Flag** is actived,

$$MeasureComm = \frac{Measure - Offset}{RatedValue} \times \frac{32767}{Limit}$$

- When **Nominal Flag** is NOT actived,

$$MeasureComm = (Measure - Offset) \times \frac{32767}{Limit}$$

Deadbands

- Deadbands are used for configuring *Analog Input Change* objects (Object 32).
- A Deadband is defined as a percentage over the **Full Scale Range (FSR)**.
- The Deadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface), between 0.00% and 100.00%, in steps of 0.01%. Default value is 100.00%, meaning that generation of Analog Change Events is **DISABLED** for that input. There is an independent setting for each Analog Input.

Energy counters

The range for the energy counters in primary values is from 100wh/varh to 99999Mwh/Mvarh, and these are the values transmitted by protocol.

Atención © ***ZIV Aplicaciones y Tecnología, S.A.*** **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP3 PROTOCOL SETTINGS

DNP3 Protocol Settings						
DNP Protocol Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Relay Number	Integer	0	65519	1	1	
T Confirm Timeout	Integer	1000	65535	1000	1	msec.
Max Retries	Integer	0	65535	0	1	
Enable Unsolicited.	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Enable Unsol. after Restart	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Unsolic. Master No.	Integer	0	65519	1	1	
Unsol. Grouping Time	Integer	100	65535	1000	1	msec.
Synchronization Interval	Integer	0	120	0	1	min.
DNP 3.0 Rev.	Integer	2003 ST.ZIV	2003 ST.ZIV	2003	2003 ST.ZIV	
DNP Port 1 Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Protocol Select	**Uinteger**	**Procome Dnp3 Modbus**	**Procome Dnp3 Modbus**	**Procome**	**Procome Dnp3 Modbus**	
Baud rate	**Integer**	**300**	**38400**	**38400**	**300 600 1200 2400 4800 9600 19200 38400**	**baud**
Stop Bits	**Integer**	**1**	**2**	**1**	**1**	
Parity	**Integer**	**None Odd Even**	**None Odd Even**	**None**	**None Odd Even**	
Rx Time btw. Char	**Float**	**1**	**60000**	**0.5**	**40**	**msec.**
Comms Fail Ind. Time	**Float**	**0**	**600**	**0.1**	**60**	**s**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advaced settings						
Flow control						
CTS Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Sensitive	Bool	No Yes	No Yes	No	No Yes	
DTR Control	Integer	Inactive Active Rec. Req.	Inactive Active Rec. Req.	Inactive	Inactive Active Rec. Req.	
RTS Control	Integer	Inactive Active Rec. Req. Sen. Req.	Inactive Active Rec. Req. Sen. Req.	Inactive	Inactive Active Rec. Req. Sen. Req.	
Times						
Tx Time Factor	Float	0	100	1	0.5	
Tx Timeout Const	Uinteger	0	60000	0	1	
Message modification						
Number of Zeros	Integer	0	255	0	1	
collision						
Collision Type	Integer	NO ECHO DCD	NO ECHO DCD	NO	NO ECHO DCD	
Max Retries	Integer	0	3	0	1	
Min Retry Time	Uinteger	0	60000	0	1	msec.
Max Retry Time	Uinteger	0	60000	0	1	msec.

DNP Port 2 Configuration

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step/ Select	Unit
Protocol Select	Uinteger	Procome Dnp3 Modbus	Procome Dnp3 Modbus	Procome	Procome Dnp3 Modbus	
Baud rate	Integer	300	38400	38400	300 600 1200 2400 4800 9600 19200 38400	baud
Stop Bits	Integer	1	2	1	1	
Parity	Integer	None Odd Even	None Odd Even	None	None Odd Even	
Rx Time btw. Char	Float	1	60000	0.5	40	msec.
Comms Fail Ind. Time	Float	0	600	0.1	60	s

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advaced settings						
Operating Mode	**Integer**	**RS-232 RS-485**	**RS-232 RS-485**	**RS-232**	**RS-232 RS-485**	
Times						
Tx Time Factor	**Float**	**0**	**100**	**1**	**0.5**	
Tx Timeout Const	**Uinteger**	**0**	**60000**	**0**	**1**	
Wait N Bytes 485	**Integer**	**0**	**4**	**0**	**1**	
Message modification						
Number of Zeros	**Integer**	**0**	**255**	**0**	**1**	
collision						
Collision Type	**Integer**	**NO ECHO**	**NO ECHO**	**NO**	**NO ECHO**	
Max Retries	**Integer**	**0**	**3**	**0**	**1**	
Min Retry Time	**Uinteger**	**0**	**60000**	**0**	**1**	**msec.**
Max Retry Time	**Uinteger**	**0**	**60000**	**0**	**1**	**msec.**

Analog Inputs (Deadbands)

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step	Unit
Deadband AI#0	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#1	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#2	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#3	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#4	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#5	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#6	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#7	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#8	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#9	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#10	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#11	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#12	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#13	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#14	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#15	Float	0 %	100 %	100 %	0.01 %	

- ✓ **All settings remain unchanged after a power loss.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Protocol Configuration

- **Relay Number (RTU Address):**
  Remote Terminal Unit Address. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*.
- **T Confirm Timeout (N7 Confirm Timeout) :**
  Timeout while waiting for Application Layer Confirmation. It applies to Unsolicited messages and Class 1 and Class 2 responses with event data.
- **Max Retries (N7 Retries) :**
  Number of retries of the Application Layer after timeout while waiting for Confirmation.
- **Enable Unsolicited (Enable Unsolicited Reporting) :**
  Enables or disables Unsolicited reporting.
- **Enable Unsol. after Restart :**
  Enables or disables Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998). It has effect only if Enable Unsolicited after Restart is set.

- **Unsolic. Master No. (MTU Address) :**
  Destination address of the Master device to which the unsolicited responses are to be sent. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*. It is useful only when Unsolicited Reporting is enabled.
- **Unsol. Grouping Time (Unsolicited Delay Reporting) :**
  Delay between an event being generated and the subsequent transmission of the unsolicited message, in order to group several events in one message and to save bandwidth.
- **Synchronization Interval**
  Max interval time between two synchronization. If no synchronizing inside interval, indication IIN1-4 (NEED TIME). This setting has no effect if Synchronization Interval is zero.
- **DNP 3.0 Rev.**
  Certification revision **STANDARD ZIV** or **2003** (DNP3-2003 Intelligent Electronic Device (IED) Certification Procedure Subset Level 2 Version 2.3 29-Sept-03)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Port 1 and Port 2 Configuration

- **Number of Zeros (Advice_Time) :**
  Number of zeros before the message.
- **Max Retries (N1 Retries) :**
  Number of retries of the Physical Layer after collision detection.
- **Min Retry Time (Fixed_delay) :**
  Minimum time to retry of the Physical Layer after collision detection.
- **Max Retry Time :**
  Maximum time to retry of the Physical Layer after collision detection.
- **Collision Type :**

  Port 1:
  NO
  ECHO based on detection of transmitted data (monitoring all data transmitted on the link).

  Port 2:
  NO
  ECHO based on detection of transmitted data (monitoring all data transmitted on the link.
  DCD (Data Carrier Detect) based on detecting out-of-band carrier.

  If the device prepares to transmit and finds the link busy, it waits until is no longer busy, and then waits a backoff_time as follows:
  backoff_time = Min Retry Time + random(Max Retry Time - Max Retry Time)
  and transmit. If the device has a collision in transmission the device tries again,up to a configurable number of retries (Max Retries) if has news collision.

- **Wait N Bytes 485:**

Number of wait bytes between Reception and transmission Use Port 2 Operate Mode RS-485.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Dnp3 Basic Extended Profile

(Version 02.45.00 is the first Software Version that supports this Profile)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP V3.00 Basic Extended Profile

DEVICE PROFILE DOCUMENT

This document must be accompanied by: **Implementation Table** and **Point List**.

Vendor Name: **ZIV Aplicaciones y Tecnología S.A.**

Device Name: **RTF**

Highest DNP Level Supported:	Device Function:
For Requests 2 For Responses 2	☐ Master ☒ Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

1) Supports Enable/Disable Unsolicited Responses (FC=20 and 21), for classes 1 and 2.
2) Supports Write operations (FC=2) on Time and Date objects.
3) Supports Delay measurement Fine (FC=23).
4) Supports Warm Start command (FC=14).
5) Supports **Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998)**
6) Supports selection of DNP3 Revision.
7) Supports indication of no **synchronization in time.**
8) Supports simultaneous communications with two different Master devices
9) Supports respond to Multiple Read Request with multiple object types in the same Application Fragment .

Maximum Data Link Frame Size (octets):	Maximum Application Fragment Size (octets):
Transmitted 292 Received 292	Transmitted 2048 (if >2048, must be configurable) Received 249 (must be <= 249)

Maximum Data Link Re-tries:	Maximum Application Layer Re-tries:
☒ None ☐ Fixed at _____ ☐ Configurable, range ___ to ____	☐ None ☒ Configurable, range 0 to 3 (Fixed is not permitted)

Requires Data Link Layer Confirmation:

☒ Never
☐ Always
☐ Sometimes. If 'Sometimes', when?
_____
☐ Configurable. If 'Configurable', how?
_____

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always (not recommended)
- ☒ When reporting Event Data (Slave devices only) For unsolicited, Class 1 and Class 2 responses that contain Event Data. (If there is no Event Data reported into a Class 1 or 2 response, Application Layer Confirmation is not requested)
- ☐ When sending multi-fragment responses (Slave devices only)
- ☐ Sometimes. If 'Sometimes', when?
- ☐ Configurable. If 'Configurable', how?

Timeouts while waiting for:

Data Link Confirm	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Complete Appl. Fragment	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Application Confirm	☐ None	☐ Fixed at ____	☐ Variable	☒ Configurable
Complete Appl. Response	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable

Others

_____

Attach explanation if 'Variable' or 'Configurable' was checked for any timeout

Application Confirm timeout setting (***MMI***): Range 50 ms. 65.535 ms.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Sends/Executes Control Operations:

- Maximum number of CROB (obj. 12, var. 1) objects supported in a single message 1
- Maximum number of Analog Output (obj. 41, any var.) supported in a single message 0

☐ Pattern Control Block and Pattern Mask (obj. 12, var. 2 and 3 respectively) supported.

☐ CROB (obj. 12) and Analog Output (obj. 41) permitted together in a single message.

WRITE Binary Outputs	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
SELECT (3) / OPERATE (4)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE (5)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE - NO ACK (6)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Count > 1	☐ Never	☐ Always	☒ Sometimes	☐ Configurable
Pulse On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Pulse Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
Clear Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable

Attach explanation:

- All points support the same Function Codes: (3) Select, (4) Operate, (5) Direct Operate and (6) Direct Operate - No ACK.
- Maximum Select/Operate Delay Time: 60 seconds.
- Count can be >1 only for PULSE ON and PULSE OFF

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

<table>
<tr><td colspan="2">FILL OUT THE FOLLOWING ITEMS FOR SLAVE DEVICES ONLY:</td></tr>
<tr><td>Reports Binary Input Change Events when no specific variation requested:

☐ Never
☒ Only time-tagged
☐ Only non-time-tagged
☐ Configurable to send both, one or the other (attach explanation)</td><td>Reports time-tagged Binary Input Change Events when no specific variation requested:

☐ Never
☒ Binary Input Change With Time
☐ Binary Input Change With Relative Time
☐ Configurable (attach explanation)</td></tr>
<tr><td>Sends Unsolicited Responses:

☐ Never
☒ Configurable (See Note D)
☒ Only certain objects (Class 1 and 2)
☐ Sometimes (attach explanation)

☒ ENABLE/DISABLE UNSOLICITED Function codes supported</td><td>Sends Static Data in Unsolicited Responses:

☒ Never
☐ When Device Restarts
☐ When Status Flags Change

No other options are permitted.</td></tr>
<tr><td>Default Counter Object/Variation:

☐ No Counters Reported
☐ Configurable (attach explanation)
☒ Default Object 20,21
Default Variation 1
☐ Point-by-point list attached</td><td>Counters Roll Over at:

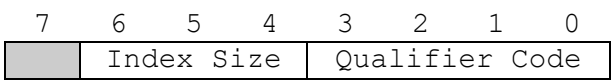
☐ No Counters Reported
☐ Configurable (attach explanation)
☐ 16 Bits
☐ 32 Bits
☒ Other Value 31 Bits
☐ Point-by-point list attached</td></tr>
<tr><td colspan="2">Sends Multi-Fragment Responses: ☒ Yes ☐ No</td></tr>
</table>

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

QUICK REFERENCE FOR DNP3.0 LEVEL 2 FUNCTION CODES & QUALIFIERS

Function Codes

1	Read
2	Write
3	Select
4	Operate
5	Direct Operate
9	Direct Operate-No ACK
10	Immediate Freeze
11	Immediate Freeze no ACK
13	Cold Start
14	Warm Start
20	Enable Unsol. Messages
21	Disable Unsol. Messages
23	Delay Measurement
129	Response
130	Unsolicited Message



Index Size

0- No Index, Packed
1- 1 byte Index
2- 2 byte Index
3- 4 byte Index
4- 1 byte Object Size
5- 2 byte Object Size
6- 4 byte Object Size

Qualifier Code

0- 8-Bit Start and Stop Indices
1- 16-Bit Start and Stop Indices
2- 32-Bit Start and Stop Indices
3- 8-Bit Absolute address Ident.
4- 16-Bit Absolute address Ident.
5- 32-Bit Absolute address Ident.
6- No Range Field (all)
7- 8-Bit Quantity
8- 16-Bit Quantity
9- 32-Bit Quantity
11-(0xB) Variable array

Atención *© ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

IMPLEMENTATION TABLE

OBJECT			REQUEST (RTF will parse)		RESPONSE (RTF will respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
1	0	Binary Input – All variations	1	6			
1	1	Binary Input			129	1	Assigned to Class 0.
2	0	Binary Input Change – All variations	1	6,7,8			
2	1	Binary Input Change without Time	1	6,7,8	129		B
2	2	Binary Input Change with Time	1	6,7,8	129,130	28	Assigned to Class 1.
2	3	Binary Input Change with Relative Time	1	6,7,8	129		B
10	0	Binary Outputs – All variations	1	6	129		A
12	1	Control Relay Output Block	3,4,5,6	17,28	129	17,28	
20	0	Binary Counter – All variations	1	6	129		~~A~~
20	1	32 Bits Binary Counter			129	1	
21	0	Frozen Counter – All variations	1	6	129		~~A~~
21	1	32 Bits Frozen Counter			129	1	
22	0	Counter Change Event – All variations	1	6,7,8	129		B
30	0	Analog Input – All variations	1	6			
30	2	16-Bit Analog Input			129	1	Assigned to Class 0.
32	0	Analog Change Event – All variations	1	6,7,8			
32	4	16-Bit Analog Change Event with Time			129,130	28	Assigned to Class 2.
40	0	Analog Output Status – All variations	1	6	129		A
41	2	16-Bit Analog Output Block	3,4,5,6	17,28	129		A
50	1	Time and Date	2	7 count=1	129		C
52	2	Time Delay Fine	23		129	1	F,G

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

OBJECT			REQUEST (RTF will parse)		RESPONSE (RTF will respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
60	1	Class 0 Data	1	6	129	1	
60	2	Class 1 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	3	Class 2 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	4	Class 3 Data	1	6,7,8	N/A		B
			20,21	6			
80	1	Internal Indications	2	0 index=7			E
--	--	No Object (Cold Start)	13				F
--	--	No Object (Warm Start)	14				F
--	--	No Object (Delay Measurement)	23				G

NOTES

A: Device implementation level does not support this group and variation of object or, for static objects, it has no objects with this group and variation. **OBJECT UNKNOWN** response (IIN2 bit 1 set).

B: No point range was specified, and device has no objects of this type. **NULL response** (no IIN bits set, but no objects of the specified type returned).

C: Device supports write operations on Time and Date objects. Time Synchronization-Required Internal Indication bit (IIN1-4) will be cleared on the response.

D: The device can be configured to send or not, unsolicited responses depending on a configuration option by means of ***MMI*** (Man-Machine Interface or front-panel user interface). Then, the Master can Enable or Disable Unsolicited messages (for Classes 1 and 2) by means of requests (FC 20 and 21).
If the unsolicited response mode is configured "on", then upon device restart, the device will transmit an initial Null unsolicited response, requesting an application layer confirmation. While waiting for that application layer confirmation, the device will respond to all function requests, including READ requests.

E: Restart Internal Indication bit (IIN1-7) can be cleared explicitly by the master.

F: The outstation, upon receiving a ***Cold or Warm Start*** request, will respond sending a Time Delay Fine object message (which specifies a time interval until the outstation will be ready for further communications), restarting the DNP process, clearing events stored in its local buffers and setting IIN1-7 bit (Device Restart).

G: Device supports Delay Measurement requests (FC = 23). It responds with the Time Delay Fine object (52-2). This object states the number of milliseconds elapsed between Outstation receiving the first bit of the first byte of the request and the time of transmission of the first bit of the first byte of the response.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DEVICE SPECIFIC FEATURES

- Internal Indication IIN1-6 (Device trouble): **Set to indicate a change in the current DNP configuration in the outstation. Cleared in the next response. Used to let the master station know that DNP settings have changed at the outstation. Note that some erroneous configurations could make impossible to communicate this condition to a master station.**

  This document also states the DNP3.0 settings currently available in the device. If the user changes whatever of these settings, it will set the *Device Trouble Internal Indication* bit on the next response sent.
- Event buffers**: device can hold as much as** 50 Binary Input Changes **and** 50 Analog Input Changes**. If these limits are reached the device will set the *Event Buffers Overflow Internal Indication* bit on the next response sent. It will be cleared when the master reads the changes, making room for new ones.**
- Configuration ➔ Operation Enable **menu: the device can enable or disable** permissions **for the operations over al Control Relay Output Block. In case permissions are configured off (disabled) the response to a command (issued as Control Relay Output Block) will have the Status code NOT_AUTHORIZED. In case the equipment is** blocked **the commands allowed are the configured when permitted. While blocked, the relay will accept commands over the configured signal. If the equipment is in** operation inhibited state**, the response to all commands over the configured signal will have the Status code NOT_AUTHORIZED.**
- Configuration ➔ Binary Inputs/Outputs **menu: contains the default configuration (as shipped from factory or after a reset by means of F4 key), but customers can configure Inputs/Outputs to suit their needs, by means of** *ZIVercomPlus*® **software.**

Atención © ***ZIV Aplicaciones y Tecnología, S.A.*** **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

POINT LIST

BINARY INPUT (OBJECT 1) -> Assigned to Class 0. BINARY INPUT CHANGE (OBJECT 2) -> Assigned to Class 1.		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 2048 points**	
1	***Configure by ZIVercomPlus®* 2048 points**	
2	***Configure by ZIVercomPlus®* 2048 points**	
3	***Configure by ZIVercomPlus®* 2048 points**	
4	***Configure by ZIVercomPlus®* 2048 points**	
5	***Configure by ZIVercomPlus®* 2048 points**	
6	***Configure by ZIVercomPlus®* 2048 points**	
7	***Configure by ZIVercomPlus®* 2048 points**	
8	***Configure by ZIVercomPlus®* 2048 points**	
9	***Configure by ZIVercomPlus®* 2048 points**	
10	***Configure by ZIVercomPlus®* 2048 points**	
11	***Configure by ZIVercomPlus®* 2048 points**	
12	***Configure by ZIVercomPlus®* 2048 points**	
13	***Configure by ZIVercomPlus®* 2048 points**	
14	***Configure by ZIVercomPlus®* 2048 points**	
15	***Configure by ZIVercomPlus®* 2048 points**	
16	***Configure by ZIVercomPlus®* 2048 points**	
17	***Configure by ZIVercomPlus®* 2048 points**	
...	***Configure by ZIVercomPlus®* 2048 points**	
253	***Configure by ZIVercomPlus®* 2048 points**	
254	***Configure by ZIVercomPlus®* 2048 points**	
255	***Configure by ZIVercomPlus®* 2048 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
0	***Configure by ZIVercomPlus*® 256 points**	
1	***Configure by ZIVercomPlus*® 256 points**	
2	***Configure by ZIVercomPlus*® 256 points**	
3	***Configure by ZIVercomPlus*® 256 points**	
4	***Configure by ZIVercomPlus*® 256 points**	
5	***Configure by ZIVercomPlus*® 256 points**	
6	***Configure by ZIVercomPlus*® 256 points**	
7	***Configure by ZIVercomPlus*® 256 points**	
8	***Configure by ZIVercomPlus*® 256 points**	
9	***Configure by ZIVercomPlus*® 256 points**	
10	***Configure by ZIVercomPlus*® 256 points**	
11	***Configure by ZIVercomPlus*® 256 points**	
12	***Configure by ZIVercomPlus*® 256 points**	
13	***Configure by ZIVercomPlus*® 256 points**	
14	***Configure by ZIVercomPlus*® 256 points**	
15	***Configure by ZIVercomPlus*® 256 points**	
16	***Configure by ZIVercomPlus*® 256 points**	
17	***Configure by ZIVercomPlus*® 256 points**	
...	***Configure by ZIVercomPlus*® 256 points**	
253	***Configure by ZIVercomPlus*® 256 points**	
254	***Configure by ZIVercomPlus*® 256 points**	
255	***Configure by ZIVercomPlus*® 256 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0. ANALOG INPUT CHANGE (OBJECT 32) -> Assigned to Class 2.		
Index	**Description**	**Deadband**
0	*Configure by ZIVercomPlus*® 512 points	Deadband_1.
1	*Configure by ZIVercomPlus*® 512 points	Deadband_2.
2	*Configure by ZIVercomPlus*® 512 points	Deadband_3.
3	*Configure by ZIVercomPlus*® 512 points	Deadband_4.
4	*Configure by ZIVercomPlus*® 512 points	Deadband_5.
5	*Configure by ZIVercomPlus*® 512 points	Deadband_6.
6	*Configure by ZIVercomPlus*® 512 points	Deadband_7.
7	*Configure by ZIVercomPlus*® 512 points	Deadband_8.
8	*Configure by ZIVercomPlus*® 512 points	Deadband_9.
9	*Configure by ZIVercomPlus*® 512 points	Deadband_10.
10	*Configure by ZIVercomPlus*® 512 points	Deadband_11.
11	*Configure by ZIVercomPlus*® 512 points	Deadband_12.
12	*Configure by ZIVercomPlus*® 512 points	Deadband_13.
13	*Configure by ZIVercomPlus*® 512 points	Deadband_14.
14	*Configure by ZIVercomPlus*® 512 points	Deadband_15.
15	*Configure by ZIVercomPlus*® 512 points	Deadband_16.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Additional assign with *ZIVercomPlus*®:

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0.	
Index	**Description**
16	***Configure by ZIVercomPlus® 512 points***
17	***Configure by ZIVercomPlus® 512 points***
18	***Configure by ZIVercomPlus® 512 points***
19	***Configure by ZIVercomPlus® 512 points***
20	***Configure by ZIVercomPlus® 512 points***
21	***Configure by ZIVercomPlus® 512 points***
22	***Configure by ZIVercomPlus® 512 points***
23	***Configure by ZIVercomPlus® 512 points***
24	***Configure by ZIVercomPlus® 512 points***
25	***Configure by ZIVercomPlus® 512 points***
26	***Configure by ZIVercomPlus® 512 points***
27	***Configure by ZIVercomPlus® 512 points***
....	***Configure by ZIVercomPlus® 512 points***
254	***Configure by ZIVercomPlus® 512 points***
255	***Configure by ZIVercomPlus® 512 points***

The full scale ranges are adjustable and user's magnitudes can be created. It's possible to choose between primary and secondary values, considering CT and PT ratios. Typical ranges in secondary values are:

Description	**Full Scale Range**		
	Engineering units	**Counts**	
Currents (Phases, sequences, harmonics)	0 to 1,2 x In_{PHASE} A	0 to 32767	**Deadband**
Currents (Ground, polarizing)	0 to 1,2 x In_{GROUND} A	0 to 32767	**Deadband**
Currents (Ground sensitive, isolated neutral)	0 to 1,2 A	0 to 32767	**Deadband**
Voltages (Phase to ground, sequences, harmonics)	0 to 1,2 x Vn/√3 V	0 to 32767	**Deadband**
Voltages(Phase to phase, synchronizing)	0 to 1,2 x Vn V	0 to 32767	**Deadband**
Power (Real, reactive, apparent)	0 to 3 x 1,4 x In_{PHASE} x Vn/√3 W	-32768 to 32767	**Deadband**
Power factor	-1 to 1	-32768 to 32767	**Deadband**
Frequency	0 to 1,2 x Rated frequency (50/60 Hz)	0 to 32767	**Deadband**
Thermal value	0 to 200%	0 to 32767	**Deadband**
Distance to Fault - **Percentage of line length:** 100% sends 32767 counts (range from -100% to 100%) - **Distance in kilometers:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in km) - **Distance in miles:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in miles)		-32768 to 32767	**Deadband**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

With ***ZIVercomPlus®*** program it's possible to define the ***Full Scale Range*** that is desired to transmit each magnitude in *counts*, which is the unit used by the protocol. There are three parameters to determine the distance range covered:

- **Offset:** minimum value of each magnitude to transmit 0 counts.
- **Limit:** it's the length of the magnitude range used to calculate the number of counts to transmit. If **offset** is 0, it's the same as the value of the magnitude for which the maximum number of counts defined by the protocol is sent (32767 counts).
- **Nominal Flag:** this *flag* defines if the **limit** is proportional to the rated value of the magnitude or not. The rated value of the new magnitudes defined by the user is a setting, while for the pre-defined magnitudes is a fix value.

Mathematical expression to describe the ***Full Scale Range*** is:

- When **Nominal Flag** is actived,

$$MeasureComm = \frac{Measure - Offset}{RatedValue} \times \frac{32767}{Limit}$$

- When **Nominal Flag** is NOT actived,

$$MeasureComm = (Measure - Offset) \times \frac{32767}{Limit}$$

Deadbands

- Deadbands are used for configuring *Analog Input Change* objects (Object 32).
- A Deadband is defined as a percentage over the **Full Scale Range (FSR)**.
- The Deadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface), between 0.00% and 100.00%, in steps of 0.01%. Default value is 100.00%, meaning that generation of Analog Change Events is **DISABLED** for that input. There is an independent setting for each Analog Input.

Energy counters

The range for the energy counters in primary values is from 100wh/varh to 99999Mwh/Mvarh, and these are the values transmitted by protocol.

Atención © ***ZIV Aplicaciones y Tecnología, S.A.*** **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP3 PROTOCOL SETTINGS

DNP3 Protocol Settings						
DNP Protocol Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Relay Number	Integer	0	65519	1	1	
T Confirm Timeout	Integer	1000	65535	1000	1	msec.
Max Retries	Integer	0	65535	0	1	
Enable Unsolicited.	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Enable Unsol. after Restart	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Unsolic. Master No.	Integer	0	65519	1	1	
Unsol. Grouping Time	Integer	100	65535	1000	1	msec.
Synchronization Interval	Integer	0	120	0	1	min.
DNP 3.0 Rev.	Integer	2003 ST.ZIV	2003 ST.ZIV	2003	2003 ST.ZIV	
DNP Port 1 Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Protocol Select	**Uinteger**	**Procome Dnp3 Modbus**	**Procome Dnp3 Modbus**	**Procome**	**Procome Dnp3 Modbus**	
Baud rate	**Integer**	**300**	**38400**	**38400**	**300 600 1200 2400 4800 9600 19200 38400**	**baud**
Stop Bits	**Integer**	**1**	**2**	**1**	**1**	
Parity	**Integer**	**None Odd Even**	**None Odd Even**	**None**	**None Odd Even**	
Rx Time btw. Char	**Float**	**1**	**60000**	**0.5**	**40**	**msec.**
Comms Fail Ind. Time	**Float**	**0**	**600**	**0.1**	**60**	**s**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advaced settings						
Flow control						
CTS Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Sensitive	Bool	No Yes	No Yes	No	No Yes	
DTR Control	Integer	Inactive Active Rec. Req.	Inactive Active Rec. Req.	Inactive	Inactive Active Rec. Req.	
RTS Control	Integer	Inactive Active Rec. Req. Sen. Req.	Inactive Active Rec. Req. Sen. Req.	Inactive	Inactive Active Rec. Req. Sen. Req.	
Times						
Tx Time Factor	Float	0	100	1	0.5	
Tx Timeout Const	Uinteger	0	60000	0	1	
Message modification						
Number of Zeros	Integer	0	255	0	1	
collision						
Collision Type	Integer	NO ECHO DCD	NO ECHO DCD	NO	NO ECHO DCD	
Max Retries	Integer	0	3	0	1	
Min Retry Time	Uinteger	0	60000	0	1	msec.
Max Retry Time	Uinteger	0	60000	0	1	msec.

DNP Port 2 Configuration

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step/ Select	Unit
Protocol Select	Uinteger	Procome Dnp3 Modbus	Procome Dnp3 Modbus	Procome	Procome Dnp3 Modbus	
Baud rate	Integer	300	38400	38400	300 600 1200 2400 4800 9600 19200 38400	baud
Stop Bits	Integer	1	2	1	1	
Parity	Integer	None Odd Even	None Odd Even	None	None Odd Even	
Rx Time btw. Char	Float	1	60000	0.5	40	msec.
Comms Fail Ind. Time	Float	0	600	0.1	60	s

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advaced settings						
Operating Mode	**Integer**	**RS-232 RS-485**	**RS-232 RS-485**	**RS-232**	**RS-232 RS-485**	
Times						
Tx Time Factor	**Float**	**0**	**100**	**1**	**0.5**	
Tx Timeout Const	**Uinteger**	**0**	**60000**	**0**	**1**	
Wait N Bytes 485	**Integer**	**0**	**4**	**0**	**1**	
Message modification						
Number of Zeros	**Integer**	**0**	**255**	**0**	**1**	
collision						
Collision Type	**Integer**	**NO ECHO**	**NO ECHO**	**NO**	**NO ECHO**	
Max Retries	**Integer**	**0**	**3**	**0**	**1**	
Min Retry Time	**Uinteger**	**0**	**60000**	**0**	**1**	**msec.**
Max Retry Time	**Uinteger**	**0**	**60000**	**0**	**1**	**msec.**

Analog Inputs (Deadbands)

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step	Unit
Deadband AI#0	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#1	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#2	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#3	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#4	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#5	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#6	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#7	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#8	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#9	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#10	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#11	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#12	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#13	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#14	Float	0 %	100 %	100 %	0.01 %	
Deadband AI#15	Float	0 %	100 %	100 %	0.01 %	

- ✓ **All settings remain unchanged after a power loss.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Protocol Configuration

- **Relay Number (RTU Address):**
  Remote Terminal Unit Address. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*.
- **T Confirm Timeout (N7 Confirm Timeout) :**
  Timeout while waiting for Application Layer Confirmation. It applies to Unsolicited messages and Class 1 and Class 2 responses with event data.
- **Max Retries (N7 Retries) :**
  Number of retries of the Application Layer after timeout while waiting for Confirmation.
- **Enable Unsolicited (Enable Unsolicited Reporting) :**
  Enables or disables Unsolicited reporting.
- **Enable Unsol. after Restart :**
  Enables or disables Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998). It has effect only if Enable Unsolicited after Restart is set.

- **Unsolic. Master No. (MTU Address) :**
  Destination address of the Master device to which the unsolicited responses are to be sent. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*. It is useful only when Unsolicited Reporting is enabled.
- **Unsol. Grouping Time (Unsolicited Delay Reporting) :**
  Delay between an event being generated and the subsequent transmission of the unsolicited message, in order to group several events in one message and to save bandwidth.
- **Synchronization Interval**
  Max interval time between two synchronization. If no synchronizing inside interval, indication IIN1-4 (NEED TIME). This setting has no effect if Synchronization Interval is zero.
- **DNP 3.0 Rev.**
  Certification revision **STANDARD ZIV** or **2003** (DNP3-2003 Intelligent Electronic Device (IED) Certification Procedure Subset Level 2 Version 2.3 29-Sept-03)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Port 1 and Port 2 Configuration

- **Number of Zeros (Advice_Time) :**
  Number of zeros before the message.
- **Max Retries (N1 Retries) :**
  Number of retries of the Physical Layer after collision detection.
- **Min Retry Time (Fixed_delay) :**
  Minimum time to retry of the Physical Layer after collision detection.
- **Max Retry Time :**
  Maximum time to retry of the Physical Layer after collision detection.
- **Collision Type :**

  Port 1:

  NO

  ECHO based on detection of transmitted data (monitoring all data transmitted on the link).

  Port 2:

  NO

  ECHO based on detection of transmitted data (monitoring all data transmitted on the link.

  DCD (Data Carrier Detect) based on detecting out-of-band carrier.

  If the device prepares to transmit and finds the link busy, it waits until is no longer busy, and then waits a backoff_time as follows:

  backoff_time = Min Retry Time + random(Max Retry Time - Max Retry Time)

  and transmit. If the device has a collision in transmission the device tries again,up to a configurable number of retries (Max Retries) if has news collision.

- **Wait N Bytes 485:**
  Number of wait bytes between Reception and transmission Use Port 2 Operate Mode RS-485.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Dnp3 Profile II

(Version 02.46.00 is the first Software Version that supports this Profile)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP V3.00 Profile II

DEVICE PROFILE DOCUMENT

This document must be accompanied by: **Implementation Table** and **Point List**.

Vendor Name: **ZIV Aplicaciones y Tecnología S.A.**

Device Name: **RTF**

Highest DNP Level Supported:	Device Function:
For Requests 2 For Responses 2	☐ Master ☒ Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

1) Supports Enable/Disable Unsolicited Responses (FC=20 and 21), for classes 1 and 2.
2) Supports Write operations (FC=2) on Time and Date objects.
3) Supports Delay measurement Fine (FC=23).
4) Supports Warm Start command (FC=14).
5) Supports **Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998)**
6) Supports selection of DNP3 Revision.
7) Supports indication of no **synchronization in time.**
8) Supports simultaneous communications with two different Master devices
9) Supports assign event Class for Binary, Analog and Counter events:
   Class 1 , Class 2, Class 3, None
10) Supports respond to Multiple Read Request with multiple object types in the same Application Fragment .

Maximum Data Link Frame Size (octets):	Maximum Application Fragment Size (octets):
Transmitted 292 Received 292	Transmitted 2048 (if >2048, must be configurable) Received 249 (must be <= 249)

Maximum Data Link Re-tries:	Maximum Application Layer Re-tries:
☒ None ☐ Fixed at _____ ☐ Configurable, range ___ to ____	☐ None ☒ Configurable, range 0 to 3 (Fixed is not permitted)

Requires Data Link Layer Confirmation:

☒ Never
☐ Always
☐ Sometimes. If 'Sometimes', when?
_____
☐ Configurable. If 'Configurable', how?
_____

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always (not recommended)
- ☒ When reporting Event Data (Slave devices only) For unsolicited, Class 1 Class 2 and Class 3 responses that contain Event Data. (If there is no Event Data reported into a Class 1 2 or 3 response, Application Layer Confirmation is not requested)
- ☐ When sending multi-fragment responses (Slave devices only)
- ☐ Sometimes. If 'Sometimes', when?
- ☐ Configurable. If 'Configurable', how?

Timeouts while waiting for:

Data Link Confirm	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Complete Appl. Fragment	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Application Confirm	☐ None	☐ Fixed at ____	☐ Variable	☒ Configurable
Complete Appl. Response	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable

Others _____

Attach explanation if 'Variable' or 'Configurable' was checked for any timeout

Application Confirm timeout setting (***MMI***): Range 50 ms. 65.535 ms.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Sends/Executes Control Operations:

- Maximum number of CROB (obj. 12, var. 1) objects supported in a single message 1
- Maximum number of Analog Output (obj. 41, any var.) supported in a single message 0

☐ Pattern Control Block and Pattern Mask (obj. 12, var. 2 and 3 respectively) supported.

☐ CROB (obj. 12) and Analog Output (obj. 41) permitted together in a single message.

WRITE Binary Outputs	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
SELECT (3) / OPERATE (4)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE (5)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE - NO ACK (6)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Count > 1	☐ Never	☐ Always	☒ Sometimes	☐ Configurable
Pulse On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Pulse Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
Clear Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable

Attach explanation:

- All points support the same Function Codes: (3) Select, (4) Operate, (5) Direct Operate and (6) Direct Operate - No ACK.
- Maximum Select/Operate Delay Time: 60 seconds.
- Count can be >1 only for PULSE ON and PULSE OFF

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

<table>
<tr><td colspan="2">FILL OUT THE FOLLOWING ITEMS FOR SLAVE DEVICES ONLY:</td></tr>
<tr><td>Reports Binary Input Change Events when no specific variation requested:

☐ Never
☒ Only time-tagged
☐ Only non-time-tagged
☐ Configurable to send both, one or the other (attach explanation)</td><td>Reports time-tagged Binary Input Change Events when no specific variation requested:

☐ Never
☒ Binary Input Change With Time
☐ Binary Input Change With Relative Time
☐ Configurable (attach explanation)</td></tr>
<tr><td>Sends Unsolicited Responses:

☐ Never
☒ Configurable (See Note D)
☒ Only certain objects (Class 1 2 and 3)
☐ Sometimes (attach explanation)

☒ ENABLE/DISABLE UNSOLICITED Function codes supported</td><td>Sends Static Data in Unsolicited Responses:

☒ Never
☐ When Device Restarts
☐ When Status Flags Change

No other options are permitted.</td></tr>
<tr><td>Default Counter Object/Variation:

☐ No Counters Reported
☐ Configurable (attach explanation)
☒ Default Object _20,21____
Default Variation _____1_____
☐ Point-by-point list attached</td><td>Counters Roll Over at:

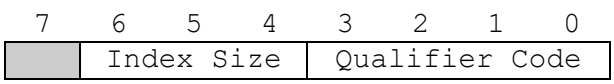
☐ No Counters Reported
☐ Configurable (attach explanation)
☐ 16 Bits
☐ 32 Bits
☒ Other Value ____31 Bits____
☐ Point-by-point list attached</td></tr>
<tr><td colspan="2">Sends Multi-Fragment Responses: ☒ Yes ☐ No</td></tr>
</table>

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

QUICK REFERENCE FOR DNP3.0 LEVEL 2 FUNCTION CODES & QUALIFIERS

Function Codes

1	Read
2	Write
3	Select
4	Operate
5	Direct Operate
6	Direct Operate-No ACK
7	Immediate Freeze
8	Immediate Freeze no ACK
13	Cold Start
14	Warm Start
20	Enable Unsol. Messages
21	Disable Unsol. Messages
23	Delay Measurement
129	Response
130	Unsolicited Message



Index Size

0- No Index, Packed
1- 1 byte Index
2- 2 byte Index
3- 4 byte Index
4- 1 byte Object Size
5- 2 byte Object Size
6- 4 byte Object Size

Qualifier Code

0- 8-Bit Start and Stop Indices
1- 16-Bit Start and Stop Indices
2- 32-Bit Start and Stop Indices
3- 8-Bit Absolute address Ident.
4- 16-Bit Absolute address Ident.
5- 32-Bit Absolute address Ident.
6- No Range Field (all)
7- 8-Bit Quantity
8- 16-Bit Quantity
9- 32-Bit Quantity
11-(0xB) Variable array

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

IMPLEMENTATION TABLE

OBJECT			REQUEST (RTF parse)		RESPONSE (RTF respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
1	0	Binary Input – All variations	1	0,1,6,7,8			Assigned to Class 0.
1	1	Binary Input	1	0,1,6,7,8	129	0,1	
2	0	Binary Input with Status	1	0,1,6,7,8	129	0,1	
2	0	Binary Input Change – All variations	1	6,7,8			
2	2	Binary Input Change with Time	1	6,7,8	129,130	17,,28	Assign to Event Class
12	1	Control Relay Output Block	3,4,5,6	17,28	129	17,28	Echo of request
20	0	Binary Counter – All variations	1	0,1,6,7,8			Assigned to Class 0.
20	1	32 Bits Binary Counter			129	0,1	
21	0	Frozen Counter – All variations	1	0,1,6,7,8			
21	1	32 Bits Frozen Counter			129	0,1	
22	0	Counter Change Event – All variations	1	6,7,8			
22	5	32 Bits Counter Change Event With Time			129,130	17,,28	Assign to Event Class
30	0	Analog Input – All variations	1	0,1,6,7,8			Assigned to Class 0.
30	1	32-Bit Analog Input	1	0,1,6,7,8	129	1	
30	2	16-Bit Analog Input	1	0,1,6,7,8	129	1	
32	0	Analog Change Event – All variations	1	6,7,8			
32	3	32-Bit Analog Change Event with Time	1	6,7,8	129,130	28	Assign to Event Class
32	4	16-Bit Analog Change Event with Time	1	6,7,8	129,130	28	Assign to Event Class
50	1	Time and Date	2	7 count=1	129		C
52	2	Time Delay Fine	23		129	1	F,G

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

OBJECT			REQUEST (RTF parse)		RESPONSE (RTF respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
60	1	Class 0 Data	1	6	129	1	
60	2	Class 1 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	3	Class 2 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	4	Class 3 Data	1	6,7,8	129,130	28	D
			20,21	6			
80	1	Internal Indications	2	0 index=7			E
--	--	No Object (Cold Start)	13				F
--	--	No Object (Warm Start)	14				F
--	--	No Object (Delay Measurement)	23				G

NOTES

C: Device supports write operations on Time and Date objects. Time Synchronization-Required Internal Indication bit (IIN1-4) will be cleared on the response.

D: The device can be configured to send or not, unsolicited responses depending on a configuration option by means of ***MMI*** (Man-Machine Interface or front-panel user interface ***ZIVercomPlus***). Then, the Master can Enable or Disable Unsolicited messages (for Classes 1, 2 and 3) by means of requests (FC 20 and 21).
If the unsolicited response mode is configured "on", then upon device restart, the device will transmit an initial Null unsolicited response, requesting an application layer confirmation. While waiting for that application layer confirmation, the device will respond to all function requests, including READ requests.

E: Restart Internal Indication bit (IIN1-7) can be cleared explicitly by the master.

F: The outstation, upon receiving a ***Cold or Warm Start*** request, will respond sending a Time Delay Fine object message (which specifies a time interval until the outstation will be ready for further communications), restarting the DNP process, clearing events stored in its local buffers and setting IIN1-7 bit (Device Restart).

G: Device supports Delay Measurement requests (FC = 23). It responds with the Time Delay Fine object (52-2). This object states the number of milliseconds elapsed between Outstation receiving the first bit of the first byte of the request and the time of transmission of the first bit of the first byte of the response.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DEVICE SPECIFIC FEATURES

- Internal Indication IIN1-6 (Device trouble): **Set to indicate a change in the current DNP configuration in the outstation. Cleared in the next response. Used to let the master station know that DNP settings have changed at the outstation. Note that some erroneous configurations could make impossible to communicate this condition to a master station.**

  This document also states the DNP3.0 settings currently available in the device. If the user changes whatever of these settings, it will set the *Device Trouble Internal Indication* bit on the next response sent.
- Event buffers**: device can hold as much as 128** Binary Input Changes**,** 64 Analog Input Changes and 64 Counter Input Change. **If these limits are reached the device will set the *Event Buffers Overflow Internal Indication* bit on the next response sent. It will be cleared when the master reads the changes, making room for new ones.**
- Configuration ➔ Operation Enable **menu: the device can enable or disable** permissions **for the operations over al Control Relay Output Block. In case permissions are configured off (disabled) the response to a command (issued as Control Relay Output Block) will have the Status code NOT_AUTHORIZED. In case the equipment is** blocked **the commands allowed are the configured when permitted. While blocked, the relay will accept commands over the configured signal. If the equipment is in** operation inhibited state**, the response to all commands over the configured signal will have the Status code NOT_AUTHORIZED.**
- **Customers can configure Inputs/Outputs to suit their needs, by means of** *ZIVercomPlus*® **software.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

POINT LIST

BINARY INPUT (OBJECT 1) -> Assigned to Class 0. BINARY INPUT CHANGE (OBJECT 2) -> Assign to Class.		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 2048 points**	
1	***Configure by ZIVercomPlus®* 2048 points**	
2	***Configure by ZIVercomPlus®* 2048 points**	
3	***Configure by ZIVercomPlus®* 2048 points**	
4	***Configure by ZIVercomPlus®* 2048 points**	
5	***Configure by ZIVercomPlus®* 2048 points**	
6	***Configure by ZIVercomPlus®* 2048 points**	
7	***Configure by ZIVercomPlus®* 2048 points**	
8	***Configure by ZIVercomPlus®* 2048 points**	
9	***Configure by ZIVercomPlus®* 2048 points**	
10	***Configure by ZIVercomPlus®* 2048 points**	
11	***Configure by ZIVercomPlus®* 2048 points**	
12	***Configure by ZIVercomPlus®* 2048 points**	
13	***Configure by ZIVercomPlus®* 2048 points**	
14	***Configure by ZIVercomPlus®* 2048 points**	
15	***Configure by ZIVercomPlus®* 2048 points**	
16	***Configure by ZIVercomPlus®* 2048 points**	
17	***Configure by ZIVercomPlus®* 2048 points**	
...	***Configure by ZIVercomPlus®* 2048 points**	
253	***Configure by ZIVercomPlus®* 2048 points**	
254	***Configure by ZIVercomPlus®* 2048 points**	
255	***Configure by ZIVercomPlus®* 2048 points**	

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 256 points**	
1	***Configure by ZIVercomPlus®* 256 points**	
2	***Configure by ZIVercomPlus®* 256 points**	
3	***Configure by ZIVercomPlus®* 256 points**	
4	***Configure by ZIVercomPlus®* 256 points**	
5	***Configure by ZIVercomPlus®* 256 points**	
6	***Configure by ZIVercomPlus®* 256 points**	
7	***Configure by ZIVercomPlus®* 256 points**	
8	***Configure by ZIVercomPlus®* 256 points**	
9	***Configure by ZIVercomPlus®* 256 points**	
10	***Configure by ZIVercomPlus®* 256 points**	
11	***Configure by ZIVercomPlus®* 256 points**	
12	***Configure by ZIVercomPlus®* 256 points**	
13	***Configure by ZIVercomPlus®* 256 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
14	***Configure by ZIVercomPlus*® 256 points**	
15	***Configure by ZIVercomPlus*® 256 points**	
16	***Configure by ZIVercomPlus*® 256 points**	
17	***Configure by ZIVercomPlus*® 256 points**	
...	***Configure by ZIVercomPlus*® 256 points**	
253	***Configure by ZIVercomPlus*® 256 points**	
254	***Configure by ZIVercomPlus*® 256 points**	
255	***Configure by ZIVercomPlus*® 256 points**	

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0. ANALOG INPUT CHANGE (OBJECT 32) -> Assign to Class		
Index	**Description**	**Deadband**
0	***Configure by ZIVercomPlus*® 256 points**	**Deadband_1.**
1	***Configure by ZIVercomPlus*® 256 points**	**Deadband_2.**
2	***Configure by ZIVercomPlus*® 256 points**	**Deadband_3.**
3	***Configure by ZIVercomPlus*® 256 points**	**Deadband_4.**
4	***Configure by ZIVercomPlus*® 256 points**	**Deadband_5.**
5	***Configure by ZIVercomPlus*® 256 points**	**Deadband_6.**
6	***Configure by ZIVercomPlus*® 256 points**	**Deadband_7.**
7	***Configure by ZIVercomPlus*® 256 points**	**Deadband_8.**
8	***Configure by ZIVercomPlus*® 256 points**	**Deadband_9.**
9	***Configure by ZIVercomPlus*® 256 points**	**Deadband_10.**
10	***Configure by ZIVercomPlus*® 256 points**	**Deadband_11.**
11	***Configure by ZIVercomPlus*® 256 points**	**Deadband_12.**
12	***Configure by ZIVercomPlus*® 256 points**	**Deadband_13.**
13	***Configure by ZIVercomPlus*® 256 points**	**Deadband_14.**
14	***Configure by ZIVercomPlus*® 256 points**	**Deadband_15.**
15	***Configure by ZIVercomPlus*® 256 points**	**Deadband_16.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Additional assign with ***ZIVercomPlus***®:

Index	Description
16	***Configure by ZIVercomPlus® 256 points***
17	***Configure by ZIVercomPlus® 256 points***
18	***Configure by ZIVercomPlus® 256 points***
19	***Configure by ZIVercomPlus® 256 points***
20	***Configure by ZIVercomPlus® 256 points***
21	***Configure by ZIVercomPlus® 256 points***
22	***Configure by ZIVercomPlus® 256 points***
23	***Configure by ZIVercomPlus® 256 points***
24	***Configure by ZIVercomPlus® 256 points***
25	***Configure by ZIVercomPlus® 256 points***
26	***Configure by ZIVercomPlus® 256 points***
27	***Configure by ZIVercomPlus® 256 points***
....	***Configure by ZIVercomPlus® 256 points***
62	***Configure by ZIVercomPlus® 256 points***
63	***Configure by ZIVercomPlus® 256 points***

The full scale ranges are adjustable and user's magnitudes can be created. It's possible to choose between primary and secondary values, considering CT and PT ratios. Typical ranges in secondary values are:

Description	Full Scale Range		
	Engineering units	Counts	
Currents (Phases, sequences, harmonics)	0 to 1,2 x In_{PHASE} A	0 to 32767	**Deadband**
Currents (Ground, polarizing)	0 to 1,2 x In_{GROUND} A	0 to 32767	**Deadband**
Currents (Ground sensitive, isolated neutral)	0 to 1,2 A	0 to 32767	**Deadband**
Voltages (Phase to ground, sequences, harmonics)	0 to 1,2 x Vn/√3 V	0 to 32767	**Deadband**
Voltages(Phase to phase, synchronizing)	0 to 1,2 x Vn V	0 to 32767	**Deadband**
Power (Real, reactive, apparent)	0 to 3 x 1,4 x In_{PHASE} x Vn/√3 W	-32768 to 32767	**Deadband**
Power factor	-1 to 1	-32768 to 32767	**Deadband**
Frequency	0 to 1,2 x Rated frequency (50/60 Hz)	0 to 32767	**Deadband**
Thermal value	0 to 200%	0 to 32767	**Deadband**
Distance to Fault - **Percentage of line length:** 100% sends 32767 counts (range from -100% to 100%) - **Distance in kilometers:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in km) - **Distance in miles:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in miles)		-32768 to 32767	**Deadband**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Communication Measure in Counts

With ***ZIVercomPlus*** program is possible to define the ***Full Scale Range*** that is desired to transmit each magnitude in *counts*. Parameters necessary to configure the Mathematical expression are:

- **Offset:** A number indicating the compensation of de Magnitude.
- **Limit:** it's the Maximum value of magnitude range.
- **Max Communication:** it's a constant that depend of the Number Bits of Analog Input.
  Max Communication=2(Number Bits Analog Input - 1)**
  For 16-Bit Analog Input (Obj 30 Var. 2) 2**(15) = 32.767 counts
  For 32-Bit Analog Input (Obj 30 Var. 1) 2**(31) = 2.147.483.647 counts
- **Rated value:** Nominal Value of the magnitude.
- **Nominal Flag:** This *flag* defines if the **limit** is proportional to the **rated value** of the magnitude.
- **TR:** Secondary to Primary Transformation Ratio.

Mathematical expression to describe the ***Full Scale Range*** is:

- When **Nominal Flag** is actived,

$$MeasureCom = TR \times \frac{Measure - Offset}{RatedValue} \times \frac{MaxComunication}{Limit}$$

- When **Nominal Flag** is NOT actived,

$$MeasureCom = TR \times (Measure - Offset) \times \frac{MaxComunication}{Limit}$$

Communication Measure in Engineering Units

With ***ZIVercomPlus*** program **also** it's possible to transmit each magnitude in Engineering Units. Parameters necessary to configure the Mathematical expression are:

- **Offset:** A number indicating the compensation of de magnitude.
- **Limit:** it's the Maximum value of magnitude range.
- **Rated value:** Nominal Value of the magnitude.
- **Nominal Flag:** this *flag* defines if the **limit** is proportional to the **rated value** of the magnitude or not. The rated value of the new magnitudes defined by the user is a setting, while for the pre-defined magnitudes is a fix value.
- **TR:** Secondary to Primary Transformation Ratio.
- **Scaling Factor:** Multiply Factor of magnitude.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Mathematical expression to obtain **Measure in Engineering Units** is:

- When **Nominal Flag** is actived,

$$MeasureCom = TR \times \frac{Measure - Offset}{RatedValue} \times ScalingFactor$$

- When **Nominal Flag** is NOT actived,

$$MeasureCom = TR \times (Measure - Offset) \times ScalingFactor$$

DeadBands

- Deadband is an area of a magnitude range or band where no generate magnitude change (the magnitude is dead). Meaning that no generation of Analogical Change Events if difference with value of generation of previous change is not equal or greater that DeadBand calculated. There is an independent setting for each 16 Measures with change.
- A Deadband is calculated as a percentage defined in DeadBand Setting over value of **parameter Limit**.
- The Deadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface *ZIVercomPlus*), between 0.0000% and 100.00%, in steps of 0.0001%. Default value is 100.00%, meaning that generation of Analog Change Events is **DISABLED** for that input. There is an independent setting for each Magnitude with change.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

BINARY COUNTER (OBJECT 20) -> Assigned to Class 0. FROZEN COUNTER (OBJECT 21) 32 BIT COUNTER CHANGE EVENT (OBJECT 22) -> Assign to Class		
Index	**Description**	**Deadband**
0	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_1.**
1	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_2.**
2	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_3.**
3	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_4.**
4	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_5.**
5	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_6**
6	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_7.**
7	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_8.**
8	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_9.**
9	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_10.**
10	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_11.**
11	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_12.**
12	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_13.**
13	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_14.**
14	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_15.**
15	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_16.**
16	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_17.**
17	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_18.**
18	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_19.**
19	***Configure by ZIVercomPlus*® 256 points**	**CounterDeadBand_20.**

CounterDeadBands

- CounterDeadband is an area of a counter magnitude range or band, where no generate counter magnitude change (the communication counter magnitude is dead).Meaning that no generation of Counter Change Events if difference with value of generation of previous change is not equal or greater that CounterDeadBand setting. There is an independent setting for each Counter.

- The CounterDeadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface *ZIVercomPlus*), between 1 and 32767, in steps of 1, default value is 1.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP3 PROTOCOL SETTINGS

DNP3 Protocol Settings

DNP Protocol Configuration

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step/ Select	Unit
Relay Number	Integer	0	65519	1	1	
T Confirm Timeout	Integer	1000	65535	1000	1	msec.
Max Retries	Integer	0	65535	0	1	
Enable Unsolicited.	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Enable Unsol. after Restart	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Unsolic. Master No.	Integer	0	65519	1	1	
Unsol. Grouping Time	Integer	100	65535	1000	1	msec.
Synchronization Interval	Integer	0	120	0	1	min.
DNP 3.0 Rev.	Integer	2003 ST.ZIV	2003 ST.ZIV	2003	2003 ST.ZIV	
Binary Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 1	None Class 1 Class 2 Class 3	
Analog Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 2	None Class 1 Class 2 Class 3	
Counter Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 3	None Class 1 Class 2 Class 3	
Binary Status Change	Boolean	0 (No)	1 (Yes)	1 (Yes)	1	
32 Bits Analog Input	Boolean	0 (No)	1 (Yes)	1 (Yes)	1	

Analog Inputs (Deadbands)

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step	Unit
Deadband AI#0	Float	0 %	100 %	100 %	0.0001 %	
Deadband AI#1	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#2	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#3	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#4	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#5	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#6	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#7	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#8	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#9	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#10	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#11	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#12	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#13	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#14	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#15	Float	0 %	100 %	100 %	0. 0001 %	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Counter Inputs (CounterDeadbands)						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step**	**Unit**
Deadband Cont.I#0	Integer	1	32767	1	1	
Deadband Cont.I#1	Integer	1	32767	1	1	
Deadband Cont.I#2	Integer	1	32767	1	1	
Deadband Cont.I#3	Integer	1	32767	1	1	
Deadband Cont.I#4	Integer	1	32767	1	1	
Deadband Cont.I#5	Integer	1	32767	1	1	
Deadband Cont.I#6	Integer	1	32767	1	1	
Deadband Cont.I#7	Integer	1	32767	1	1	
Deadband Cont.I#8	Integer	1	32767	1	1	
Deadband Cont.I#9	Integer	1	32767	1	1	
Deadband Cont.I#10	Integer	1	32767	1	1	
Deadband Cont.I#11	Integer	1	32767	1	1	
Deadband Cont.I#12	Integer	1	32767	1	1	
Deadband Cont.I#13	Integer	1	32767	1	1	
Deadband Cont.I#14	Integer	1	32767	1	1	
Deadband Cont.I#15	Integer	1	32767	1	1	
Deadband Cont.I#16	Integer	1	32767	1	1	
Deadband Cont.I#17	Integer	1	32767	1	1	
Deadband Cont.I#18	Integer	1	32767	1	1	
Deadband Cont.I#19	Integer	1	32767	1	1	

DNP Port 1 Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Protocol Select	**Uinteger**	**Procome Dnp3 Modbus**	**Procome Dnp3 Modbus**	**Procome**	**Procome Dnp3 Modbus**	
Baud rate	**Integer**	**300**	**38400**	**38400**	**300 600 1200 2400 4800 9600 19200 38400**	**baud**
Stop Bits	**Integer**	**1**	**2**	**1**	**1**	
Parity	**Integer**	**None Odd Even**	**None Odd Even**	**None**	**None Odd Even**	
Rx Time btw. Char	**Float**	**1**	**60000**	**0.5**	**40**	**msec.**
Comms Fail Ind. Time	**Float**	**0**	**600**	**0.1**	**60**	**s**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advanced Settings						
Flow control						
CTS Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Flow	Bool	No Yes	No Yes	No	No Yes	
DSR Sensitive	Bool	No Yes	No Yes	No	No Yes	
DTR Control	Integer	Inactive Active Rec. Req.	Inactive Active Rec. Req.	Inactive	Inactive Active Rec. Req.	
RTS Control	Integer	Inactive Active Rec. Req. Sen. Req.	Inactive Active Rec. Req. Sen. Req.	Inactive	Inactive Active Rec. Req. Sen. Req.	
Times						
Tx Time Factor	Float	0	100	1	0.5	
Tx Timeout Const	Uinteger	0	60000	0	1	
Message modification						
Number of Zeros	Integer	0	255	0	1	
collision						
Collision Type	Integer	NO ECHO DCD	NO ECHO DCD	NO	NO ECHO DCD	
Max Retries	Integer	0	3	0	1	
Min Retry Time	Uinteger	0	60000	0	1	msec.
Max Retry Time	Uinteger	0	60000	0	1	msec.

DNP Port 2 and 3 Configuration

Setting Name	Type	Minimum Value	Maximum Value	Default Value	Step/ Select	Unit
Protocol Select	Uinteger	Procome Dnp3 Modbus	Procome Dnp3 Modbus	Procome	Procome Dnp3 Modbus	
Baud rate	Integer	300	38400	38400	300 600 1200 2400 4800 9600 19200 38400	baud
Stop Bits	Integer	1	2	1	1	
Parity	Integer	None Odd Even	None Odd Even	None	None Odd Even	
Rx Time btw. Char	Float	1	60000	0.5	40	msec.
Comms Fail Ind. Time	Float	0	600	0.1	60	s

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Advanced Settings						
Operating Mode	Integer	RS-232 RS-485	RS-232 RS-485	RS-232	RS-232 RS-485	
Times						
Tx Time Factor	Float	0	100	1	0.5	
Tx Timeout Const	Uinteger	0	60000	0	1	
Wait N Bytes 485	Integer	0	4	0	1	
Message modification						
Number of Zeros	Integer	0	255	0	1	
collision						
Collision Type	Integer	NO ECHO	NO ECHO	NO	NO ECHO	
Max Retries	Integer	0	3	0	1	
Min Retry Time	Uinteger	0	60000	0	1	msec.
Max Retry Time	Uinteger	0	60000	0	1	msec.

✓ **All settings remain unchanged after a power loss.** F4

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Protocol Configuration

- **Relay Number (RTU Address):**
  Remote Terminal Unit Address. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*.
- **T Confirm Timeout (N7 Confirm Timeout) :**
  Timeout while waiting for Application Layer Confirmation. It applies to Unsolicited messages and Class 1 and Class 2 responses with event data.
- **Max Retries (N7 Retries) :**
  Number of retries of the Application Layer after timeout while waiting for Confirmation.
- **Enable Unsolicited (Enable Unsolicited Reporting) :**
  Enables or disables Unsolicited reporting.
- **Enable Unsol. after Restart :**
  Enables or disables Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998). It has effect only if Enable Unsolicited after Restart is set.
- **Unsolic. Master No. (MTU Address) :**
  Destination address of the Master device to which the unsolicited responses are to be sent. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*. It is useful only when Unsolicited Reporting is enabled.
- **Unsol. Grouping Time (Unsolicited Delay Reporting) :**
  Delay between an event being generated and the subsequent transmission of the unsolicited message, in order to group several events in one message and to save bandwidth.
- **Synchronization Interval**
  Max interval time between two synchronization. If no synchronizing inside interval, indication IIN1-4 (NEED TIME). This setting has no effect if Synchronization Interval is zero.
- **DNP 3.0 Rev.**
  Certification revision **STANDARD ZIV** or **2003** (DNP3-2003 Intelligent Electronic Device (IED) Certification Procedure Subset Level 2 Version 2.3 29-Sept-03)
- **Binary Changes CLASS.**
  Selection to send Binary Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Analog Changes CLASS.**
  Selection to send Analog Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Counter Changes CLASS.**
  Selection to send Counter Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Binary Status .**
  Send Binary with status otherwise without status
- **32 Bits Analog Input .**
  Send Analog All Variations and Analog Change Event Binary Changes with 32 bits otherwise with 16 bits

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Port 1 Port 2 and Port 3 Configuration

- **Number of Zeros (Advice_Time) :**
  Number of zeros before the message.
- **Max Retries (N1 Retries) :**
  Number of retries of the Physical Layer after collision detection.
- **Min Retry Time (Fixed_delay) :**
  Minimum time to retry of the Physical Layer after collision detection.
- **Max Retry Time :**
  Maximum time to retry of the Physical Layer after collision detection.
- **Collision Type :**

  Port 1:

  NO

  ECHO based on detection of transmitted data (monitoring all data transmitted on the link).

  Port 2:

  NO

  ECHO based on detection of transmitted data (monitoring all data transmitted on the link.

  DCD (Data Carrier Detect) based on detecting out-of-band carrier.

  If the device prepares to transmit and finds the link busy, it waits until is no longer busy, and then waits a backoff_time as follows:

  backoff_time = Min Retry Time + random(Max Retry Time - Max Retry Time)

  and transmit. If the device has a collision in transmission the device tries again ,up to a configurable number of retries (Max Retries) if has news collision.

- **Wait N Bytes 485:**
  Number of wait bytes between Reception and transmission Use Port 2 Operate Mode RS-485 .

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Dnp3 Profile II Ethernet

(Version 02.60.00 is the first Software Version that supports this Profile)

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP V3.00 Dnp3 Profile II Ethernet

DEVICE PROFILE DOCUMENT
This document must be accompanied by: **Implementation Table** and **Point List**.

Vendor Name: **ZIV Aplicaciones y Tecnología S.A.**	
Device Name: **RTF**	
Highest DNP Level Supported: For Requests 2 For Responses 2	Device Function: ☐ Master ☒ Slave

Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table):

1) Supports Enable/Disable Unsolicited Responses (FC=20 and 21), for classes 1 and 2.
2) Supports Write operations (FC=2) on Time and Date objects.
3) Supports Delay measurement Fine (FC=23).
4) Supports Warm Start command (FC=14).
5) Supports **Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998)**
6) Supports selection of DNP3 Revision.
7) Supports indication of no **synchronization in time.**
8) Supports simultaneous communications with two different Master devices
9) Supports assign event Class for Binary, Analog and Counter events:
   Class 1 , Class 2, Class 3, None
10) Supports respond to Multiple Read Request with multiple object types in the same Application Fragment .

Maximum Data Link Frame Size (octets): Transmitted 292 Received 292	Maximum Application Fragment Size (octets): Transmitted 2048 (if >2048, must be configurable) Received 249 (must be <= 249)
Maximum Data Link Re-tries: ☒ None ☐ Fixed at _____ ☐ Configurable, range ___ to ___	Maximum Application Layer Re-tries: ☐ None ☒ Configurable, range 0 to 3 (Fixed is not permitted)

Requires Data Link Layer Confirmation:

☒ Never
☐ Always
☐ Sometimes. If 'Sometimes', when?
_____
☐ Configurable. If 'Configurable', how?

Atención © ZIV Aplicaciones y Tecnología, S.A. Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Requires Application Layer Confirmation:

- ☐ Never
- ☐ Always (not recommended)
- ☒ When reporting Event Data (Slave devices only) For unsolicited, Class 1 Class 2 and Class 2 responses that contain Event Data. (If there is no Event Data reported into a Class 1 2 or 3 response, Application Layer Confirmation is not requested)
- ☐ When sending multi-fragment responses (Slave devices only)
- ☐ Sometimes. If 'Sometimes', when?
- ☐ Configurable. If 'Configurable', how?

Timeouts while waiting for:

Data Link Confirm	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Complete Appl. Fragment	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable
Application Confirm	☐ None	☐ Fixed at ____	☐ Variable	☒ Configurable
Complete Appl. Response	☒ None	☐ Fixed at ____	☐ Variable	☐ Configurable

Others _____

Attach explanation if 'Variable' or 'Configurable' was checked for any timeout

Application Confirm timeout setting (***MMI***): Range 50 ms. 65.535 ms.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Sends/Executes Control Operations:

- Maximum number of CROB (obj. 12, var. 1) objects supported in a single message 1
- Maximum number of Analog Output (obj. 41, any var.) supported in a single message 0

☐ Pattern Control Block and Pattern Mask (obj. 12, var. 2 and 3 respectively) supported.

☐ CROB (obj. 12) and Analog Output (obj. 41) permitted together in a single message.

WRITE Binary Outputs	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
SELECT (3) / OPERATE (4)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE (5)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
DIRECT OPERATE - NO ACK (6)	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Count > 1	☐ Never	☐ Always	☒ Sometimes	☐ Configurable
Pulse On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Pulse Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch On	☐ Never	☒ Always	☐ Sometimes	☐ Configurable
Latch Off	☐ Never	☒ Always	☐ Sometimes	☐ Configurable

Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable
Clear Queue	☒ Never	☐ Always	☐ Sometimes	☐ Configurable

Attach explanation:

- All points support the same Function Codes: (3) Select, (4) Operate, (5) Direct Operate and (6) Direct Operate - No ACK.
- Maximum Select/Operate Delay Time: 60 seconds.
- Count can be >1 only for PULSE ON and PULSE OFF

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

FILL OUT THE FOLLOWING ITEMS FOR SLAVE DEVICES ONLY:	
Reports Binary Input Change Events when no specific variation requested: ☐ Never ☒ Only time-tagged ☐ Only non-time-tagged ☐ Configurable to send both, one or the other (attach explanation)	Reports time-tagged Binary Input Change Events when no specific variation requested: ☐ Never ☒ Binary Input Change With Time ☐ Binary Input Change With Relative Time ☐ Configurable (attach explanation)
Sends Unsolicited Responses: ☐ Never ☒ Configurable (See Note D) ☒ Only certain objects (Class 1 2 and 3) ☐ Sometimes (attach explanation) ☒ ENABLE/DISABLE UNSOLICITED Function codes supported	Sends Static Data in Unsolicited Responses: ☒ Never ☐ When Device Restarts ☐ When Status Flags Change No other options are permitted.
Default Counter Object/Variation: ☐ No Counters Reported ☐ Configurable (attach explanation) ☒ Default Object 20,21 Default Variation 1 ☐ Point-by-point list attached	Counters Roll Over at: ☐ No Counters Reported ☐ Configurable (attach explanation) ☐ 16 Bits ☐ 32 Bits ☒ Other Value 31 Bits ☐ Point-by-point list attached
Sends Multi-Fragment Responses: ☒ Yes ☐ No	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

QUICK REFERENCE FOR DNP3.0 LEVEL 2 FUNCTION CODES & QUALIFIERS

Function Codes

1	Read
2	Write
3	Select
4	Operate
5	Direct Operate
9	Direct Operate-No ACK
10	Immediate Freeze
11	Immediate Freeze no ACK
13	Cold Start
14	Warm Start
20	Enable Unsol. Messages
21	Disable Unsol. Messages
23	Delay Measurement
24	Record Current Time
129	Response
130	Unsolicited Message

7	6	5	4	3	2	1	0
	Index Size			Qualifier Code			

Index Size

0- No Index, Packed
1- 1 byte Index
2- 2 byte Index
3- 4 byte Index
4- 1 byte Object Size
5- 2 byte Object Size
6- 4 byte Object Size

Qualifier Code

0- 8-Bit Start and Stop Indices
1- 16-Bit Start and Stop Indices
2- 32-Bit Start and Stop Indices
3- 8-Bit Absolute address Ident.
4- 16-Bit Absolute address Ident.
5- 32-Bit Absolute address Ident.
6- No Range Field (all)
7- 8-Bit Quantity
8- 16-Bit Quantity
9- 32-Bit Quantity
11-(0xB) Variable array

Atención *© ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

IMPLEMENTATION TABLE

OBJECT			REQUEST (RTF parse)		RESPONSE (RTF respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
1	0	Binary Input – All variations	1	0,1,6,7,8			Assigned to Class 0.
1	1	Binary Input	1	0,1,6,7,8	129	0,1	
2	0	Binary Input with Status	1	0,1,6,7,8	129	0,1	
2	0	Binary Input Change – All variations	1	6,7,8			
2	2	Binary Input Change with Time	1	6,7,8	129,130	17,,28	Assign to Event Class
12	1	Control Relay Output Block	3,4,5,6	17,28	129	17,28	Echo of request
20	0	Binary Counter – All variations	1	0,1,6,7,8			Assigned to Class 0.
20	1	32 Bits Binary Counter			129	0,1	
21	0	Frozen Counter – All variations	1	0,1,6,7,8			
21	1	32 Bits Frozen Counter			129	0,1	
22	0	Counter Change Event – All variations	1	6,7,8			
22	5	32 Bits Counter Change Event With Time			129,130	17,,28	Assign to Event Class
30	0	Analog Input – All variations	1	0,1,6,7,8			Assigned to Class 0.
30	1	32-Bit Analog Input	1	0,1,6,7,8	129	1	
30	2	16-Bit Analog Input	1	0,1,6,7,8	129	1	
32	0	Analog Change Event – All variations	1	6,7,8			
32	3	32-Bit Analog Change Event with Time	1	6,7,8	129,130	28	Assign to Event Class
32	4	16-Bit Analog Change Event with Time	1	6,7,8	129,130	28	Assign to Event Class
50	1	Time and Date	2	7 count=1	129		C
50	3	Time and Date at Last Recorded Time	2	7 count=1	129		C
52	2	Time Delay Fine	23		129	1	F,G

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

OBJECT			REQUEST (RTF parse)		RESPONSE (RTF respond)		
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes (dec)	Qual Codes (hex)	Notes
60	1	Class 0 Data	1	6	129	1	
60	2	Class 1 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	3	Class 2 Data	1	6,7,8	129,130	28	D
			20,21	6			
60	4	Class 3 Data	1	6,7,8	129,130	28	D
			20,21	6			
80	1	Internal Indications	2	0 index=7			E
--	--	No Object (Cold Start)	13				F
--	--	No Object (Warm Start)	14				F
--	--	No Object (Delay Measurement)	23				G

NOTES

C: Device supports write operations on Time and Date objects. Time Synchronization-Required Internal Indication bit (IIN1-4) will be cleared on the response.

D: The device can be configured to send or not, unsolicited responses depending on a configuration option by means of ***MMI*** (Man-Machine Interface or front-panel user interface ***ZIVercomPlus***). Then, the Master can Enable or Disable Unsolicited messages (for Classes 1, 2 and 3) by means of requests (FC 20 and 21).
If the unsolicited response mode is configured "on", then upon device restart, the device will transmit an initial Null unsolicited response, requesting an application layer confirmation. While waiting for that application layer confirmation, the device will respond to all function requests, including READ requests.

E: Restart Internal Indication bit (IIN1-7) can be cleared explicitly by the master.

F: The outstation, upon receiving a ***Cold or Warm Start*** request, will respond sending a Time Delay Fine object message (which specifies a time interval until the outstation will be ready for further communications), restarting the DNP process, clearing events stored in its local buffers and setting IIN1-7 bit (Device Restart).

G: Device supports Delay Measurement requests (FC = 23). It responds with the Time Delay Fine object (52-2). This object states the number of milliseconds elapsed between Outstation receiving the first bit of the first byte of the request and the time of transmission of the first bit of the first byte of the response.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DEVICE SPECIFIC FEATURES

- Internal Indication IIN1-6 (Device trouble): **Set to indicate a change in the current DNP configuration in the outstation. Cleared in the next response. Used to let the master station know that DNP settings have changed at the outstation. Note that some erroneous configurations could make impossible to communicate this condition to a master station.**

  This document also states the DNP3.0 settings currently available in the device. If the user changes whatever of these settings, it will set the *Device Trouble Internal Indication* bit on the next response sent.
- Event buffers**: device can hold as much as 128** Binary Input Changes**,** 64 Analog Input Changes and 64 Counter Input Change**. If these limits are reached the device will set the *Event Buffers Overflow Internal Indication* bit on the next response sent. It will be cleared when the master reads the changes, making room for new ones.**
- Configuration ➔ Operation Enable **menu: the device can enable or disable** permissions **for the operations over al Control Relay Output Block. In case permissions are configured off (disabled) the response to a command (issued as Control Relay Output Block) will have the Status code NOT_AUTHORIZED. In case the equipment is** blocked **the commands allowed are the configured when permitted. While blocked, the relay will accept commands over the configured signal. If the equipment is in** operation inhibited state**, the response to all commands over the configured signal will have the Status code NOT_AUTHORIZED.**
- **Customers can configure Inputs/Outputs to suit their needs, by means of** *ZIVercomPlus*® **software.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

POINT LIST

BINARY INPUT (OBJECT 1) -> Assigned to Class 0. BINARY INPUT CHANGE (OBJECT 2) -> Assign to Class.		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 2048 points**	
1	***Configure by ZIVercomPlus®* 2048 points**	
2	***Configure by ZIVercomPlus®* 2048 points**	
3	***Configure by ZIVercomPlus®* 2048 points**	
4	***Configure by ZIVercomPlus®* 2048 points**	
5	***Configure by ZIVercomPlus®* 2048 points**	
6	***Configure by ZIVercomPlus®* 2048 points**	
7	***Configure by ZIVercomPlus®* 2048 points**	
8	***Configure by ZIVercomPlus®* 2048 points**	
9	***Configure by ZIVercomPlus®* 2048 points**	
10	***Configure by ZIVercomPlus®* 2048 points**	
11	***Configure by ZIVercomPlus®* 2048 points**	
12	***Configure by ZIVercomPlus®* 2048 points**	
13	***Configure by ZIVercomPlus®* 2048 points**	
14	***Configure by ZIVercomPlus®* 2048 points**	
15	***Configure by ZIVercomPlus®* 2048 points**	
16	***Configure by ZIVercomPlus®* 2048 points**	
17	***Configure by ZIVercomPlus®* 2048 points**	
...	***Configure by ZIVercomPlus®* 2048 points**	
253	***Configure by ZIVercomPlus®* 2048 points**	
254	***Configure by ZIVercomPlus®* 2048 points**	
255	***Configure by ZIVercomPlus®* 2048 points**	

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
0	***Configure by ZIVercomPlus®* 256 points**	
1	***Configure by ZIVercomPlus®* 256 points**	
2	***Configure by ZIVercomPlus®* 256 points**	
3	***Configure by ZIVercomPlus®* 256 points**	
4	***Configure by ZIVercomPlus®* 256 points**	
5	***Configure by ZIVercomPlus®* 256 points**	
6	***Configure by ZIVercomPlus®* 256 points**	
7	***Configure by ZIVercomPlus®* 256 points**	
8	***Configure by ZIVercomPlus®* 256 points**	
9	***Configure by ZIVercomPlus®* 256 points**	
10	***Configure by ZIVercomPlus®* 256 points**	
11	***Configure by ZIVercomPlus®* 256 points**	
12	***Configure by ZIVercomPlus®* 256 points**	
13	***Configure by ZIVercomPlus®* 256 points**	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

CONTROL RELAY OUTPUT BLOCK (OBJECT 12)		
Index	**Description**	
14	***Configure by ZIVercomPlus*® 256 points**	
15	***Configure by ZIVercomPlus*® 256 points**	
16	***Configure by ZIVercomPlus*® 256 points**	
17	***Configure by ZIVercomPlus*® 256 points**	
...	***Configure by ZIVercomPlus*® 256 points**	
253	***Configure by ZIVercomPlus*® 256 points**	
254	***Configure by ZIVercomPlus*® 256 points**	
255	***Configure by ZIVercomPlus*® 256 points**	

ANALOG INPUT (OBJECT 30) -> Assigned to Class 0. ANALOG INPUT CHANGE (OBJECT 32) -> Assign to Class		
Index	**Description**	**Deadband**
0	***Configure by ZIVercomPlus*® 256 points**	**Deadband_1.**
1	***Configure by ZIVercomPlus*® 256 points**	**Deadband_2.**
2	***Configure by ZIVercomPlus*® 256 points**	**Deadband_3.**
3	***Configure by ZIVercomPlus*® 256 points**	**Deadband_4.**
4	***Configure by ZIVercomPlus*® 256 points**	**Deadband_5.**
5	***Configure by ZIVercomPlus*® 256 points**	**Deadband_6.**
6	***Configure by ZIVercomPlus*® 256 points**	**Deadband_7.**
7	***Configure by ZIVercomPlus*® 256 points**	**Deadband_8.**
8	***Configure by ZIVercomPlus*® 256 points**	**Deadband_9.**
9	***Configure by ZIVercomPlus*® 256 points**	**Deadband_10.**
10	***Configure by ZIVercomPlus*® 256 points**	**Deadband_11.**
11	***Configure by ZIVercomPlus*® 256 points**	**Deadband_12.**
12	***Configure by ZIVercomPlus*® 256 points**	**Deadband_13.**
13	***Configure by ZIVercomPlus*® 256 points**	**Deadband_14.**
14	***Configure by ZIVercomPlus*® 256 points**	**Deadband_15.**
15	***Configure by ZIVercomPlus*® 256 points**	**Deadband_16.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Additional assign with *ZIVercomPlus*®:

Index	Description
16	***Configure by ZIVercomPlus® 256 points***
17	***Configure by ZIVercomPlus® 256 points***
18	***Configure by ZIVercomPlus® 256 points***
19	***Configure by ZIVercomPlus® 256 points***
20	***Configure by ZIVercomPlus® 256 points***
21	***Configure by ZIVercomPlus® 256 points***
22	***Configure by ZIVercomPlus® 256 points***
23	***Configure by ZIVercomPlus® 256 points***
24	***Configure by ZIVercomPlus® 256 points***
25	***Configure by ZIVercomPlus® 256 points***
26	***Configure by ZIVercomPlus® 256 points***
27	***Configure by ZIVercomPlus® 256 points***
....	***Configure by ZIVercomPlus® 256 points***
62	***Configure by ZIVercomPlus® 256 points***
63	***Configure by ZIVercomPlus® 256 points***

The full scale ranges are adjustable and user's magnitudes can be created. It's possible to choose between primary and secondary values, considering CT and PT ratios. Typical ranges in secondary values are:

Description	Full Scale Range		
	Engineering units	Counts	
Currents (Phases, sequences, harmonics)	0 to 1,2 x In_{PHASE} A	0 to 32767	**Deadband**
Currents (Ground, polarizing)	0 to 1,2 x In_{GROUND} A	0 to 32767	**Deadband**
Currents (Ground sensitive, isolated neutral)	0 to 1,2 A	0 to 32767	**Deadband**
Voltages (Phase to ground, sequences, harmonics)	0 to 1,2 x Vn/√3 V	0 to 32767	**Deadband**
Voltages(Phase to phase, synchronizing)	0 to 1,2 x Vn V	0 to 32767	**Deadband**
Power (Real, reactive, apparent)	0 to 3 x 1,4 x In_{PHASE} x Vn/√3 W	-32768 to 32767	**Deadband**
Power factor	-1 to 1	-32768 to 32767	**Deadband**
Frequency	0 to 1,2 x Rated frequency (50/60 Hz)	0 to 32767	**Deadband**
Thermal value	0 to 200%	0 to 32767	**Deadband**
Distance to Fault - **Percentage of line length:** 100% sends 32767 counts (range from -100% to 100%) - **Distance in kilometers:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in km) - **Distance in miles:** with the "line length" sends 32767 counts (range from - "line length" to the "line length" set in miles)		-32768 to 32767	**Deadband**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Communication Measure in Counts

With ***ZIVercomPlus*** program is possible to define the ***Full Scale Range*** that is desired to transmit each magnitude in *counts*. Parameters necessary to configure the Mathematical expression are:

- **Offset:** A number indicating the compensation of de Magnitude.
- **Limit:** it's the Maximum value of magnitude range.
- **Max Communication:** it's a constant that depend of the Number Bits of Analog Input.
  Max Communication=2(Number Bits Analog Input - 1)**
  For 16-Bit Analog Input (Obj. 30 Var. 2) 2**(15) = 32.767 counts
  For 32-Bit Analog Input (Obj. 30 Var. 1) 2**(31) = 2.147.483.647 counts
- **Rated value:** Nominal Value of the magnitude.
- **Nominal Flag:** This *flag* defines if the **limit** is proportional to the **rated value** of the magnitude.
- **TR:** Secondary to Primary Transformation Ratio.

Mathematical expression to describe the ***Full Scale Range*** is:

- When **Nominal Flag** is actived,

$$MeasureCom = TR \times \frac{Measure - Offset}{RatedValue} \times \frac{MaxComunication}{Limit}$$

- When **Nominal Flag** is NOT actived,

$$MeasureCom = TR \times (Measure - Offset) \times \frac{MaxComunication}{Limit}$$

Communication Measure in Engineering Units

With ***ZIVercomPlus*** program **also** it's possible to transmit each magnitude in Engineering Units. Parameters necessary to configure the Mathematical expression are:

- **Offset:** A number indicating the compensation of de magnitude.
- **Limit:** it's the Maximum value of magnitude range.
- **Rated value:** Nominal Value of the magnitude.
- **Nominal Flag:** this *flag* defines if the **limit** is proportional to the **rated value** of the magnitude or not. The rated value of the new magnitudes defined by the user is a setting, while for the pre-defined magnitudes is a fix value.
- **TR:** Secondary to Primary Transformation Ratio.
- **Scaling Factor:** Multiply Factor of magnitude.

Atención © ***ZIV Aplicaciones y Tecnología, S.A.*** **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Mathematical expression to obtain **Measure in Engineering Units** is:

- When **Nominal Flag** is actived,

$$MeasureCom = TR \times \frac{Measure - Offset}{RatedValue} \times ScalingFactor$$

- When **Nominal Flag** is NOT actived,

$$MeasureCom = TR \times (Measure - Offset) \times ScalingFactor$$

DeadBands

- Deadband is an area of a magnitude range or band where no generate magnitude change (the magnitude is dead). Meaning that no generation of Analogical Change Events if difference with value of generation of previous change is not equal or greater that DeadBand calculated. There is an independent setting for each 16 Measures with change.
- A Deadband is calculated as a percentage defined in DeadBand Setting over value of **parameter Limit**.
- The Deadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface *ZIVercomPlus*), between 0.0000% and 100.00%, in steps of 0.0001%. Default value is 100.00%, meaning that generation of Analog Change Events is **DISABLED** for that input. There is an independent setting for each Magnitude with change.

BINARY COUNTER (OBJECT 20) -> Assigned to Class 0.
FROZEN COUNTER (OBJECT 21)

32 BIT COUNTER CHANGE EVENT (OBJECT 22) -> Assign to Class

Index	Description	Deadband
0	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_1.**
1	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_2.**
2	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_3.**
3	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_4.**
4	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_5.**
5	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_6**
6	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_7.**
7	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_8.**
8	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_9.**
9	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_10.**
10	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_11.**
11	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_12.**
12	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_13.**
13	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_14.**
14	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_15.**
15	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_16.**
16	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_17.**
17	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_18.**
18	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_19.**
19	***Configure by ZIVercomPlus®*** **256 points**	**CounterDeadBand_20.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

CounterDeadBands

- CounterDeadband is an area of a counter magnitude range or band, where no generate counter magnitude change (the communication counter magnitude is dead).Meaning that no generation of Counter Change Events if difference with value of generation of previous change is not equal or greater that CounterDeadBand setting. There is an independent setting for each Counter.

- The CounterDeadband can be adjusted to the device by means of ***MMI*** (Man-Machine Interface or front-panel user interface *ZIVercomPlus*), between 1 and 32767, in steps of 1, default value is 1.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP3 PROTOCOL SETTINGS

DNP3 Protocol Settings						
DNP Protocol Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step/ Select**	**Unit**
Relay Number	Integer	0	65519	1	1	
T Confirm Timeout	Integer	1000	65535	1000	1	msec.
Max Retries	Integer	0	65535	0	1	
Enable Unsolicited.	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Enable Unsol. after Restart	Boolean	0 (No)	1 (Yes)	0 (No)	1	
Unsolic. Master No.	Integer	0	65519	1	1	
Unsol. Grouping Time	Integer	100	65535	1000	1	msec.
Synchronization Interval	Integer	0	120	0	1	min.
DNP 3.0 Rev.	Integer	2003 ST.ZIV	2003 ST.ZIV	2003	2003 ST.ZIV	
Binary Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 1	None Class 1 Class 2 Class 3	
Analog Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 2	None Class 1 Class 2 Class 3	
Counter Changes CLASS	Integer	None Class 1 Class 2 Class 3	None Class 1 Class 2 Class 3	Class 3	None Class 1 Class 2 Class 3	
Binary Status Change	Boolean	0 (No)	1 (Yes)	1 (Yes)	1	
32 Bits Analog Input	Boolean	0 (No)	1 (Yes)	1 (Yes)	1	
Analog Inputs (Deadbands)						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step**	**Unit**
Deadband AI#0	Float	0 %	100 %	100 %	0.0001 %	
Deadband AI#1	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#2	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#3	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#4	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#5	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#6	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#7	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#8	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#9	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#10	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#11	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#12	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#13	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#14	Float	0 %	100 %	100 %	0. 0001 %	
Deadband AI#15	Float	0 %	100 %	100 %	0. 0001 %	

Atención © *ZIV Aplicaciones y Tecnología, S.A.* **Zamudio 2004**
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

Counter Inputs (CounterDeadbands)						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step**	**Unit**
Deadband Cont.I#0	Integer	1	32767	1	1	
Deadband Cont.I#1	Integer	1	32767	1	1	
Deadband Cont.I#2	Integer	1	32767	1	1	
Deadband Cont.I#3	Integer	1	32767	1	1	
Deadband Cont.I#4	Integer	1	32767	1	1	
Deadband Cont.I#5	Integer	1	32767	1	1	
Deadband Cont.I#6	Integer	1	32767	1	1	
Deadband Cont.I#7	Integer	1	32767	1	1	
Deadband Cont.I#8	Integer	1	32767	1	1	
Deadband Cont.I#9	Integer	1	32767	1	1	
Deadband Cont.I#10	Integer	1	32767	1	1	
Deadband Cont.I#11	Integer	1	32767	1	1	
Deadband Cont.I#12	Integer	1	32767	1	1	
Deadband Cont.I#13	Integer	1	32767	1	1	
Deadband Cont.I#14	Integer	1	32767	1	1	
Deadband Cont.I#15	Integer	1	32767	1	1	
Deadband Cont.I#16	Integer	1	32767	1	1	
Deadband Cont.I#17	Integer	1	32767	1	1	
Deadband Cont.I#18	Integer	1	32767	1	1	
Deadband Cont.I#19	Integer	1	32767	1	1	
DNP Port 1 Port 2 and 3 DNP 3 Profile II Ethernet Configuration						
Setting Name	**Type**	**Minimum Value**	**Maximum Value**	**Default Value**	**Step**	**Unit**
Protocol Select	**Uinteger**	**Procome Dnp3 Modbus**	**Procome Dnp3 Modbus**	**Procome**	**Procome Dnp3 Modbus**	
Enable Ethernet Port	**Boolean**	**0 (No)**	**1 (Yes)**	**1 (Yes)**	**1**	
IP Address Port 1	**Byte[4]**	**ddd.ddd.ddd.ddd**	**ddd.ddd.ddd.ddd**	**192.168.1.51**	**1**	
IP Address Port 2	**Byte[4]**	**ddd.ddd.ddd.ddd**	**ddd.ddd.ddd.ddd**	**192.168.1.61**	**1**	
IP Address Port 3	**Byte[4]**	**ddd.ddd.ddd.ddd**	**ddd.ddd.ddd.ddd**	**192.168.1.71**	**1**	
Subnet Mask	**Byte[4]**	**128.0.0.0**	**255.255.255.254**	**255.255.255.0**	**1**	
Port Number	**Uinteger**	**0**	**65535**	**20000**	**1**	
Keepalive Time	**Float**	**0**	**65**	**30**	**60**	**s.**
Rx Time Characters	**Float**	**1**	**60000**	**1**	**0.5**	**ms.**
Comms Fail Timer	**Float**	**0**	**600**	**60**	**0.1**	**s.**

✓ **All settings remain unchanged after a power loss.**

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP Protocol Configuration

- **Relay Number (RTU Address):**
  Remote Terminal Unit Address. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*.
- **T Confirm Timeout (N7 Confirm Timeout) :**
  Timeout while waiting for Application Layer Confirmation. It applies to Unsolicited messages and Class 1 and Class 2 responses with event data.
- **Max Retries (N7 Retries) :**
  Number of retries of the Application Layer after timeout while waiting for Confirmation.
- **Enable Unsolicited (Enable Unsolicited Reporting) :**
  Enables or disables Unsolicited reporting.
- **Enable Unsol. after Restart :**
  Enables or disables Unsolicited after Restart (for compatibility with terminals whose revision is before DNP3-1998). It has effect only if Enable Unsolicited after Restart is set.
- **Unsolic. Master No. (MTU Address) :**
  Destination address of the Master device to which the unsolicited responses are to be sent. Addresses 0xFFF0 to 0xFFFF are reserved as *Broadcast Addresses*. It is useful only when Unsolicited Reporting is enabled.
- **Unsol. Grouping Time (Unsolicited Delay Reporting) :**
  Delay between an event being generated and the subsequent transmission of the unsolicited message, in order to group several events in one message and to save bandwidth.
- **Synchronization Interval**
  Max interval time between two synchronization. If no synchronizing inside interval, indication IIN1-4 (NEED TIME). This setting has no effect if Synchronization Interval is zero.
- **DNP 3.0 Rev.**
  Certification revision **STANDARD ZIV** or **2003** (DNP3-2003 Intelligent Electronic Device (IED) Certification Procedure Subset Level 2 Version 2.3 29-Sept-03)
- **Binary Changes CLASS.**
  Selection to send Binary Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Analog Changes CLASS.**
  Selection to send Analog Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Counter Changes CLASS.**
  Selection to send Counter Changes as CLASS 1 CLASS 2 CLASS 3 or None.
- **Binary Status .**
  Send Binary with status otherwise without status
- **32 Bits Analog Input .**
  Send Analog All Variations and Analog Change Event Binary Changes with 32 bits otherwise with 16 bits

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

DNP PROFILE II ETHERNET Port 1 Port 2 and Port 3 Configuration

- **Enable Ethernet Port :**
  Enables or disables Ethernet Port.

- **IP Address :**
  Identification Number of Ethernet device.

- **Subnet Mask :**
  Indicate the part of IP Address is the Net Address and the part of IP Address is the Device Number.

- **Port Number :**
  Indicate to Destinatión Device the path to send the recived data.

- **Keepalive Time :**
  Number of second between Keepalive paquets, if zero no send packages Keepalive. These packages allow to Server know if a Client is present in the Net.

- **Rx Time Between Characters :**
  Maximum time between Characters.

- **Comm Fail Timer :**
  Maximum time between Messages without indicate Communication Fail.

Atención © *ZIV Aplicaciones y Tecnología, S.A.* Zamudio 2004
Este documento contiene información confidencial propiedad de ZIV S.A. Cualquier forma de reproducción o divulgación está absolutamente prohibida y puede ser causa de severas medidas legales.

C. MODBUS RTU Documentation. Address Map

C.1 Preliminary Information C-2
C.2 Function 01: Read Coil Status C-2
C.2.1 Modbus Address Map for RTF C-2
C.3 Function 02: Read Input Status C-3
C.3.1 Modbus Address Map for RTF C-3
C.4 Function 03: Read Holding Registers C-3
C.4.1 Modbus Address Map for RTF C-3
C.5 Function 04: Read Input Registers C-4
C.5.1 Modbus Address Map for RTF C-4
C.6 Function 05: Force Single Coil C-5
C.6.1 Modbus Address Map for RTF C-5

C.1 Preliminary Information

This a reference document for implementing the MODBUS RTU protocol in the **RTF** IED.

This document provides a detailed MODBUS address map (input status, coil status, input registers and force single coil) and their equivalent in the **RTF** relay.

The functions that will be implemented are:

ModBus Function	Meaning
01	Read Coil Status
02	Read Input Status
04	Read Input Registers
05	Force Single Coil

Any other function not among those indicated will be considered illegal and will return exception code 01 (Illegal function).

C.2 Function 01: Read Coil Status

C.2.1 Modbus Address Map for RTF

The MODBUS coil status address map for the **RTF** relay will be:

Address	Description
Configurable through the *ZIV e-NET tool*®	Any input or output logic signal from the protection modules or generated by the programmable logic.

The content of the addresses is variable (reflection of each relay's configuration). The range of addresses is from 0 to 1023 and they are assigned automatically by the ***ZIV e-NET tool***® program.

Non-configured addresses will be considered illegal and will return exception code 02 (Illegal Data Address).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

C.3 Function 02: Read Input Status

C.3.1 Modbus Address Map for RTF

The MODBUS input status address map for the **RTF** relay will be:

Address	Description
Configurable through the *ZIV e-NET tool*®	Any input or output logic signal from the protection modules or generated by the programmable logic.

The content of the addresses is variable (reflection of each relay's configuration). The range of addresses is from 0 to 1023 and they are assigned automatically by the ***ZIV e-NET tool***® program.

Non-configured addresses will be considered illegal and will return exception code 02 (Illegal Data Address).

C.4 Function 03: Read Holding Registers

C.4.1 Modbus Address Map for RTF

The MODBUS read holding registers address map for the **RTF** relay will be:

Address	Description
Configurable through the *ZIV e-NET tool*®	Any input or output logic signal from the protection modules or generated by the programmable logic whose number of changes is to be measured.

Configurable through the ***ZIV e-NET tool***®: Counters can be created with any signal configured in the programmable logic or from the protection modules. The default counters are those of the real energies (positive and negative) and the reactive energies (capacitive and inductive).

The metering range of energies in primary values is from 100wh/varh to 6553.5 kWh/kVArh. This is the magnitude transmitted via communications. That is, one (1) count represents 100 wh/varh.

To obtain an energy counter with a higher maximum value, a “user magnitude” must be created using this counter. For example, dividing the value of the counter by 1000 and making the output of the divider the new magnitude yields an energy counter with a range from 100 kWh/kVArh to 6553.5 MWh/Mvarh; that is, one (1) count represents 100 kWh/varh.

The content of the addresses is variable (reflection of each relay's configuration). The range of addresses is from 0 to 255 and they are assigned automatically by the ***ZIV e-NET tool***® program.

Non-configured addresses will be considered illegal and will return exception code 02 (Illegal Data Address).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

C.5 Function 04: Read Input Registers

C.5.1 Modbus Address Map for RTF

The MODBUS read input registers address map for the **RTF** relay will be:

Address	Description
Configurable through the *ZIV e-NET tool*®	Any magnitude measured or calculated by the protection or generated by the programmable logic. It is possible to select between primary and secondary values, taking into account the corresponding transformation ratios.

All the full scale values of the magnitudes are definable, and these magnitudes can be used to create *User Defined Values*. Some typical values are:

- Phase and sequence currents and harmonics: **Rated value I_{PHASE} + 20**% sends 4095 counts.
- Ground and synchronization currents: **Rated value I_{GROUND} + 20%** sends 4095 counts.
- Sensitive ground and directional ungrounded currents: **1.2 A** sends 4095 counts.
- Phase voltages, sequence and harmonics voltages: **(Rated value V / √3) + 20%** sends 4095 counts.
- Line and polarization voltages: **Rated value V + 20%** sends 4095 counts.
- Powers: 3 x 1.4 x Rated value I_{PHASE} x Rated value / √3 sends 4095 counts.
- Power factor: from **–1** to **1** sends from –4095 to 4095 counts.
- Frequency: from **0 Hz** to **1.2 x Frequency$_{RATED}$** (50Hz / 60Hz) sends 4095 counts.
- Thermal value: **240%** sends 4095 counts
- Distance to the fault:
  - Percentage value: **±100%** sends ±4095 counts (range from -100% to 100%).
  - Value in kilometers: with the ***Length*** of the line, it sends ±4095 counts (range from 0 km to the length of the line set in km. It can also send negative values).
  - Value in miles: with the ***Length*** of the line, it sends ±4095 counts (range from 0 km to the length of the line set in miles. It can also send negative values).

With the ***ZIV e-NET tool***® program, it is possible to define the full-scale value to be used to transmit this magnitude in counts, the unit that all the protocols use. There are three definable parameters that determine the range of distance covered:

- **Offset value**: the minimum value of the magnitude for which 0 counts are sent.
- **Limit**: the length of the range of the magnitude on which it is interpolated to calculate the number of counts to send. If the offset value is 0, it coincides with the value of the magnitude for which the defined maximum of counts (4095) is sent.
- **Nominal flag**: this flag allows determining whether the limit set is proportional to the rated value of the magnitude or not. The rated value of the new magnitudes defined by the user in the programmable logic can be configured, while the rest of the existing magnitudes are fixed.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- When the Nominal flag is enabled,

$$CommunicationsMeasurement = \frac{Measurement - Offset}{Nominal} \times \frac{32767}{Limit}$$

- When the Nominal flag is NOT enabled,

$$CommunicationsMeasurement = (Measurement - Offset) \times \frac{32767}{Limit}$$

The content of the addresses is variable (reflection of each relay's configuration). The range of addresses is from 0 to 255 and they are assigned automatically by the ***ZIV e-NET tool***® program.

Non-configured addresses will be considered illegal and will return exception code 02 (Illegal Data Address).

C.6 Function 05: Force Single Coil

C.6.1 Modbus Address Map for RTF

The MODBUS force single coil address map of the **RTF** relay will be:

Address	Description
Configurable through the *ZIV e-NET tool*®	A command can be made on any input from the protection modules and on any signal configured in the programmable logic.

The content of the addresses is variable (reflection of each relay's configuration). The range of addresses is from 0 to 255 and they are assigned automatically by the ***ZIV e-NET tool***® program.

Non-configured addresses will be considered illegal and will return exception code 02 (Illegal Data Address).

Any value other than 00H or FFH will be considered illegal and will return exception code 03 (Illegal Data Value).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D. IEC 61850 Ed.2

D.1 IEC 61850 Standard D-2
D.2 Communications Stack D-3
D.3 IEC 61850 Server and Data Model D-4
D.4 Web Server D-5
D.5 Communications Port D-7
D.6 File Transfer D-8
D.7 CID Configuration File D-9
D.8 Mod/Beh D-10
D.9 Data Set D-11
D.10 Send GOOSE Messages D-12
D.11 Subscription to GOOSE Message Data D-14
D.12 Report Control Blocks (RCBs) D-21
D.13 Measurement Configuration (Data CF) D-23
D.14 Commands D-24
D.15 SNTP Synchronization D-25
D.15.1 SNTP Synchronism Status Calculation D-25
D.15.1.a *Unicast* Client D-25
D.15.1.b *Broadcast* Client D-26

D.1 IEC 61850 Standard

IEC 61850 relay models have an extra protection and control function defined by **IEC 61850** standard.

Extra services provided by **IEC 61850** relays are:

- Reporting relay data (pickups, trips, blockings, etc) to a higher level equipment (Central Unit, Remote Control, HMI, etc).
- Quick data reporting (GOOSE) to same level relay (protections, control equipment, auxiliary services) or, even to other higher level equipment.
- MMS communications allowing any MMS client to receive the relay data model, thus being able to interact with it for editing settings and parameters and carry out commands.
- Managing a single file (**CID**) that allows to have a *backup* containing all protection, control and communications parameters.
- FTP access to oscillograms, logs, etc.
- Web server providing information on the relay status, errors, status and measurements, subscription to GOOSE messages, etc.

Each protection element contains **IEC 61850** mapping information with regard to node name and settings, available digital signals, commanding data, measurements, etc.

IEC 61850 is a substation automation standard defined by the TC57 Technical Committee. The standard is segregated into 10 parts and deals with issues related to general system requirements, engineering project management and communications requirements, putting forward a data model on which IED capacities are described. This data model is developed through the substation description language (SCL) also defined in the standard. Relay functions are modelled from the so called Logic Nodes (LN) that, at the same time, are formed from *Common Data Classes* and *Common Data Attributes*, following an object abstraction philosophy. Together with these objects, the standard defines a set of services through the so called *Abstract Communication Service Interface* (ACSI). Sections 8 and 9 of the standard explain how these objects and services are mapped in terms of given protocols, specifically, MMS, GOOSE and Sampled Values. The last section of the standard deals with the conformity tests that a relay or architecture must pass in order to be approved according to the standard, thus covering all aspects.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Therefore, the standard includes the chapters or parts below:

- *IEC 61850-1: Introduction and overview.*
- *IEC 61850-2: Glossary.*
- *IEC 61850-3: General requirements.*
- *IEC 61850-4: System and project management.*
- *IEC 61850-5: Communication requirements for functions and device models.*
- *IEC 61850-6: Configuration language for communication in electrical substations related to IEDs.*
- *IEC 61850-7: Basic communication structure for substation and feeder equipment.*
  IEC 61850-7-1: Principles and models.
  IEC 61850-7-2: Abstract communication service interface (ACSI).
  IEC 61850-7-3: Common Data Classes.
  IEC 61850-7-4: Compatible logical node classes and data classes.
- *IEC 61850-8-1: Specific communication service mapping (SCSM) Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2) and to ISO/IEC8802-3.*
- *IEC 61850-9: Specific communication service mapping (SCSM).*
  IEC 61850-9-1: Sampled values over serial unidirectional multidrop point to point link.
  IEC 61850-9-2: Sampled values over ISO/IEC 802-3.
- *IEC 61850-10: Conformance testing.*

D.2 Communications Stack

The IED will be based on the *Client-Server* model to give data contained in its data model in a vertical way. It is a connection oriented communications, always initiated by the client and, in this case, using the MMS (*Manufacturing Message Specification*) standard, specifically developed for industrial applications, specified according to ISO 9506 and used for data interchange in production environments. This protocol is independent of the type of network or connected devices and, therefore, can be maintained as physical communications technology evolves. The protocol defines communications messages transferred between controllers, as well as between the engineering station and the controller, so that the server (IED) will make available to the clients (central units, gateways, SCADAs, computers, etc.) the data selected in a *Data Set* that will have been allocated to a *Report Control Block*. The IEC 61850-8-1 part defines the mapping between the MMS protocol service and the IEC 61850 abstract services.

The IED also has the *Publisher-Subscriber* model that the GOOSE service is based on. In this case, it is a high speed non connection oriented communications, thus enabling horizontal communications between IEDs. The message sent by the publisher will be a *multicast* message that will propagate through the local network, thus reaching all the IEDs connected to the same.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.3 IEC 61850 Server and Data Model

The IED server and, thus, the physical device, contains four *Logical Devices*. Those *Logical Device* includes all the different *Logical Nodes* that, at the same time, contain *Data Objects* composed of *Data Attributes* and that, as a whole, form the relay data model. Services to carry out a number of functions, as they are reading and writing data, commands, reporting, etc., are available at every level.

The distribution of the Logical Nodes inside the Logical Devices is the following one:

- **SYS**: *Logical Device* of the System where the *Report Control Blocks, GOOSE Control Blocks, Setting Group Control Blocks, LOGs*, etc. are located. Data Set will appear also here once configured and this is the place where the *Logical Nodes* related to the hardware of the IED are located (inputs, outputs, communications, synchronization, etc.).
- **CTRL**: *Logical device* where are located all the control *Logical Nodes* that can be instantiated with the configuration tool.
- **PROT**: *Logical device* where are located the Logical Nodes of the IED.
- **MEA**: *Logical device* where are located the *Logical Nodes* related to measurements.

Apart from the protection nodes, such as PHSPIOC, PTOV, PTOF, PTUF, RREC, RBRF, PTRC, etc. that are defined in the applicable chapters where the relay protection functions are explained, the relay has the configurable control nodes described below. These control nodes will not be present in the relay data models unless they have been registered and configured with the configuration tool:

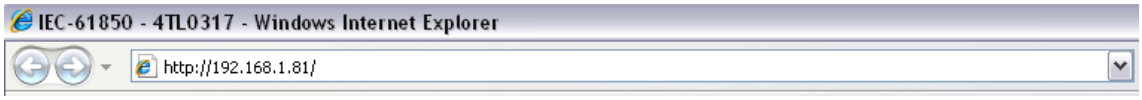
- XCBR: control node that features a double digital data used to map the status of a three pole breaker.
- XSWI: node that features a double digital data used to map the status of the disconnect switches.
- CSWI: this control node contains the double commands on the switchgear (breaker and disconnect switches).
- CILO: control node used to map the permits of the different commanding objects.
- GAPC: general control node with single and double general purpose states and commands except for switchgear elements (breakers and disconnect switches).
- GENGGIO: general control node with single and double status and integer and floating analog measurements used to have any relay data available in IEC 61850. Although there are up to a maximum of 4 nodes of this type, using as far as possible the relay own protection nodes is recommended, restricting the use of these nodes to own user data generated in the control logic.
- CALH: control node used to map bay alarms.
- SIMG: control node used to map SF6 alarm and trip.
- PLSMMTR: control node used to map energy meters calculated in control logic, normally from pulse inputs coming from external energy meters.
- SETGGIO: control node used to map and thus have user settings generated in the relay control logic available through MMS.
- LGOS: control node used to monitor the state of an input GOOSE.

The MICS file (Model Implementation Conformance Statement), which describes the extensions of the IEC 61850 data model in relation to the standard, is generated automatically by the configuration tool once defined the IED model.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.4 Web Server

Firmware versions, boot up status and useful relay data, can be accessed through the web server (using HTTP or HTTPS). To gain access, write the relay IP in a web browser:



Once authenticated (user data, password for only read access), the following data will be displayed:

- **Configuration**: relay identification data (hostname, location, contact, complete product model, firmware version, firmware reference and serial number) and access control data and certificates (see Cybersecurity Annex) are displayed. Additionally, it is allowed, only with the corresponding permission, to enable and disable Serial Log (option for analysis of internal anomalies by the manufacturer). Click ***Send*** and ***Apply*** to run this action.
- **Statistics**: this section shows the time the relay has been operating since the last boot up, the date and UTC time, the percentage of memory used and the percentage of CPU used. The relay date can be edit with permission to change settings.
  - **Routing**: traffic statistics can be accessed in case of using routers.
- **Log menu.** It is accessible with permission to manage logs. Shows the following information:
  - **System log:** register with boot up and system operation data that informs the user on the relay status where the reasons for CID rejection and other issues can be consulted. This register is stored in non-volatile memory. Click the button located at the top of the screen within section Download of System log, named Download File, to download the data into a text file.
  - **Security log**: see Cybersecurity Annex.
- **IEC-61850**. A number of data related to IEC 61850 standard are displayed.
  - **CID log**: register with loading data of new CID files. This register is stored in volatile memory since it stores data related to the last load. The history file may be obtained from System log.
  - **Analog signals list**: list of analog measurements available in IEC 61850 with the following data:
    - Description.
    - MMS path.
    - Value.
    - Quality: it consists of 3 fields:
      - Validity (**G**ood, **I**nvalid, **R**eserved, **Q**uestionable)
      - Quality Bit (**OV** overflow, **OR** out of range, **BR** bad reference, **OS** oscillatory, **FL** failure, **OD** old data, **ER** inconsistent, **IN** inaccurate)
      - Origin (**P** process, **S** substituted)/**T**est/Operator**B**locked.
    - Date of last update.
    - Information concerning maximum and minimum calculation (whether automatic or not).
    - Maximum value.
    - Minimum value.
    - Magnitude deadband setting.
    - Angle deadband setting.
  - **Digital signals list**: list of digital signals available in IEC 61850 with description, MMS path, value, quality and date of last update.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **GOOSE subscription list**: list of subscriptions to GOOSE messages where the configured subscription data can be seen (MAC, APPID, GOID, etc.) and the subscription status:
  - NOT FOUND: The configured GOOSE has never been received. The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA. It is the initial state of subscriptions.
  - OK: The GOOSE has been received perfectly and has been received before the TAL (TimeAllowedToLive). The quality of the data subscribed to that GOOSE (node GIGGIO1) will be either that contained in the GOOSE if the data is subscribed to the quality or GOOD if it is not.
  - TIME OUT: The GOOSE has ever been perfectly received and is no longer received in the TAL (TimeAllowedToLive). The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA.
  - STRUCT ERROR: The GOOSE has been received but the type of data does not match the expected type or the information is not present in the GOOSE. The quality of the data subscribed to that GOOSE (node GIGGIO1) whose type does not match the expected type will be INVALID and without cause. If any of the information expected in the GOOSE mapped to the data does not match or that information does not travel in the GOOSE, the quality of the data will be marked as INVALID (that is, if for the GIGGIO1.Ind1 data the stVal, q and t of the data is mapped and the t is received with a type that does not correspond or does not travel in the GOOSE, the GIGGIO1.Ind1.q quality will be INVALID, even though the stVal and q are being received OK). Within that GOOSE, data received correctly will be processed normally.
  - NDSCOM ERROR: The received GOOSE comes with the NdsCom field to TRUE. The GOOSE is ignored and the quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA.
  - ERROR HOLD TIME: The received GOOSE has TAL=0. In this case, the GOOSE is ignored.
  - CONFREV ERROR: The GOOSE has been received perfectly, but with ConfRev different from that configured. The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately passed to QUESTIONABLE by OLDDATA.
  - DATSET ERROR: The GOOSE has been received perfectly, but with a different DatSet than the one configured. The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately transferred to QUESTIONABLE by OLDDATA.
  - INTERRUPTED: The IED has stopped/interrupted the subscription to this GOOSE (for example, because the computer switches to Off mode). The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately switched to QUESTIONABLE by OLDDATA.
  - WAITING: Indicates that, having received and processed GOOSEs correctly, a change of LPHD1.Sim=FALSE has been detected. The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA. This status will only be changed when a change in LPHD1.Sim=FALSE is detected and LGOS[X].SimSt=TRUE has just been obtained.
- **Download file:** the name of the active CID file that the relay is operating with is displayed to the top as title. Click the Download File button located under it to download the file.

- **Actions menu** (only with administrator access).
  - **Apply**. After having been changed and sent, the parameters are applied to the relay.
  - **Clear Statistics**. Deletes statistics stored in the relay.
  - **Reboot**. Resets the relay.
  - **Reflash**. Updates the relay with a new firmware version.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Taking into account the differences between the actions below (only available for administrator users) is very important.

- Send changed parameters to the relay. Click ***Send*** in the modified page to carry out this action.
- Once the desired parameters have been configured, the ***Apply*** action will activate these changes and the relay will commence to use the new applied configuration.
- Click ***Reboot*** to reset the relay.

D.5 Communications Port

The IEDs have two or four LAN ports for IEC 61850 communications. This LAN ports use the Ethernet network, using the TCP/IP protocol for MMS (standard used to pack the information in the network) communications, sending and receiving GOOSE messages, file transfer through FTP, etc. Therefore, regardless the physical media and the connection (fiber, copper, etc.), configuring the relay network IP configuration is necessary.

The relay can communicate in IEC 61850 with up to 10 clients and with 4 masters simultaneously, the port number and the protocol (PROCOME, DNP3 or MODBUS) being able to be configured. Also, the relay will always be able to communicate simultaneously with the manufacturer tool for relay remote management through the fixed port 32001.

The relay will therefore have a menu to configure the LAN ports:

- DHCP enable.
- IP address.
- Network mask.
- Routing configuration menu if required.
- Redundancy type.

And a menu to configure the TCP/IP protocols simultaneously enabled together with IEC 61850:

- PROCOME protocol: fixed connection to the TCP/IP 32001 port for remote relay management through the manufacturer tool.
- Protocols 1, 2, 3 and 4: settings to indicate protocol, TCP/IP port, etc. for simultaneous TCP/IP communications with the relay.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.6 File Transfer

File transfer access (using FTP or SFTP) will enable the availability of a number of relay folders. Different access levels will be obtained as a function of the user and password.

Accessing the equipment with user with visualization permission, read only access is gained to the following directories:

- COMTRADE: folder where the generated oscillograms are saved.
- SCL: folder containing the active CID that the relay is working with (SCL/active/).

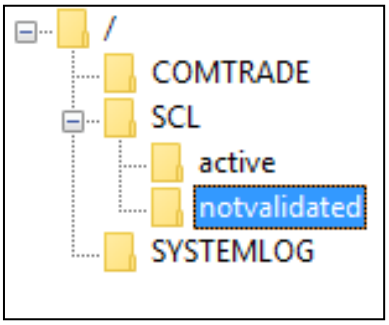


Figure D.1 Directory Structure for File Transfer.

Accessing the equipment with a user with permission to manage logs, you have read-only access to the following directory:

- **SYSTEM LOG**: folder containing *System.log* and *Security.log*.

Accessing the equipment with user with configuration loading permission, the equipment also offers write permission on the */SCL/notvalidated* folder, where the user can copy the new CID to load the equipment. When the new CID is copied to that location the equipment begins its validation.

In those cases where the relay is reset or has had a bad operation, the firmware automatically generates a file, *coredump,* where the status at the time of the failure is stored so as to be able to analyse the issue. Accessing by file transfer with a user with permission to manage logs, access to a read only folder with this information is gained.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.7 CID Configuration File

The standard defines the following files that will form part of the IED configuration process:

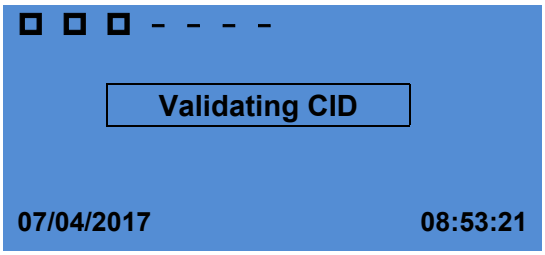
- ICD: file describing the IED capabilities. All nodes are extended and without configuration.
- CID: file containing a specific IED configuration at IED name, communications, Reports, etc. level

Both files allow knowing the relay data model in Logical Devices, Logical Nodes, Data and Attribute form. Once the relay has an IEC 61850 firmware, a file (**CID**) will be available in the format proposed by the **IEC 61850** standard according to section 6 (SCL) that can be downloadable by file transfer, web server or FileTransfer service of IEC 61850.

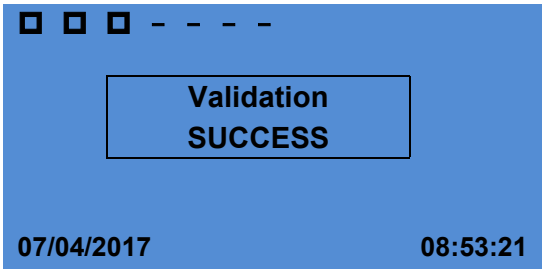
The CID file is used to configure send GOOSE message parameters, subscription to data of other GOOSE messages, create and allocate *datasets* to Report Control Blocks (RCBs) and GOOSE Control Blocks (GCBs), edit settings, control logic, descriptions, parameters etc.

The file can be edited using the program ***ZIV e-NET Tool***®. This program allows configuring the file that will later be sent to the relay through file transfer from the configuration tool. The starting CID file can be the file downloaded from the relay or a new file generated from the tool itself.

When a new CID file is loaded to the relay through file transfer (using a user with configuration loading permission), it is validated by the relay checking it is a correct SCL and that the configured IP in the file matches the IP configured in the relay, and the message **Validating CID** is displayed on the screen.

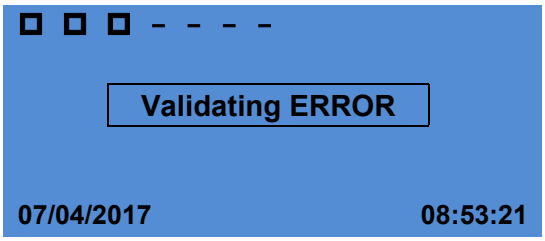


Once it has been validated, if the result is correct, the message **Validation SUCCESS** is displayed on the screen and the relay will be rebooted and reconfigured. The relay will be reset and will displayed the message **Configuring Device** and a progress bar on the screen. Upon completion of the reconfiguration process, the relay will be rebooted with the new configuration. The complete validation and reconfiguration process lasts about the minute.



© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Upon failed validation, the CID file will be rejected and deleted from the loading directory (non validated), the message **Validation ERROR** being displayed on the screen. In this case, web server logs can be accessed (through the web server, file transfer or File Transfer service of IEC 61850) in order to know the reasons for file rejection. Therefore, the relay will keep operating with the CID file that was active and communications will never be lost.



D.8 Mod/Beh

The standard defines the following values in the Logical Nodes for the Mod and Beh.

Value	Status	LN Behaviour
1	On	The application represented by the LN works. All communication services work and get updated values. DOs will be transmitted with a relevant quality. Control commands with Test=false will be accepted. Control commands with Test=true will be rejected.
2	Blocked	The application represented by the LN works. No (wired) output data will be issued to the process. All communication services work and get updated values. DOs will be transmitted with a relevant quality. Control commands with Test=false will be accepted. Control commands with Test=true will be rejected.
3	Test	The application represented by the LN works. All communication services work and get updated values. DOs will be transmitted with q.test=true, except Mod, Beh and Health that have q.test=false. Control commands with Test=false will be rejected. Control commands with Test=true will be accepted.
4	Test/Blocked	The application represented by the LN works. No (wired) output data will be issued to the process. All communication services work and get updated values. DOs will be transmitted with q.test=true, except Mod, Beh and Health that have q.test=false. Control commands with Test=false will be rejected. Control commands with Test=true will be accepted.
5	Off	The application represented by the LN does not work. All communication services work (output with quality.validity=invalid, except Mod, Beh and Health that will have q.validity=good). No process output will be done. Control commands to the process will be rejected. Only Mod accepts control command with Test=false. Settings and configuration attributes are still modifiable.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The complete IED (not by LN) supports the five modes. The LNs individually support ON and OFF modes and most of the protection related LNs also support the Blocked.

It is implemented a hierarchy management for the LDs (*GrRef* of LLN0). The format for the *GrRef.setSrcRef* in the SCL is: "@<*LDinst*>" or "<*IEDname*><*LDinst*>" and in the on-line data model is: "<*IEDname*><*LDinst*>" or "<*LDname*>".

The "root" is **SYS** and therefore all the other LDs will contain the *GrRef* in their LLN0 with "**@SYS**" value, which will be read only, so that all the LDs will inherit the status of **SYS** LD.

The IED will provide the following features related to the test mode:

- All the information sent/available in the IED will have test indication (q.test=true) and the following inputs will be considered as valid:
  - Data received by GOOSE message with *q*.test = true.
  - Commands received with Test=true attribute.
- Multicast signals used for simulation (GOOSE):
  - Suscription: Sim is the data object used to change the status/behaviour. It is present just in LPHD1 LN of **SYS** LD and will indicate the behaviour of the GOOSE simulation for all the IED. When the IED is receiving the same GOOSEin both ways, real (simulation bit=false) and simulated (simulation bit=true), the IED will take into account just to one of them depending on the value/status of *SYS/LPHD1.Sim.stVal.*
    - Real GOOSE if SYS/LPHD1.Sim.stVal=false.
    - Simulated GOOSE/SV if *SYS/LPHD1.Sim.stVal=false*. In this case, the SimSt of SYS/LGOS LN configured to monitor that GOOSE message will go to TRUE, showing that the IED is receiving and processing a simulated GOOSE message.
  - Publishing: The IED will have one setting per Goose Control Block (***Goose Control Block X Simulated***) that allows sending normal or simulated GOOSE messages. Therefore, depending on the settings, the IED will send the corresponding GOOSE message with the simulated bit in TRUE or FALSE.

D.9 Data Set

The relay supports a maximum of 35 Data Sets, each containing a maximum of 500 FCDAs.

The FC allowed in a Data Set which will be assigned to a RCB are the following ones: ST, MX, SP, CF, DC, SG, SR, OR, BL and EX.

The FC allowed in a Data Set which will be assigned to a GCB are the following ones: ST, MX and SP.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.10 Send GOOSE Messages

This service is defined in the standard and enables horizontal, fast and safe communications between IEDs. They are *multicast* messages and, thus, the emitter will place the data in the network and this will be received by any relay connected to the same. It has a message repeat algorithm, so that the data can be received by new relays connected to the network and, in this way, the receiving IEDs can detect communications or own emitter failures and act accordingly. The IEDs have 10 GCBs, so that they can be configured to send up to 10 different GOOSE messages. Each GCB has the following configurable parameters:

- MAC: send GOOSE message virtual MAC address
- VLAN ID: VLAN identifier
- AppID: application identifier. Parameter used to differentiate between GOOSE messages.
- VLAN Priority: message priority identifier.
- MinTime: minimum GOOSE message repeat time.
- MaxTime: maximum failure detection time on the part of the receiver (MaxTAL). The maximum GOOSE message repeat time will be MaxTime/2.
- GoID: string with a maximum size of 65 octets, which identifies the GOOSE message.
- GoRef: with a maximum size of 65 octets, which identifies the name of the GCB.
- Data Set: Data Set to be sent in the GOOSE message.
- Description: user-editable identifier to provide extra information.

Configuration version (ConfRev) is automatically calculated by the configuration tool and update at the time of generating the CID file.

Both *Data Attributes* and *Data Objects* (any FCD with a single FC ST/MX) can be sent through GOOSE and the same Data Set can be allocated to a GCB and a RCB. The relay can send both single and double digital signals, (SPS) and (DPS), integer data (INT) or analog measurements (FLOAT). When a measurement is allocated to a Data Set that will later be allocated to a GCB, it must be taken into account that, if the *deadband* associated to this measurement is configured to 0, this measurement will not be assessed, it will never generate a change and, therefore, will not cause GOOSE *trigger* by a change of value. If, otherwise, an instantaneous measurement is selected in the Data Set associated to a GOOSE message, every change of measurement will produce GOOSE sending.

In order to carry out the configuration, a Data Set must be first generated with the data to be sent in the GOOSE message. As a rule, attribute pairs (data, q) are sent but the relay can work with any type of Data Set. Later, this Data Set will be allocated to the desired GCB, any of the 10 existing in the relay model.

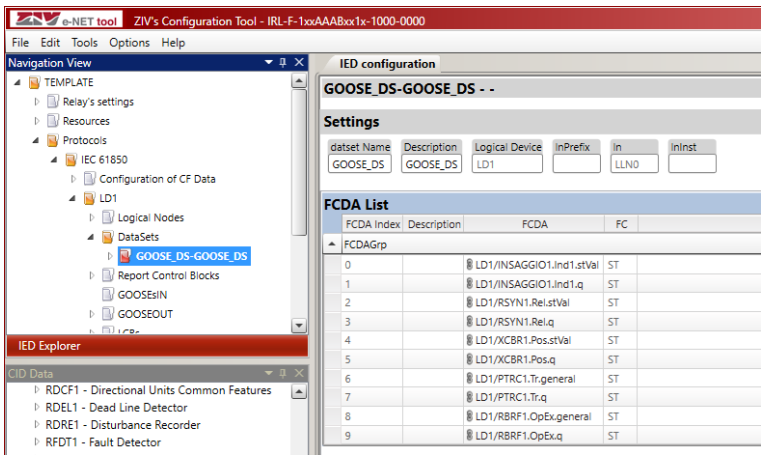


Figure D.2 Data Set configuration for GOOSE.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

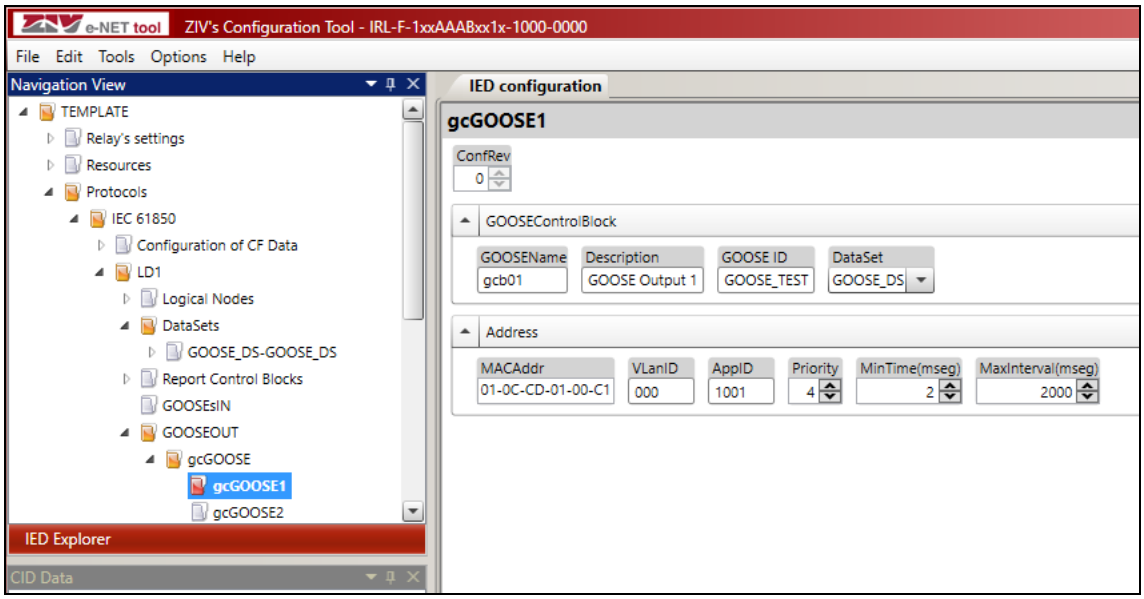


Figure D.3 GCB1 Configuration with Data Set Generated in Advance.

In this way, when a tool-generated CID is sent to the relay, after boot up, it will start sending a GOOSE message with the configured Data Set data.

If the Data Set allocated to the GCB is so large that the relay is not able to process and send, all relay services will be booted up normally, but the GOOSE message will not be sent, since it will have been disabled, the *NDSCom* attribute of the GCB having been set to TRUE. The *System Log* will display a message stating this condition:

ERR - [IEC61850ED1] Goose encoding error, setting GCB invalid (GoEna=False, NdsCom=True)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.11 Subscription to GOOSE Message Data

Subscription to GOOSE message data is carried out through the GIGGIO node.

Using the GIGGIO node, you can subscribe to a total of 400 elements using the *ExtRefs* of that node. The different attributes of GOOSE can be mapped to 200 single signal type data (*GIGGIO1.IndX* data), 100 double signal type data (*GIGGIO1.DPInX* data), 50 integer type data (*GIGGIO1.IntInX* data) and 50 floating type data (*GIGGIO1.AnInX* data). Each subscribed element (value, quality and/or timestamp) will occupy an independent *ExtRef*.

The device can receive GOOSEs containing both data (CDF) and attributes (FCDA), but the subscription has to be made only to final attributes of type boolean (assignable to *GIGGIO1.IndX* data), *DbPos* (assignable to *GIGGIO1.DPInX* data), int (assignable to *GIGGIO1.IntInX* data), float (assignable to *GIGGIO1.AnInX* data), quality and timestamp (assignable to any of the *GIGGIO1* data). For example, if an SPS data travels in the GOOSE, the equipment should subscribe to the *stVal* attribute, the *q* attribute and the *t* attribute (if desired), using three *ExtRefs*.

There is going to be just one GIGGIO *Logical Node* and it will appear always instantiated in the data model.

So, as defined before, the subscription is carried out through the GIGGIO node, where it will be mapped the internal data where the data received through the GOOSE service will be stored. Because of this, at the time of configuring a subscription, the required user resources (digital and/or analogue signals) must be generated. Those user resources will be the ones where mapped in the GIGGIO Logica Node and therefore where the data received through the GOOSE message will be stored.

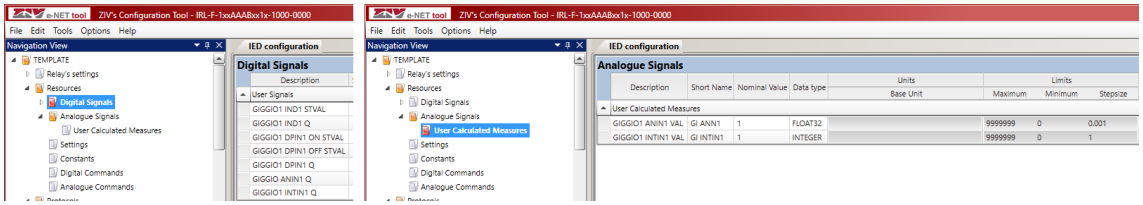


Figure D.4 Generation of User Signals (Digital and Analog) for Receiving the Subscribed Value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

From the tools window, with the ***Referable*** data tab selected, map the user resources registered in advance in the GIGGIO node.

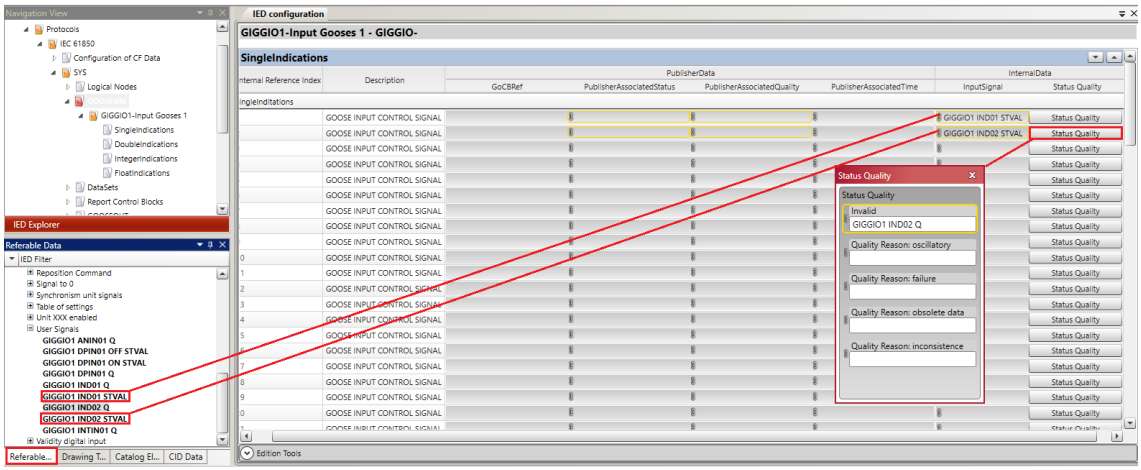


Figure D.5 Mapping for Receiving a Single Point Status Data (SPS) and its *Quality*.

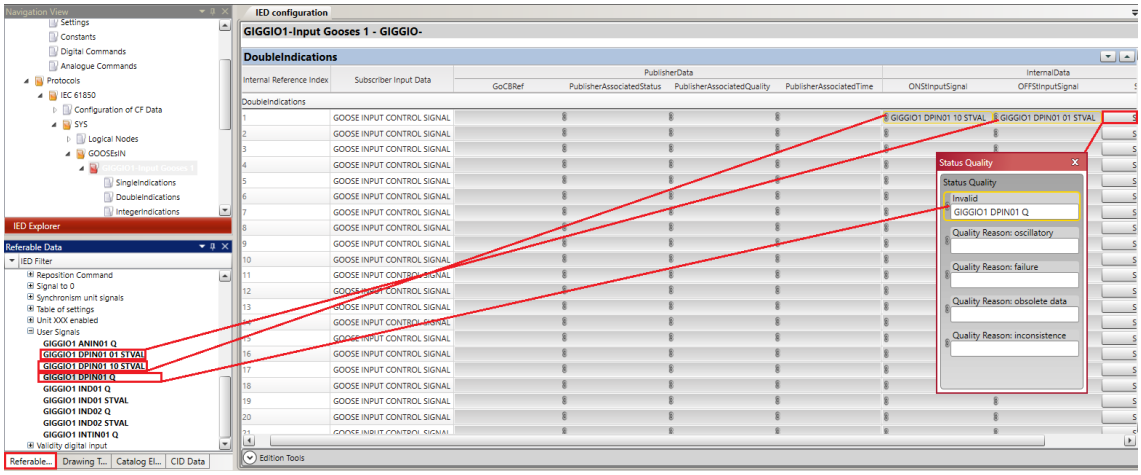


Figure D.6 Mapping for Receiving a Double Point Status Data (DPS) and its *Quality*.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

At the time of subscribing to a double point status data, the relay will receive the DPS data and will represent its value by means of two user signals.

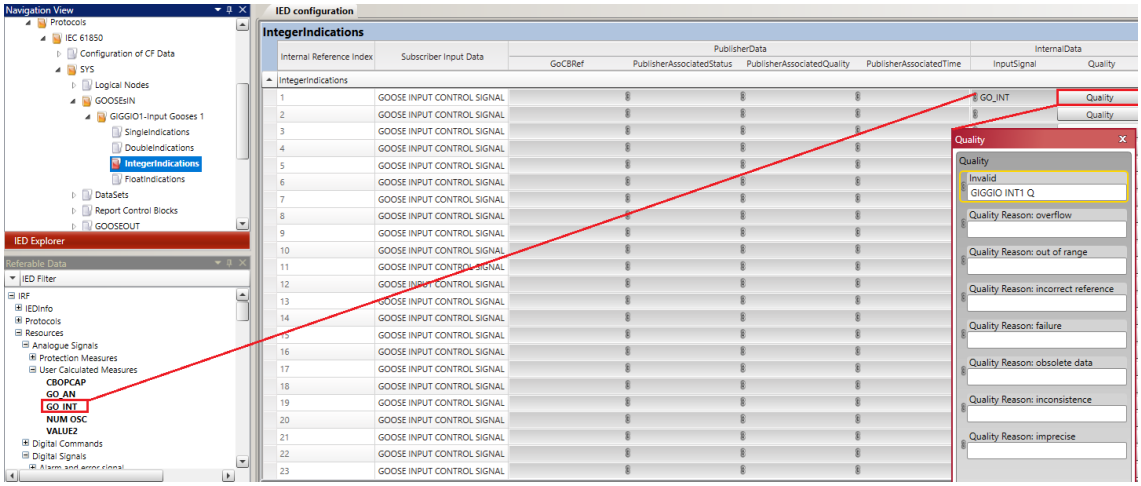


Figure D.7 Mapping for Receiving an Integer Data (INT) and its *Quality*.

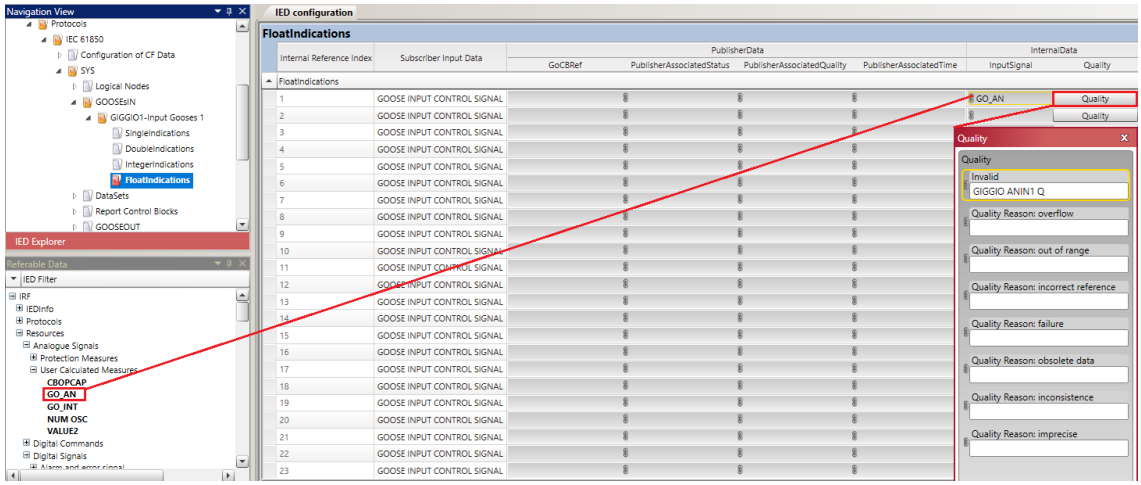


Figure D.8 Mapping for Receiving an Analog Data (FLOAT) and its *Quality*.

In the example, both the data value and its quality, in case both are sent through the GOOSE message, have been mapped to have this quality value in a user signal and be able to act accordingly, but this is not mandatory. When the GOOSE is being received correctly and the *quality* of the subscribed element is valid, the user signal mapped to the GIGGIO node in the ***Validity*** box will have a **TRUE** value. When the *quality* sent through the GOOSE is invalid or the relay is not receiving the GOOSE message, this signal will have a **FALSE** value, being able to use this signal in the relay logic to generate alarms, blockings or whatever is required. On the other hand, more user signals may be mapped if the reasons for a non valid quality must be known.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Once the GIGGIO node has been mapped with all digital signals or measurements to be received through GOOSE message, the subscription can be configured. Right click ***Input GOOSEs*** to display the submenu ***Configure incoming GOOSE***. When selected, the program prompts to select the relay CID configured to send the GOOSE message, CID from which it will retrieve the data related to the configured GCB and Data Set. After selecting the file, in the ***Tools*** window, with the ***CID Data*** tab selected, the configured GCBs of the open CID will be shown.

To carry out the subscription of a single element (attributes type *boolean*, *quality* and / or *timestamp*), select single point data from the CID Data window and drag to the ***Publisher Associated Status*** field of the simple elements of the GIGGIO. When selecting the Data Attribute, if inside the Data Set its corresponding quality or timestamp is located, their subscription will also be done automatically. When making the subscription of a quality or timestamp just that subscription will be done.

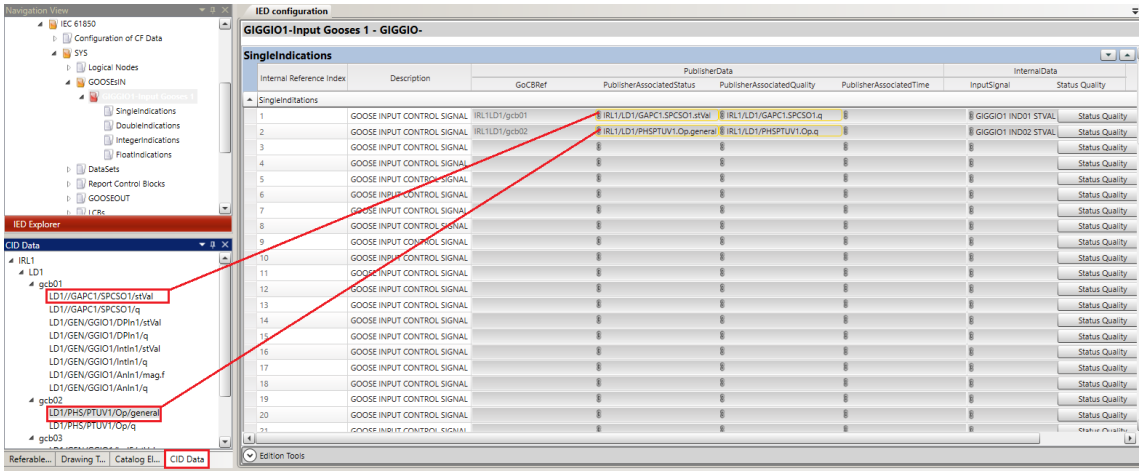


Figure D.9 Subscription to a Single Point Data.

In the example, the quality subscription of both elements has been done automatically by the configuration tool.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To carry out the subscription of a double element (attributes type *DbPos*, *quality* and / or *timestamp*), select double point data from the ***CID Data*** window and drag to the ***Publisher Associated Status*** of the double elements of the GIGGIO.

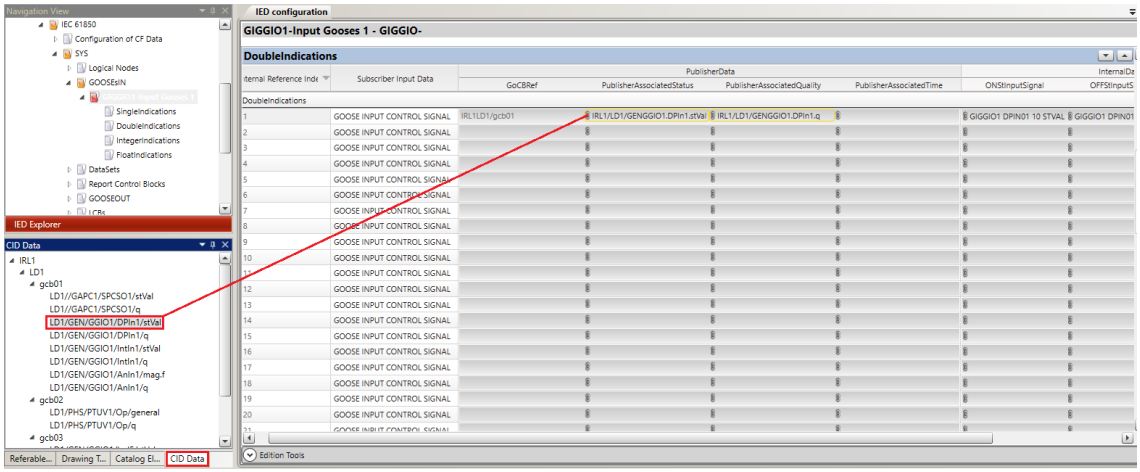


Figure D.10 Subscription to a Double Point Data.

To carry out the subscription of an integer element (attributes type *int, quality* and / or *timestamp*), select integer data from the ***CID Data*** window and drag to the ***Publisher Associated Status*** of the integer elements of the GIGGIO.

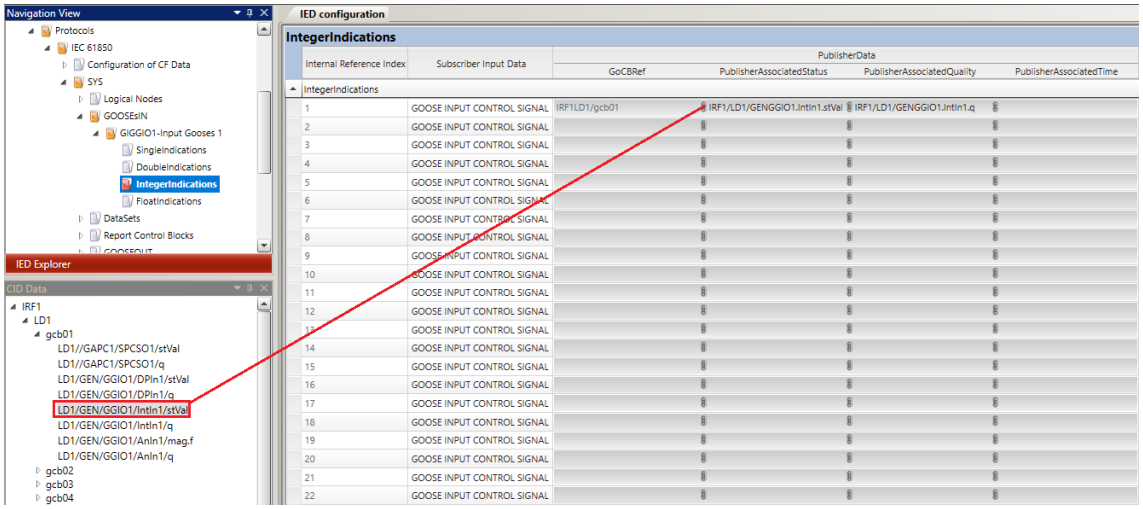


Figure D.11 Subscription to an Integer Data.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To carry out the subscription of an analog element (attributes type *int, quality* and / or *timestamp*), select floating data from the ***CID Data*** window and drag to the ***Publisher Associated Status*** of the floating elements of the GIGGIO.

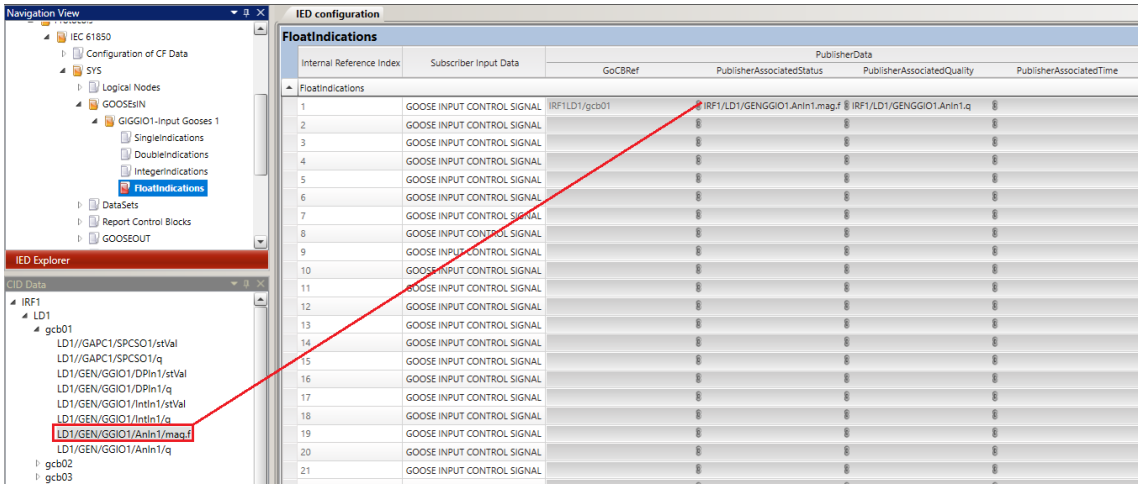


Figure D.12 Subscription to an Analogue Data.

If you try to subscribe to a wrong data type (for example, an integer data in a FLOAT), the tool displays the following message: ***Invalid Type!***, and does not allow subscription.

When configuring a subscription, the corresponding ExtRef with the information to be received will be automatically registered in the GIGGIO node and in the Communication field of the IED and in the *DataTypeTemplates* all the information of the IED who is sending that data in a GOOSE message so that the subscriptor IED can perform the subscription.

Once the relay is configured with the appropriate subscriptions to GOOSE messages, access to the status of each subscription can be gained from the web server.

Next, an example of subscription to a data (data object or FCD). As mentioned, subscriptions to attributes must always be made. The tool automatically displays the attributes of the FCD in the ***CID Data*** window and the user will individually configure the attributes as indicated above.

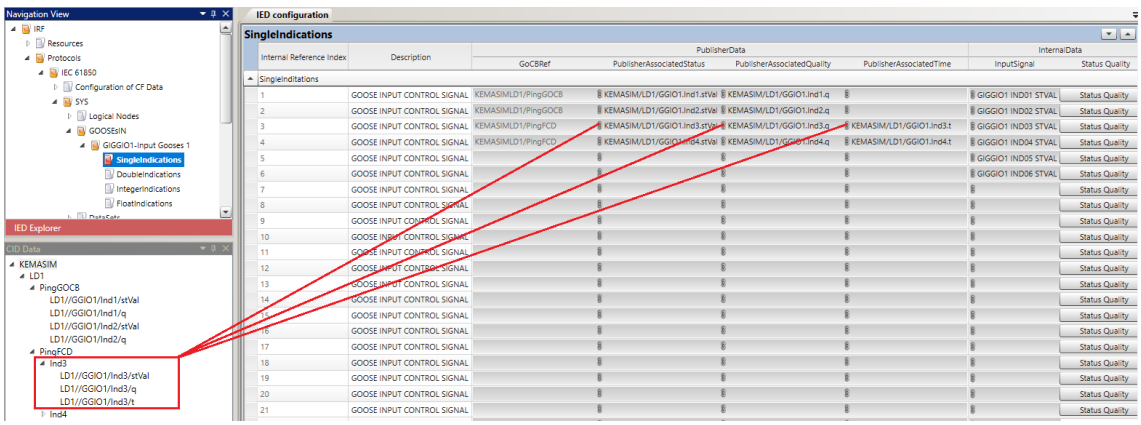


Figure D.13 Suscription to a Data Object.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The Mod status of the IED (LD SYS.LLN0.Mod) will define the way the IED will process the GOOSE subscription elements.

GOOSE input value	on	blocked	test	test-blocked	off
value=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=good *detailQual*=0 *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=quest *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
GOOSE is no longer being received	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=false	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=false	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=true	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=true	*value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false

where:

(*) OD = OldData.
“Processed as valid” means that the application should react according to the quality and intended functionality of the LN.
“**Processed as invalid**” means the application should react as if the quality of the data had been invalid or as the data source has failed.
“**Processed as questionable**” means that the application should decide how to consider the status value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.12 Report Control Blocks (RCBs)

This method is used in the standard for an effective vertical communication between the IED (server) and the clients (central units, gateways, SCADAs, etc.). The IEDs have 20 RCBs, 10 of them being Buffered RCBs and the other 10, Unbuffered RCBs. All 20 are always present in the data model and, the following parameters can be edited by configuration:

- BRCB:
  - Configuration revision.
  - Buffer time. Buffer size is 30 kbytes.
  - Description.
  - Data Set associated with BRCB.
  - rptID.
  - Integrity Period.
  - Trigger Options (Data Update is not supported by the relay).
  - Optional fields.
- URCB:
  - Configuration revision.
  - Description.
  - Data Set associated with URCB.
  - rptID.
  - Integrity Period.
  - Trigger Options (Data Update is not supported by the relay).
  - Optional fields.

The same Data Set may be allocated to different RCBs in order to be able to send the same data to different clients (for example, central units or redundant SCADAs).

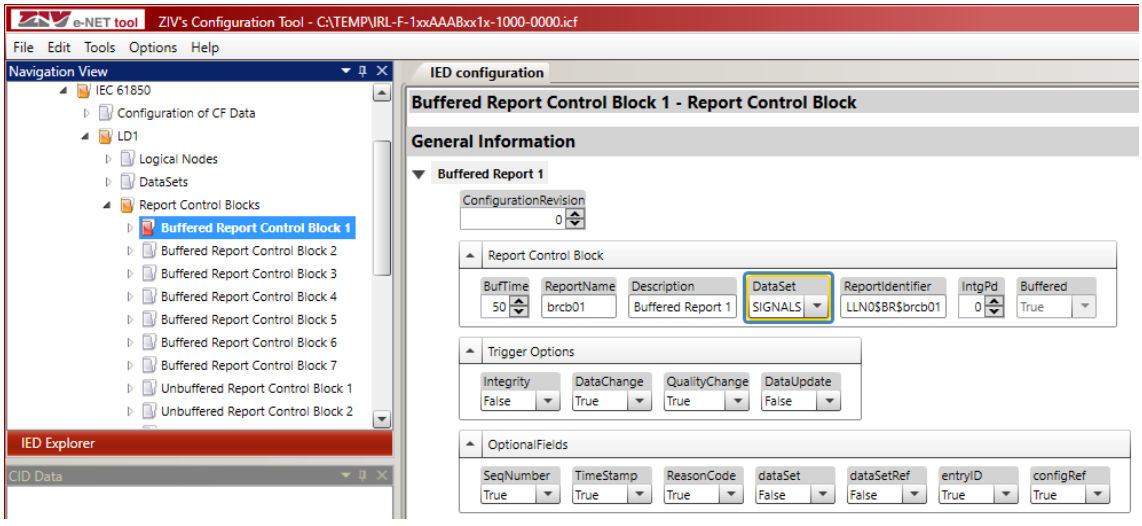


Figure D.14 Configuration of a BRCB.

The moment a client enables a RCB after having connected and associated with the relay, this RCB is then no longer available for other clients. Although all the configuration parameters are available in the tool, the client (once connected and prior to enabling the RCB) can edit the same according to its needs, except for the Data Set and ***Configuration Revision*** (***SqNum***, ***GI*** and ***TimeofEntry*** *cannot be edited either*).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The IED supports the following ***Trigger Options***, apart from ***General Interrogation***:

- ***Integrity***: the relay will send periodically a *Report* with all the information of the Data Set, according to ***Integrity Period*** setting configuration.
- ***Data Change***: the relay will send a *Report* when a change in a the value of any Data Set element is detected and only this changed data will be sent.
- ***Quality Change***: the relay will send a *Report* when a change in Data Set element quality is detected and only this changed data will be sent.

The IED allows preconfiguring RCBs to specific clients so that those RCBs can just be configured and enabled by the preconfigured clients. In order to carry out that configuration it is necessary having the ICD/IID/CID/SCD file where the information of the client appears. Clicking with the right button of the mouse over the ***Report Control Blocks*** it appears a menu (***Open SCL file***) from where you can select the SCL file of the client. The tool will extract from that file the necessary information to preconfigure the desired RCB (LN and AccessPoint of the corresponding IED). Once selected the SCL file, it will appear in the ***Tools*** window, when being selected ***CID Data***, the information of the SCL file which will be used to configure the ***ClientLN*** and ***ClientAP*** fields of the desired RCB.

It is necessary that the SCL file of the client contains the Clientservices of the bufReport and/or unbufReport enabled (true) into the *Services* section so that the tool can preconfigure the RCBs.

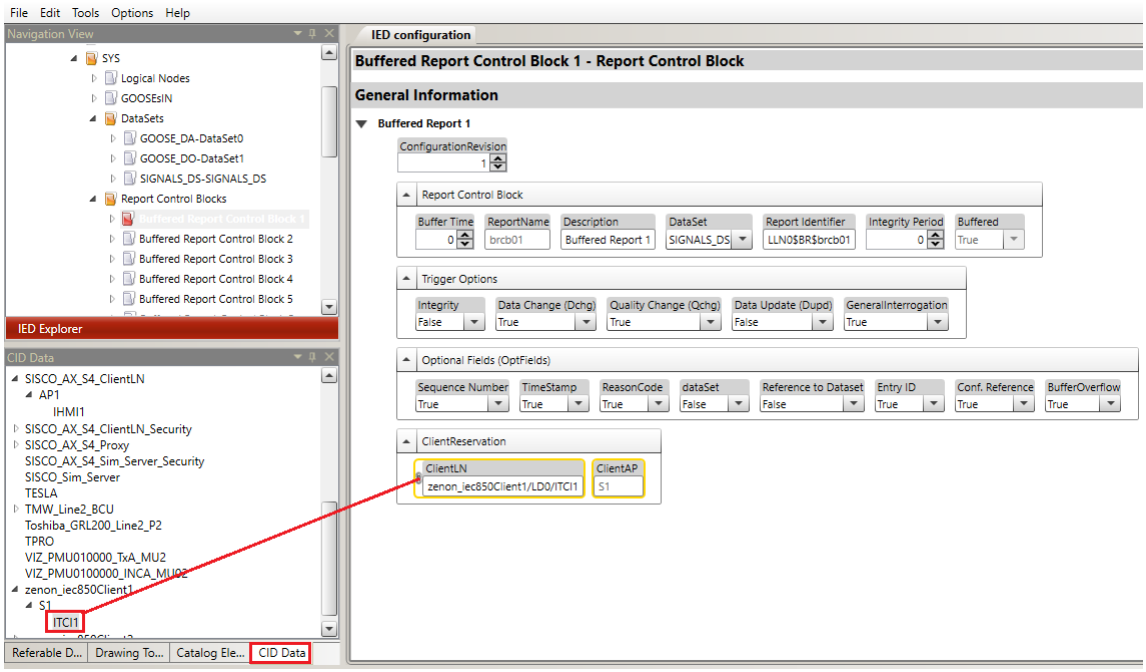


Figure D.15 Preconfiguration of a RCB.

In the hypothetical case in which a ***ClientLN*** has been configured without a ***ClientAp*** and the client IED has several *AccessPoints* with the same server (*ServerAt*), this is, when the tool can not determine the *AccessPoint* of the Logical Node selected of the client, the preconfiguration of the RCB will be refused. In this case, the ***ClientLN*** will be ignored and an error notification will be displayed.

When performing a preconfiguration of a RCB, the tool will automatically add to the CID the information of the client IED (Communications field, DataTypeTemplates, etc.).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.13 Measurement Configuration (Data CF)

When the automatic measurement range calculation setting is enabled (AutoRanMag data located in the logic node LPHD), the relay will carry out the automatic calculation of the 6 elements of the measurements *rangeC*. In this case, these elements will be *read only* type. The automatic calculation will be as follows:

- max: will be calculated as a function of the measurement, its nominal and corresponding transformation ratios.
- hhLim = min + ((max-min) * 80 / 100)
- hLim = min + ((max-min) * 60 / 100)
- lLim = min + ((max-min) * 40 / 100)
- llLim = min + ((max-min) * 20 / 100)
- min: will be calculated as a function of the measurement, its nominal and corresponding transformation ratios.

When the setting is disabled, the user can configure these *rangeC* elements as deemed appropriate, either from the configuration tool or through MMS, although the following checks will be carried out:

- rangeC.max > rangeC.min
- max>=hhLim>=hLim>=lLim>=llLim>=min

Any change in the *rangeC* values will be updated in the CID file.

On the other hand, each measurement has its *deadband* (***db*** attribute). *Deadband* represents the difference percentage between maximum and minimum values of a measurement in 1 per thousand (0.001). This setting is present in the data model since the measurements consist of two data: "**instMag/instCVal**" representing the instantaneous and continuous measurement value and "**mag/cVal**". This "**mag/cVal**" data is updated when the instantaneous measurement value is subject to a certain change, defined in the ***db*** setting and it is this "**mag/cVal**" data that is subject to the Reports and LOGS (*data change*) assessment function, namely, the data that is sent through communications in Reports and is stored in the LOG files.

Regarding GOOSE messages, both the instantaneous and the *deadband* data generate change and, thereby, the GOOSE message change *trigger*, so that instantaneous data selection in the Data Set associated with GOOSE messages is not recommended. Below is a graph with the relation between instantaneous and deadband data.

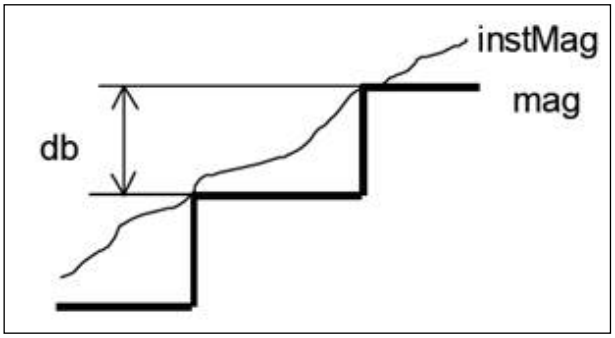


Figure D.16 Relation between Instantaneous and *Deadband* Measurement.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

As an example, below is shown the influence of the ***db*** data in the generation of changes of the measurement to be reported.

RangeC setting values max=30326402.0 and min=-30326402.
max-min= 60652804 W

db = 1000
1% del max-min => 606,5 kW
When the measurement varies 606.5 kW, a change is detected and the report is sent. In the graph above, the steps would be 606.5 kW.

db=10
0,01% del max-min => 6,065 kW
When the measurement varies 6.065, a change is detected and the report is sent. In the graph above, the steps would be 6.065 KW.

db=1
0,001% del max-min => 606,5 W
When the measurement varies 606.5, a change is detected and the report is sent. In the graph above, the steps would be 606.5 W.

D.14 Commands

Relays support SBO and direct commands, with or without enhanced safety as a function of the ***ctlModel*** setting value present in every relay commanding data:

- ***ctlModel*** = 0: non commanding data.
- ***ctlModel*** = 1: direct command with normal safety, which can be run after writing the applicable *Oper* attribute.
- ***ctlModel*** = 2: SBO command with normal safety. Before running it, first select the data by reading the *SBO* attribute. The IED will return the *path* of the selected data as indication of a good operation and “null” in case of error. Once selected, the data can be run after writing the corresponding Oper before the time ***sboTimeout*** times out, after which time the element is not longer selected.
- ***ctlModel*** = 3: direct command with enhanced safety that can be run after writing the corresponding *Oper* attribute. The IED will send information on how the command has been run: execution of the command rejected, failed termination or successful termination, indicating the cause of the failure in the first two situations
- ***ctlModel*** = 4: SBO command with enhanced safety. In order to run it, first select the data by writing the *SBOw* attribute. Once selected, the data can be run after writing the corresponding Oper with the same SBOw write parameters before the time ***sboTimeout*** times out, after which time the element is not longer selected. The IED will send information on how the command has been run: selection of the command rejected, execution of the command rejected, failed termination or successful termination, indicating the cause of the failure in the first three situations.

The device supports the *interlock-check* for any configurable command, so that, depending on the value of the mentioned *Check* attribute, the device will apply the information of the associated CILO Logical Node to the command to block it or to skip such blocking.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

D.15 SNTP Synchronization

The IED is able to synchronize through the communications network by SNTP protocol (*Simple Network Time Protocol*), as indicated by IEC 61850. The SNTP client of the equipment can be configured in *broadcast* or *unicast* mode: with one or two servers:

- *Broadcast*: the relay will wait to receive *broadcast* messages sent by the GPS clock for synchronizing.
- *Unicast*: the relay will send a date and time request to the GPS clock and will be synchronized with the message received.

The settings are detailed in the Physical Description section of the Description and Start-Up chapter.

D.15.1 SNTP Synchronism Status Calculation

The SNTP module recalculates its status every time any client (*unicast* or *broadcast*) calculates its own, which occurs with a change in its status (online/offline) due to timing, at the end of each interrogation cycle with response (correct structure) on the part of a server (*unicast client*) or with each received *broadcast* message (*broadcast* client).

The calculation method varies as a function of the ***Synchronism status calculation*** setting value:

- If the setting has been configured as ***Leap indicator***, the SNTP module status will be the latest status calculated by any of the *unicast* and *broadcast* clients.
- If the setting has been configured as ***Timing***, the SNTP module status will be a combined status of both *unicast* and *broadcast* clients, following two possible algorithms:
  - If ***broadcast error timing*** is set to 0, the SNTP module status is only a function of the *unicast* client status, except when the *broadcast* client switches from offline to online, at which time the SNTP module switches to the online status until a new *unicast* client status calculation.
  - If ***broadcast error timing*** is set to a value other than 0, the SNTP module status is a combination of the *unicast* and *broadcast* client statuses. In this mode, the SNTP module status will be:
    Synchronized if any client is in synchronized status.
    Non Synchronized if no client is synchronized and any client is not synchronized.
    Non calculated if all the clients are in non-calculated status.

D.15.1.a *Unicast* Client

A disabled *unicast* client does not make synchronization requests to servers. Therefore, when the IED client is enabled, it will interrogate the servers that have a configured IP address other than 0.0.0.0, which is the server identifier to be ignored.

Synchronization Period and ***Interval Between Retries*** settings define the time request interval to the servers when the client is in synchronized status and non-synchronized status respectively. The ***Number of Retries*** setting defines the maximum number of retries on a server if a valid response is not received. A 0 value indicates that retries will not be made, namely, only one connection attempt will be made. The ***SNTP Time Between Retries*** setting indicates the maximum waiting time between retries.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

As a function of these settings, the relay will send the appropriate messages and will wait for the answer on the part of the SNTP server. If ***Ignore leap indicator*** is set to **NO**, the received message will be process in terms of *leap indicator* field (less than 3), *stratum* field (from 0 to 16) and time difference between server and client (less than the ***Maximum Synchronization Time Difference*** *setting* except that the setting is 0), so that these received values must be within ranges in order to accept the synchronization, but when the ***Ignore leap indicator*** setting is set to **YES**, the message will be directly accepted. If the message is not accepted, the IED will interrogate the second server. The relay, in this way, will successively interrogate the servers until receiving a valid response from one of them. If, after going through all the servers, a correct response is not received, **non-synchronized** status will be shown. The relay will listen to NTP messages sent to its own IP address.

If the synchronized status calculation is set to timing, the ***Unicast Validity Timing*** setting specifies the time lapse from the first valid message received without receiving error messages or timeouts, so that the client switches to a synchronized Status. When the setting sets to 0, the waiting time is 0 seconds, so that the unicast client will switch to synchronized Status when the first correct message is received.

Unicast Error Timing enables selecting the time lapse from the last valid message received, so that the unicast client switches to non-synchronized Status. The timing also starts at the time when the client reaches the synchronized Status, since it could remain in this status without receiving any valid message.

D.15.1.b *Broadcast* Client

The *broadcast* client receives NTP synchronization *broadcast* messages, sets the time in accordance with the same, and calculates synchronism status at all times. When disabled, the IED will ignore the received synchronization messages. The synchronized status will be produced the moment a correct message is received, provided the time set in ***Broadcast Validity Timing,*** elapsed from the first correct message received, has run out, switching to non-synchronized when no valid messages are received within the time configured in ***Broadcast Error Timing***. The *broadcast* client will permanently be awaiting to receive NTP *broadcast* synchronization messages, listening to messages received with destination IP address 255.255.255.255 or *broadcast* address corresponding to the subnetwork that it belongs to. Listening to messages sent to its IP address in particular is also deemed correct.

Force unicast setting establishes whether a new *unicast* refresh must be sent at the time of receiving a *broadcast* message. The *unicast* client, when receiving the synchronization request, will cancel the refresh in progress if applicable and will immediately start a new refresh process with the servers.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Protocol Implementation Conformance Statement for the IEC 61850 interface in RTF/DLF from ZIV Aplicaciones y Tecnología

10/04/2019, V. 0.0

UCA International Users Group
Testing Sub Committee

PICS template extracted from Server Test Procedures for Edition 2 TPCL 1.2.6

PICS Template for Server Ed1/Ed2

General

The following ACSI conformance statements are used to provide an overview and details about RTF/DLF, with firmware version 0.9.1:

- ACSI basic conformance statement,
- ACSI models conformance statement,
- ACSI service conformance statement

The statements specify the communication features mapped to IEC 61850-8-1 and IEC 61850-9-2.

ACSI basic conformance statement

The basic conformance statement is defined in Table A.1.

Table A.1 – Basic conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments
Client-Server roles				
B11	**Server** side (of TWO-PARTY-APPLICATION-ASSOCIATION)	—	Y	
B12	**Client** side of (TWO-PARTY-APPLICATION-ASSOCIATION)	N	—	
SCSMs supported				
B21	**SCSM**: IEC 61850-8-1 used	N	Y	
B22	**SCSM:** IEC 61850-9-1 used			Deprecated Ed2
B23	**SCSM**: IEC 61850-9-2 used			
B24	**SCSM**: other			
Generic substation event model (GSE)				
B31	**Publisher** side	—	Y	
B32	**Subscriber** side	Y	—	
Transmission of sampled value model (SVC)				
B41	**Publisher** side	—	N	
B42	**Subscriber** side	N	—	

– = not applicable
Y = supported
N or empty = not supported

ACSI models conformance statement

The ACSI models conformance statement is defined in Table A.2.

Table A.2 – ACSI models conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments
If **Server** side (B11) and/or **Client** side (B12) supported				
M1	**Logical device**	N	Y	
M2	**Logical node**	N	Y	
M3	**Data**	N	Y	
M4	**Data set**	N	Y	
M5	**Substitution**	N	N	
M6	**Setting group control**	N	Y	
	Reporting			
M7	**Buffered report control**	N	Y	
M7-1	sequence-number	N	Y	
M7-2	report-time-stamp	N	Y	
M7-3	reason-for-inclusion	N	Y	
M7-4	data-set-name	N	Y	
M7-5	data-reference	N	Y	
M7-6	buffer-overflow	N	Y	
M7-7	entryID	N	Y	
M7-8	BufTm	N	Y	
M7-9	IntgPd	N	Y	
M7-10	GI	N	Y	
M7-11	conf-revision	N	Y	
M8	**Unbuffered report control**	N	Y	
M8-1	sequence-number	N	Y	
M8-2	report-time-stamp	N	Y	
M8-3	reason-for-inclusion	N	Y	
M8-4	data-set-name	N	Y	
M8-5	data-reference	N	Y	
M8-6	BufTm	N	Y	
M8-7	IntgPd	N	Y	
M8-8	GI	N	Y	
M8-9	conf-revision	N	Y	
	Logging	N	N	
M9	**Log control**	N	N	
M9-1	IntgPd	N	N	
M10	**Log**	N	N	
M11	**Control**	N	Y	
M17	**File Transfer**	N	Y	
M18	**Application association**	N	Y	
M19	**GOOSE Control Block**	N	Y	
M20	**Sampled Value Control Block**	N	N	

		Client/ Subscriber	Server/ Publisher	Value/ Comments
If **GSE** (B31/32) is supported				
M12	**GOOSE**	N	Y	
M13	**GSSE**			Deprecated Ed2
If **SVC** (B41/42) is supported				
M14	Multicast SVC	N	N	
M15	Unicast SVC	N	N	
For all IEDs				
M16	**Time**	N	Y	Time source with required accuracy shall be available. Only Time Master are SNTP (Mode 4 response) time server. All other Client / Server devices require SNTP (Mode 3 request) clients
Y = service is supported N or empty = service is not supported				

ACSI service conformance statement

The ACSI service conformance statement is defined in Table A.4 (depending on the statements in Table A.1 and in Table A.3).

Table A.4 – ACSI service Conformance statement

	Ed.	Services	AA: TP/MC	Client ©	Server (S)	Comments
Server						
S1	1,2	GetServerDirectory (LOGICAL-DEVICE)	TP	N	Y	
Application association						
S2	1,2	Associate		N	Y	
S3	1,2	Abort		N	Y	
S4	1,2	Release		N	Y	
Logical device						
S5	1,2	GetLogicalDeviceDirectory	TP	N	Y	
Logical node						
S6	1,2	GetLogicalNodeDirectory	TP	N	Y	
S7	1,2	GetAllDataValues	TP	N	Y	
Data						
S8	1,2	GetDataValues	TP	N	Y	
S9	1,2	SetDataValues	TP	N	Y	
S10	1,2	GetDataDirectory	TP	N	Y	
S11	1,2	GetDataDefinition	TP	N	Y	
Data set						
S12	1,2	GetDataSetValues	TP	N	Y	
S13	1,2	SetDataSetValues	TP	N	N	
S14	1,2	CreateDataSet	TP	N	N	
S15	1,2	DeleteDataSet	TP	N	N	
S16	1,2	GetDataSetDirectory	TP	N	Y	
Substitution						
S17	1	SetDataValues	TP	N	N	
Setting group control						
S18	1,2	SelectActiveSG	TP	N	Y	
S19	1,2	SelectEditSG	TP	N	Y	
S20	1,2	SetEditSGValues	TP	N	Y	
S21	1,2	ConfirmEditSGValues	TP	N	Y	
S22	1,2	GetEditSGValues	TP	N	Y	
S23	1,2	GetSGCBValues	TP	N	Y	

	Ed.	Services	AA: TP/MC	Client ©	Server (S)	Comments
Reporting						
Buffered report control block (BRCB)						
S24	1,2	Report	TP	N	Y	
S24-1	1,2	data-change (dchg)		N	Y	
S24-2	1,2	quality-change (qchg)		N	Y	
S24-3	1,2	data-update (dupd)		N	N	
S25	1,2	GetBRCBValues	TP	N	Y	
S26	1,2	SetBRCBValues	TP	N	Y	
Unbuffered report control block (URCB)						
S27	1,2	Report	TP	N	Y	
S27-1	1,2	data-change (dchg)		N	Y	
S27-2	1,2	quality-change (qchg)		N	Y	
S27-3	1,2	data-update (dupd)		N	N	
S28	1,2	GetURCBValues	TP	N	Y	
S29	1,2	SetURCBValues	TP	N	Y	

Logging						
Log control block						
S30	1,2	GetLCBValues	TP	N	N	
S31	1,2	SetLCBValues	TP	N	N	
Log						
S32	1,2	QueryLogByTime	TP	N	N	
S33	1,2	QueryLogAfter	TP	N	N	
S34	1,2	GetLogStatusValues	TP	N	N	

Generic substation event model (GSE)						
GOOSE						
S35	1,2	SendGOOSEMessage	MC	N	Y	
GOOSE-CONTROL-BLOCK						
S36	1,2	GetGoReference	TP	N	Y	
S37	1,2	GetGOOSEElementNumber	TP	N	Y	
S38	1,2	GetGoCBValues	TP	N	Y	
S39	1,2	SetGoCBValues	TP	N	Y	
GSSE						
S40	1	SendGSSEMessage	MC			Deprecated in Edition 2
GSSE-CONTROL-BLOCK						
S41	1	GetReference	TP			Deprecated in Edition 2
S42	1	GetGSSEElementNumber	TP			Deprecated in Edition 2
S43	1	GetGsCBValues	TP			Deprecated in Edition 2
S44	1	SetGsCBValues	TP			Deprecated in Edition 2

	Ed.	Services	AA: TP/MC	Client ©	Server (S)	Comments
Transmission of sampled value model (SVC)						
Multicast SV						
S45	1,2	SendMSVMessage	MC	N	N	
Multicast Sampled Value Control Block						
S46	1,2	GetMSVCBValues	TP	N	N	
S47	1,2	SetMSVCBValues	TP	N	N	
Unicast SV						
S48	1,2	SendUSVMessage	TP	N	N	
Unicast Sampled Value Control Block						
S49	1,2	GetUSVCBValues	TP	N	N	
S50	1,2	SetUSVCBValues	TP	N	N	

Control						
S51	1,2	Select		N	Y	
S52	1,2	SelectWithValue	TP	N	Y	
S53	1,2	Cancel	TP	N	Y	
S54	1,2	Operate	TP	N	Y	
S55	1,2	CommandTermination	TP	N	Y	
S56	1,2	TimeActivatedOperate	TP	N	N	

File transfer						
S57	1,2	GetFile	TP	N	Y	
S58	1,2	SetFile	TP	N	Y	
S59	1,2	DeleteFile	TP	N	N	
S60	1,2	GetFileAttributeValues	TP	N	Y	
S61	1,2	GetServerDirectory (FILE-SYSTEM)	TP	N	Y	

Time						
T1	1,2	Time resolution of internal clock		xx	10 (1ms)	Nearest negative power of 2^{-n} in seconds (number 0 .. 24)
T2	1,2	Time accuracy of internal clock		Tx	T1	TL (ms) (low accuracy), T3 < 7) (only Ed2) T0 (ms) (<= 10 ms), 7 <= T3 < 10 T1 (µs) (<= 1 ms), 10 <= T3 < 13 T2 (µs) (<= 100 µS), 13 <= T3 < 15 T3 (µs) (<= 25 µS), 15 <= T3 < 18 T4 (µs) (<= 25 µS), 15 <= T3 < 18 T5 (µs) (<= 1 µS), T3 >= 20
T3	1,2	Supported TimeStamp resolution	-	xx	10	Nearest value of 2^{-n} in seconds (number 0 .. 24)

Protocol Implementation eXtra Information for Testing (PIXIT)
for the IEC 61850 interface in RTF/DLF
from ZIV Aplicaciones y Tecnología

10/04/2019, Version 0.1

UCA International Users Group
Testing Sub Committee

PIXIT template extracted from Server Test Procedures for Edition 2 TPCL 1.2.6

PIXIT Template for Server Ed1/Ed2

Introduction

This document specifies the protocol implementation extra information for testing (PIXIT) of the IEC 61850 interface in RTF/DLFF with firmware version 0.9.1.

Together with the PICS and the MICS the PIXIT forms the basis for a conformance test according to IEC 61850-10. The PIXIT entries contain information which is not available in the PICS, MICS, TICS documents or SCL file.

Each table specifies the PIXIT for applicable ACSI service model as structured in IEC 61850-10. The “Ed” column indicates if the entry is applicable for IEC 61850 Edition 1 and/or Edition 2.

PIXIT for Association model

ID	Ed	Description	Value / Clarification
As1	1	Maximum number of clients that can set-up an association simultaneously	10
As2	1,2	TCP_KEEPALIVE value. The recommended range is 1..20s	20 seconds
As3	1,2	Lost connection detection time	120 seconds (5 times KEEPALIVE)
As4	-	Authentication is not supported yet	
As5	1,2	What association parameters are necessary for successful association	Transport selector N Session selector N Presentation selector N AP Title N AE Qualifier N
As6	1,2	If association parameters are necessary for association, describe the correct values e.g.	Association parameters are not necessary for association
As7	1,2	What is the maximum and minimum MMS PDU size	Max MMS PDU size 65000 Min MMS PDU size Is determined by the size of the request.
As8	1,2	What is the maximum start up time after a power supply interrupt	35 seconds in normal situation (when no control configuration needs to be loaded)
As9	1,2	Does this device function only as test equipment? (test equipment need not have a non-volatile configuration; but it cannot be part of the substation automation system)	No. It has non-volatile configuration.
		<additional items>	

PIXIT for Server model

ID	Ed	Description	Value / Clarification
Sr1	1,2	Which analogue value (MX) quality bits are supported (can be set by server)	Validity: Y Good, Y Invalid, N Reserved, Y Questionable N Overflow Y OutofRange N BadReference N Oscillatory N Failure Y OldData N Inconsistent N Inaccurate Source : Y Process N Substituted Y Test N OperatorBlocked
Sr2	1,2	Which status value (ST) quality bits are supported (can be set by server)	Validity: Y Good, Y Invalid, N Reserved, Y Questionable N BadReference Y Oscillatory Y Failure Y OldData N Inconsistent N Inaccurate Source : Y Process N Substituted Y Test N OperatorBlocked
Sr3	-	What is the maximum number of data object references in one GetDataValues request	Deprecated
Sr4	-	What is the maximum number of data object references in one SetDataValues request	Deprecated

ID	Ed	Description	Value / Clarification
Sr5	1	Which Mode values are supported [1]	On Y [On-]Blocked Y Test Y Test/Blocked Y Off Y The supported Mode values are indicated by using different enumeration types for each case.
		<additional items>	

PIXIT for Data set model

ID	Ed	Description	Value / Clarification
Ds1	1	What is the maximum number of data elements in one data set (compare ICD setting)	Fixed in ICD to 500
Ds2	1	How many persistent data sets can be created by one or more clients (this number includes predefined datasets)	0
Ds3	1	How many non-persistent data sets can be created by one or more clients	0
		<additional items>	

PIXIT for Setting group control model

ID	Ed	Description	Value / Clarification
Sg1	1	What is the number of supported setting groups for each logical device	8
Sg2	1,2	What is the effect of when and how the non-volatile storage is updated (compare IEC 61850-8-1 $16.2.4)	If values are updated in a CID, these changes take effect after starting up. If values are updated by MMS services, these changes take effect immediately
Sg3	1	Can multiple clients edit the same setting group	N
Sg4	1	What happens if the association is lost while editing a setting group	The EditSG is reset to 0
Sg5	1	Is EditSG value 0 allowed	Y
Sg6	2	When ResvTms is not present how long is an edit setting group locked	ResvTms is present. Its default value is 3600 seconds
		<additional items>	

[1] IEC 61850-6:2009 clause 9.5.6 states that if only a subrange of the enumeration value set is supported, this shall be indicated within an ICD file by an enumeration type, where the unsupported values are missing

PIXIT for Reporting model

ID	Ed	Description	Value / Clarification
Rp1	1	The supported trigger conditions are (compare PICS)	integrity Y data change Y quality change Y data update N general interrogation Y
Rp2	1	The supported optional fields are	sequence-number Y report-time-stamp Y reason-for-inclusion Y data-set-name Y data-reference Y buffer-overflow Y entryID Y conf-rev Y segmentation Y
Rp3	1,2	Can the server send segmented reports (when not supported, it is allowed to refuse an association with a PDU smaller than the supported minimum PDU size)	Y
Rp4	1,2	Mechanism on second internal data change notification of the same analogue data value within buffer period (Compare IEC 61850-7-2 $14.2.2.9)	The DUT behaves as if BufTm has expired and sends the report immediately, restarts the timer with BufTm value and processes the second change
Rp5	1	Multi client URCB approach (compare IEC 61850-7-2:2003 $14.2.1)	Each URCB is visible to all clients
Rp6	-	What is the format of EntryID	Deprecated
Rp7	1,2	What is the buffer size for each BRCB or how many reports can be buffered	30 Kbytes
Rp8	-	Pre-configured RCB attributes that are dynamic, compare SCL report settings	Deprecated
Rp9	1	May the reported data set contain: - structured data objects - data attributes	 Y Y
Rp10	1,2	What is the scan cycle for binary events Is this fixed, configurable	2 ms Fixed
Rp11	1	Does the device support to pre-assign a RCB to a specific client in the SCL	Y

ID	Ed	Description	Value / Clarification
Rp12	2	After restart of the server is the value of ConfRev restored from the original configuration or retained prior to restart	Restored from original CID configuration
Rp13	1,2	Does the server accepts any client to configure/enable a BRCB with ResvTms=-1? What fields are used to do the identification?	N Client's IP Address
Rp14	2	When BRCB.ResvTms is exposed, what is default value for BRCB.ResvTms if client does not write (must be > 0) or When BRCB.ResvTms is not exposed, what is the internal reservation time (must be >= 0)	10 seconds N/A
Rp15	1,2	Each RCB should be configured with a different Data Set. In case of configuring the same Data Set in different RCBs those RCBs must be configured with the same trigger options and integrity period.	
		<additional items>	

PIXIT for Logging model

ID	Ed	Description	Value / Clarification
Lg1	1,2	What is the default value of LogEna (Compare IEC 61850-8-1 $17.3.3.2.1, the default value should be FALSE)	FALSE
Lg2	-	What is the format of EntryID	Deprecated
Lg3	1,2	Are there are multiple Log Control Blocks that specify the Journaling of the same MMS NamedVariable and TrgOps and the Event Condition (Compare IEC 61850-8-1 $17.3.3.3.2)	Single Journal Entry
Lg4	1	Pre-configured LCB attributes that cannot be changed online	LogRef and DatSet (DatSet is configurable by the IED tool)
		<additional items>	

PIXIT for GOOSE publish model

ID	Ed	Description	Value / Clarification
Gp1	1,2	Can the test (Ed1) / simulation (Ed2) flag in the published GOOSE be set	Y
Gp2	1	What is the behaviour when the GOOSE publish configuration is incorrect	If goose pdu is too large NdsCom=True and DUT keeps GoEna=False If no DatSet is configured NdsCom=True and DUT keeps GoEna=False CIDs with incorrect goose publish configuration are rejected
Gp3	1,2	Published FCD supported common data classes are	Any FCD with FC=ST/MX/SP Arrays are not supported
Gp4	1,2	What is the slow retransmission time Is it fixed or configurable	Max value: 2.147.483.647 ms Configured by GoCB MaxTime Default value: 2000 ms
Gp5	1,2	What is the fastest retransmission time Is it fixed or configurable	Min value: 2ms Configured by GoCB MinTime Default value: 2ms
Gp6	-	Can the GOOSE publish be turned on / off by using SetGoCBValues(GoEna)	Deprecated See PICS - SetGoCBValues
Gp7	1,2	What is the initial GOOSE sqNum after restart	1
Gp8	1	May the GOOSE data set contain: - structured data objects (FCD) - timestamp data attributes	 Y Y
		<additional items>	

PIXIT for GOOSE subscribe model

ID	Ed	Description	Value / Clarification
Gs1	1,2	What elements of a subscribed GOOSE message are checked to decide the message is valid and the allData values are accepted? If yes, describe the conditions. Notes: • the VLAN tag may be removed by a ethernet switch and shall not be checked • the simulation flag shall always be checked (Ed2)	Y destination MAC address Y APPID Y gocbRef Y timeAllowedtoLive Y datSet Y goID N t Y stNum N sqNum Y simulation / test Y confRev Y ndsCom Y numDatSetEntries Greater than expected: Not detected Less than expected: Detected Data-type mismatch in data set elements: Detected N out-of-order dataset members When Y (except datSet, confRev, simulation, ndsCom and numDatSetEntries): the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the GOOSE message indicating it by changing the quality (questionable-old data). When receiving a subscribed GOOSE with the simulate bit or the ndsCom flag activated or an incorrect dataset or confRev, the DUT will discard the GOOSE message without indicating it by changing the quality. In these cases, as soon as received a subscribed GOOSE with a data value change, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the message indicating it by changing the quality (questionable-old data).

ID	Ed	Description	Value / Clarification
			When receiving a subscribed GOOSE with numDatSetEntries less than expected or data-type mismatch, the DUT will discard the GOOSE message without indicating it by changing the quality. In these cases, as soon as received a subscribed GOOSE with a data value change, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the GOOSE message indicating it by changing the quality (invalid). When receiving a subscribed GOOSE with an incorrect confRev, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and immediatly the DUT will discard the GOOSE message indicating it by changing the quality (invalid).
Gs2	1,2	When is a subscribed GOOSE marked as lost (TAL = time allowed to live value from the last received GOOSE message)	Message does not arrive prior to TAL
Gs3	1,2	What is the behaviour when one or more subscribed GOOSE messages isn't received or syntactically incorrect (missing GOOSE)	If the TAL is expired the quality of the attribute in the database will be set to Questionable and Old Data and it will keep the last received value
Gs4	1,2	What is the behaviour when a subscribed GOOSE message is out-of-order	If there is a change of stNum (even with non zero sqNum) the new values are updated in the database. Otherwise, the message is ignored and the DUT keep holding the last received values in the database.
Gs5	1,2	What is the behaviour when a subscribed GOOSE message is duplicated	The DUT ignores the duplicated message.

ID	Ed	Description	Value / Clarification
Gs6	1	Does the device subscribe to GOOSE messages with/without the VLAN tag	Y, with the VLAN tag Y, without the VLAN tag
Gs7	1	May the GOOSE data set contain: - structured data objects (FCD) - timestamp data attributes	 Y Y
Gs8	1,2	Subscribed FCD supported common data classes are	SPS, DPS, INS, ENS, ACT, ACD, SEC, MV, CMV, WYE, DEL, SPC, DPC, INC, ENC, BSC, ISC, APC, BAC, SPG, ING, ENG, ASG, CURVE, CSG. Arrays are not supported
Gs9	1,2	Are subscribed GOOSE with test=T (Ed1) / simulation=T (Ed2) accepted in test/simulation mode	Y
Gs10	1,2	Max number of dataset members	Unlimited
		<additional items>	

PIXIT for Control model

ID	Ed	Description	Value / Clarification
Ct1	1	What control models are supported (compare ICD file enums for Ed2)	DOns: Y SBOns: Y DOes: Y SBOes: Y
Ct2	1,2	Is the control model fixed, configurable and/or dynamic	Dynamic
Ct3	-	Is TimeActivatedOperate supported (compare PICS or SCL)	Deprecated
Ct4	-	Is “operate-many” supported (compare sboClass)	Deprecated, see sboClass in datamodel (ICD)
Ct5	1	Will the DUT activate the control output when the test attribute is set in the SelectWithValue and/or Operate request (when N test procedure Ctl2 is applicable)	N
Ct6	-	What are the conditions for the time (T) attribute in the SelectWithValue and/or Operate request	Deprecated
Ct7	-	Is pulse configuration supported (compare pulseConfig)	Deprecated
Ct8	1	What is the behaviour of the DUT when the check conditions are set Is this behaviour fixed, configurable, online changeable	N synchrocheck Y interlock-check DUT ignores synchrocheck value. DUT uses interlock-check to perform or not the check. Fixed

ID	Ed	Description	Value / Clarification
Ct9	1,2	Which additional cause diagnosis are supported	Y Unknown Y Not-supported Y Blocked-by-switching-hierarchy Y Select-failed Y Invalid-position Y Position-reached Y Step-limit Y Blocked-by-Mode Y Blocked-by-process Y Blocked-by-interlocking N Blocked-by-synchrocheck Y Command-already-in-execution N Blocked-by-health Y 1-of-n-control N Abortion-by-cancel N Time-limit-over N Abortion-by-trip Y Object-not-selected **Edition 1 specific values:** N Parameter-change-in-execution (PCIE Ed1 semantics) **Edition 2 specific values:** Y Object-already-selected N No-access-authority N Ended-with-overshoot N Abortion-due-to-deviation N Abortion-by-communication-loss N Blocked-by-command N None Y Inconsistent-parameters Y Locked-by-other-client N Parameter-change-in-execution (PCIE Ed2 semantics)
Ct10	1,2	How to force a “test-not-ok” respond with SelectWithValue request	Invalid orCat value, orCat >= 9
Ct11	1,2	How to force a “test-not-ok” respond with Select request	The control is selected
Ct12	1,2	How to force a “test-not-ok” respond with Operate request	Invalid orCat value, orCat >= 9 DOns, SBOns, DOes: Operate value and actual position are the same SBOes: Operate values are different than selected

ID	Ed	Description	Value / Clarification
Ct13	1,2	Which origin categories are supported / accepted	Y bay-control Y station-control Y remote-control N automatic-bay Y automatic-station Y automatic-remote Y maintenance Y process
Ct14	1,2	What happens if the orCat value is not supported or invalid	DOns: command rejected SBOns: command rejected DOes: command rejected SBOes: command rejected The DUT sends reponse– with AccessResult=Object_access_denied and it sends, for enhanced security, CommandTermination with AddCause= Not-supported
Ct15	1,2	Does the IED accept a SelectWithValue / Operate with the same control value as the current status value Is this behaviour configurable	DOns: N SBOns: N DOes: N SBOes: Y/N Configurable N The DUT sends reponse– with AccessResult=Object_access_denied and it sends, for enhanced security, CommandTermination with AddCause= Position-reached
Ct16	1,2	Does the IED accept a select/operate on the same control object from 2 different clients at the same time	DOns: N SBOns: N DOes: N SBOes: N The DUT sends reponse– with AccessResult=temporarily-unavailable and it sends, for enhanced security, CommandTermination with AddCause= Object-already-selected / Command-already-in-execution

ID	Ed	Description	Value / Clarification
Ct17	1	Does the IED accept a Select/SelectWithValue from the same client when the control object is already selected (Tissue #334)	SBOns: N SBOes: N
Ct18	1,2	Is for SBOes the internal validation performed during the SelectWithValue and/or Operate step	The validation is performed during the Operate step
Ct19	-	Can a control operation be blocked by Mod=Off or [On-]Blocked (Compare PIXIT-Sr5)	Deprecated
Ct20	1,2	Does the IED support local / remote operation	Y
Ct21	1,2	Does the IED send an InformationReport with LastApplError as part of the Operate response- for control with normal security	SBOns: N DOns: N
Ct22	2	How to force a “parameter-change-in-execution”	N/A
Ct23	1,2	How many SBOns/SBOes control objects can be selected at the same time?	SBOns: multiple SBOes: multiple
Ct24	1,2	Can a controllable object be forced to keep its old state e.g. Internal Controllable Objects may not be accessible to force this, whereas a switch like Circuit Breaker outside the DUT can?	Y
Ct25	1,2	When CDC=DPC is supported, is it possible to have DPC (Controllable Double Point) go to the intermediate state? (00)	Y
Ct26	1,2	Name a DOes point (if any) with a finite operate timeout and specify the timeout (in milliseconds)	CTRL/CSWI1.Pos Timeout is configurable
Ct27	2	Does the IED support control objects with external signals?	DOns: Y SBOns: Y DOes: Y SBOes: Y
		<additional items>	

PIXIT for Time synchronisation model

ID	Ed	Description	Value / Clarification
Tm1	1	What time quality bits are supported (may be set by the IED)	Y LeapSecondsKnown N ClockFailure Y ClockNotSynchronized
Tm2	1,2	Describe the behaviour when the time server(s) ceases to respond What is the time server lost detection time	Wait for a configurable number of connection retries (unicast mode) or wait a configurable period of time (multicast mode). After that "Clock-not-synchronized" will be set. Configurable. Tested value: 10 seconds after the first request send to the time server without response.
Tm3	1,2	How long does it take to take over the new time from time server	Configurable Tested value: as soon as the new time from the time server is received.
Tm4	1,2	When is the time quality bit "ClockFailure" set	N/A
Tm5	1,2	When is the time quality bit "Clock not Synchronized" set	When connection to all time servers are lost (see PIXIT-Tm2)
Tm6	-	Is the timestamp of a binary event adjusted to the configured scan cycle	Deprecated
Tm7	1	Does the device support time zone and daylight saving	Y
Tm8	1,2	Which attributes of the SNTP response packet are validated	Y Leap indicator not equal to 3 N Mode is equal to SERVER N OriginateTimestamp is equal to value sent by the SNTP client as Transmit Timestamp N RX/TX timestamp fields are checked for reasonableness Y SNTP version 3 and/or 4 N other (describe)
Tm9	1,2	Do the COMTRADE files have local time or UTC time and is this configurable	Local Time Not configurable
		<additional items>	

PIXIT for File transfer model

ID	Ed	Description	Value / Clarification
Ft1	1	What is structure of files and directories Where are the COMTRADE files stored Are comtrade files zipped and what files are included in each zip file	/COMTRADE/ /SCL/active/ /SCL/notvalidated /SYSTEMLOG/ /COMTRADE/ Not zipped
Ft2	1,2	Directory names are separated from the file name by	"/"
Ft3	1	The maximum file name size including path (recommended 64 chars)	255 chars
Ft4	1,2	Are directory/file name case sensitive	Case sensitive
Ft5	1,2	Maximum file size for SetFile	N/A
Ft6	1	Is the requested file path included in the MMS fileDirectory respond file name	(Ed2: always complete path)
Ft7	1	Is the wild char supported MMS fileDirectory request	No
Ft8	1,2	Is it allowed that 2 clients get a file at the same time	Y same file Y different files
Ft9	1,2	Which files can be deleted	N/A
		<additional items>	

TISSUES Implementation Conformance Statement for the IEC 61850 Ed2 interface in RTF/DLF

03/04/2019, Version 0.0

UCA International Users Group
Testing Sub Committee

TICS template extracted from Server Test Procedures for Edition 2 TPCL 1.2.6

TICS Template Ed2 for TPCL 1.2.6

Introduction

This document provides a template for the Tissues conformance statement. According to the UCA IUG QAP the Tissue conformance statement is required to perform a conformance test and is referenced on the certificate.

This document is applicable for RTF/DLF with firmware version 0.9.1.

Mandatory Edition 2 Tissues

Below tables give an overview of the applicable mandatory Tissues.

Part 6 Tissue	Description	Implemented Y/na
658	Tracking related features	Y
1324	FCDA element cannot be a "functionally constrained logical node"	Y
668	Autotransformer modeling	Y
687	SGCB ResvTms	Y
719	ConfDataSet - maxAttributes definition is confusing	Y
721	Log element name	Y
768	bType VisString65 is missing	na
779	object references	Y
788	SICS S56 from optional to mandatory	na
789	ConfLdName as services applies to both server and client	Y
804	valKind and IED versus System configuration	Y
806	Max length of log name inconsistent between -6 and -7-2	Y
807	Need a way to indicate if "Owner" present in RCB	Y
823	ValKind for structured data attributes	Y
824	Short addresses on structured data attributes	Y
825	Floating point value	Y
845	SGCB ResvTms	Y
853	SBO and ProtNs	Y
855	Recursive SubFunction	na
856	VoltageLevel frequency and phases	na
857	Function/SubFunction for ConductingEquipment	na
886	Missing 8-1 P-types	na
901	tServices as AP or as IED element	Y

Part 6 Tissue	Description	Implemented Y/na
936	SupSubscription parameter usage is difficult	Y
1175	IPv6 address lowercase only	na

Part 7-1 Tissue	Description	Implemented Y/na
828	Data model namespace revision IEC 61850-7-4:2007[A]	Y
1151	simulated GOOSE disappears after 1st appearance when LPHD.Sim = TRUE	na
1468	Re-use DO from other LN	Y

Part 7-2 Tissue	Description	Implemented Y/na
778	AddCause values – add value not-supported	Y
780	What are unsupported trigger option at a control block?	Y
783	TimOper Resp- ; add Authorization check	Y
786	AddCause values 26 and 27 are switched	Y
820	Mandatory ACSI services (use for PICS template)	Y
858	typo in enumeration ServiceType	Y
861	dchg of ConfRev attribute	na
876	GenLogiclNodeClass and SGCB, GoCB, MsvCB, UsvCB	na
1038	Loss of Info Detection After Resynch	na
1050	GTS Phycomaddr definition in SCL	na
1062	Entrytime not used in CDC	na
1071	Length of DO name	Y
1091	The sentence "The initial value of EditSG shall be 0", has to be stated in part 7.2 not in 8.1	Y
1127	Missing owner attribute in BTS and UTS	na
1202	GI not optional	Y

Part 7-3 Tissue	Description	Implemented Y/na
697	persistent command / PulseConfig	na
698	Wrong case is BAC.dB attribute	Y
722	Units for 'h' and 'min' not in UnitKind enumeration.	Y

Part 7-3 Tissue	Description	Implemented Y/na
919	Presence Condition for sVC	na
925	Presence of i or f attribute - Problem with writing	Y
926	Presence Conditions within RangeConfig	Y

Part 7-4 Tissue	Description	Implemented Y/na
671	mistake in definition of Mod & Beh	Y
674	CDC of ZRRC.LocSta is wrong	na
676	Same data object name used with different CDC	Y
677	MotStr is used with different CDC in PMMS and SOPM LN classes	na
679	Remove CycTrMod Enum	na
680	SI unit for MHYD.Cndct	na
681	Enum PIDAlg	na
682	ANCR.ParColMod	na
683	Enum QVVR.IntrDetMth	na
685	Enum ParTraMod	na
686	New annex H - enums types in XML	Y
694	Data object CmdBlk	na
696	LSVS.St (Status of subscription)	na
712	interpretation of quality operatorBlocked	na
713	DO Naming of time constants in FFIL	na
724	ANCR.Auto	Y
725	Loc in LN A-group	na
734	LLN0.OpTmh vs. LPHD.OpTmh	na
736	PFSign	na
742	GAPC.Str, GAPC.Op and GAPC.StrVal	Y
743	CCGR.PmpCtl and CCGR.FanCtl	na
744	LN STMP, EEHealth and EEName	na
773	Loc, LocKey and LocSta YPSH and YLTC	na
774	ITCI.LocKey	na
800	Misspelling in CSYN	na
802	CCGR and Harmonized control authority	na
808	Presence condition of ZMoT.DExt and new DOs	na
831	Setting of ConfRevNum in LGOS	na
838	Testing in Beh=Blocked	na

Part 7-4 Tissue	Description	Implemented Y/na
844	MFLK.PhPiMax, MFLK.PhPiLoFil, MFLK.PhPiRoot DEL->WYE	na
849	Presence conditions re-assessing in case of derived statistical calculation	na
877	QVUB -settings should be optional	na
909	Remove ANCR.ColOpR and ColOpL	na
920	Resetable Counter is NOT resetable	na
932	Rename AVCO.SptVol to AVCO.VolSpt	na
939	Change CDC for ANCR.FixCol	na
991	LGOS: GoCBRef (as well as LSVS.SvCBRef) should be mandatory	na
1007	PTRC as fault indicator - Update of description required	na
1044	TapChg in AVCO	na
1077	Rename DOnames within LTIM	Y

Note: Tissues 675, 735, 772, 775, 776, 878 are not relevant for conformance testing

Part 8-1 Tissue	Description	Implemented Y/na
784	Tracking of control (CTS)	na
817	Fixed-length GOOSE float encoding	na
834	File dir name length 64	Y
951	Encoding of Owner attribute	Y
1040	More associate error codes	Y
1178	Select Response+ is non-null value	Y

Compare the TISSUE database for more details: www.tissues.iec61850.com

E. IEC 61850 Ed.2 Dynamic Model

E.1 IEC 61850 Standard E-2
E.2 Communications Stack E-3
E.3 IEC 61850 Server and Data Model E-4
E.3.1 AccesPoint E-5
E.3.2 Logical Device E-7
E.3.3 Logical Node E-7
E.4 Web Server E-9
E.5 Communications Port E-11
E.6 File Transfer E-12
E.7 CID Configuration File E-13
E.8 Mod/Beh E-14
E.9 Data Set E-16
E.10 GOOSE Messages Publishing E-17
E.11 Subscription to GOOSE Message Data E-19
E.12 Report Control Blocks (RCBs) E-22
E.13 Measurement Configuration (Data CF) E-24
E.14 Commands E-26
E.15 SNTP Synchronization E-28
E.15.1 SNTP Synchronism Status Calculation E-28
E.15.1.a *Unicast* Client E-28
E.15.1.b *Broadcast* Client E-29

E.1 IEC 61850 Standard

IEC 61850 relay models have an extra protection and control function defined by **IEC 61850** standard.

Extra services provided by **IEC 61850** relays are:

- Reporting relay data (pickups, trips, blockings, etc) to a higher level equipment (Central Unit, Remote Control, HMI, etc).
- Quick data reporting (GOOSE) to same level relay (protections, control equipment, auxiliary services) or, even to other higher level equipment.
- MMS communications allowing any MMS client to receive the relay data model, thus being able to interact with it for editing settings and parameters and carry out commands.
- Managing a single file (**CID**) that allows to have a *backup* containing all protection, control and communications parameters.
- FTP access to oscillograms, logs, etc.
- Web server providing information on the relay status, errors, status and measurements, subscription to GOOSE messages, etc.

Each protection element contains **IEC 61850** mapping information with regard to node name and settings, available digital signals, commanding data, measurements, etc.

IEC 61850 is a substation automation standard defined by the TC57 Technical Committee. The standard is segregated into 10 parts and deals with issues related to general system requirements, engineering project management and communications requirements, putting forward a data model on which IED capacities are described. This data model is developed through the substation description language (SCL) also defined in the standard. Relay functions are modelled from the so called Logic Nodes (LN) that, at the same time, are formed from *Common Data Classes* and *Common Data Attributes*, following an object abstraction philosophy. Together with these objects, the standard defines a set of services through the so called *Abstract Communication Service Interface* (ACSI). Sections 8 and 9 of the standard explain how these objects and services are mapped in terms of given protocols, specifically, MMS, GOOSE and Sampled Values. The last section of the standard deals with the conformity tests that a relay or architecture must pass in order to be approved according to the standard, thus covering all aspects.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Therefore, the standard includes the chapters or parts below:

- *IEC 61850-1: Introduction and overview.*
- *IEC 61850-2: Glossary.*
- *IEC 61850-3: General requirements.*
- *IEC 61850-4: System and project management.*
- *IEC 61850-5: Communication requirements for functions and device models.*
- *IEC 61850-6: Configuration language for communication in electrical substations related to IEDs.*
- *IEC 61850-7: Basic communication structure for substation and feeder equipment.*
  IEC 61850-7-1: Principles and models.
  IEC 61850-7-2: Abstract communication service interface (ACSI).
  IEC 61850-7-3: Common Data Classes.
  IEC 61850-7-4: Compatible logical node classes and data classes.
- *IEC 61850-8-1: Specific communication service mapping (SCSM) Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2) and to ISO/IEC8802-3.*
- *IEC 61850-9: Specific communication service mapping (SCSM).*
  IEC 61850-9-1: Sampled values over serial unidirectional multidrop point to point link.
  IEC 61850-9-2: Sampled values over ISO/IEC 802-3.
- *IEC 61850-10: Conformance testing.*

E.2 Communications Stack

The IED will be based on the *Client-Server* model to give data contained in its data model in a vertical way. It is a connection oriented communications, always initiated by the client and, in this case, using the MMS (*Manufacturing Message Specification*) standard, specifically developed for industrial applications, specified according to ISO 9506 and used for data interchange in production environments. This protocol is independent of the type of network or connected devices and, therefore, can be maintained as physical communications technology evolves. The protocol defines communications messages transferred between controllers, as well as between the engineering station and the controller, so that the server (IED) will make available to the clients (central units, gateways, SCADAs, computers, etc.) the data selected in a *Data Set* that will have been allocated to a *Report Control Block*. The IEC 61850-8-1 part defines the mapping between the MMS protocol service and the IEC 61850 abstract services.

The IED also has the *Publisher-Subscriber* model that the GOOSE service is based on. In this case, it is a high speed non connection oriented communications, thus enabling horizontal communications between IEDs. The message sent by the publisher will be a *multicast* message that will propagate through the local network, thus reaching all the IEDs connected to the same.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.3 IEC 61850 Server and Data Model

The IED server and, thus, the predefined physical device (default CID file generated by the configuration tool, eNET Tool), contains three *Logical Devices*. Those *Logical Device (LD)* includes all the different *Logical Nodes (LN)* that, at the same time, contain *Data Objects* (*DO*) composed of *Data Attributes* (*DA*) and that, as a whole, form the predefined relay data model (protection data). At each level, there are services available to carry out a number of functions, like reading and writing data, commands, reporting, etc.

The distribution of the predefined Logical Nodes inside the Logical Devices is the following one:

- **SYS**: *Logical Device* of the System where the *Setting Group Control Blocks, LOGs*, are located. This is also the place where the *Logical Nodes* related to the hardware of the IED are located (inputs, outputs, communications, synchronization, etc.).
- **PROT**: *Logical device* where are located the Logical Nodes of the IED.
- **MEA**: *Logical device* where are located the *Logical Nodes* related to measurements.

Apart from the protection nodes, such as PHSPIOC, PTOV, PTOF, PTUF, RREC, RBRF, PTRC, etc. that are defined in the applicable chapters where the relay protection functions are explained, the relay has the configurable control nodes described below. These control nodes will not be present in the relay data models unless they have been registered and configured with the configuration tool:

- XCBR: control node that features a double digital data used to map the status of a three pole breaker.
- XSWI: node that features a double digital data used to map the status of the disconnect switches.
- CSWI: this control node contains the double commands on the switchgear (breaker and disconnect switches).
- CILO: control node used to map the permits of the different commanding objects.
- GAPC: general control node with single and double general purpose states and commands except for switchgear elements (breakers and disconnect switches).
- GGIO: general control node with single and double status and integer and floating analog measurements used to have any relay data available in IEC 61850. Although there are up to a maximum of 4 nodes of this type, using as far as possible the relay own protection nodes is recommended, restricting the use of these nodes to own user data generated in the control logic.
- CALH: control node used to map bay alarms.
- SIMG: control node used to map SF6 alarm and trip.
- MMTR: control node used to map energy meters calculated in control logic, normally from pulse inputs coming from external energy meters.
- LGOS: control node used to monitor the state of an input GOOSE.

The MICS file (Model Implementation Conformance Statement), which describes the extensions of the IEC 61850 data model in relation to the standard, is generated automatically by the configuration tool once defined the IED model and the corresponding configuration.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The Dynamic Data Model allows:

- Reorganizing the IEC 61850 information, this is, create or delete LDs, LNs or DOs or moving LNs from one LD to another LD or DOs from one LN to another LN.
- Carrying out internal mappings (relating IEC 61850 data to the internal data in the relay).
- The possibility of renaming LDs, LNs (prefix and/or instance) and Control Blocks (flexible naming).
- Adding new LNs according to the LNClass defined in the standard.

The IED will have a predefined data model that will include only those LNs and DOs with an associated protection functionality. This predefined data model will be obtained using the configuration tool, ***ZIV eNET Tool***®. A device with the manufacturing configuration will have just one LD (SYS) and two LNs (LN0 and LPHD).

The user will be able to create a specific data model with the required LDs and LNs, complying with the IEC 61850 rules and taking into account the limitations of the device which are defined in the configuration tool. The LDs and LNs can be created from scratch or using the elements provided in the predefined data model. The user will be able to:

- Add DOs.
- Delete DOs.
- Remap DOs which share the same CDC (Common Data Class).
- Rename extended DOs.
- Define new DOs. The new DOs can be optional or extended. In case of being extended, the CDC must be supported by the device.

The content of a DO of the reference data model (upper left corner of the tool) cannot be modified, but it can be used in other LNs, can be deleted or renamed in the user defined data model (configuration area). On the other hand, it must be taken into account that in case of DOs which represent settings, they are allowed to appear/exist just once.

Hereafter, it is described more in detail the configuration possibilities per each element.

E.3.1 AccesPoint

Depending on the model version of the IED, the functionality related to the AccessPoints changes. In those IEDs which operate only with one AccessPoint, it will only be allowed to modify the name attribute of the *AccessPoint*.

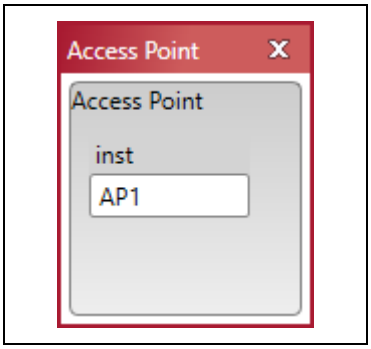


Figure E.1 AccessPoint Modification.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The models that manage AccessPoints, inside the Communications menus the user has access to their configuration.

On the one hand they will be displayed the available SubNetWorks (by default 2 or 4 depending on the number of LAN ports of the IED) and on the other hand, the AccessPoings where it can be defined the type of redundancy and the SubNetWork that it will be associated with. When any of these parameters is modified, the information shown in the SubNewWorks scressn will be automatically updated.

It should be taken into account that, from a redundancy perspective, the LAN ports operate by pairs (LAN1-LAN2 and LAN3-LAN4). Therefore, when setting the redundancy parameter with a value different to “none”, one of the ports will disappear (LAN2 or LAN4) and with it the corresponding SubNetWork.

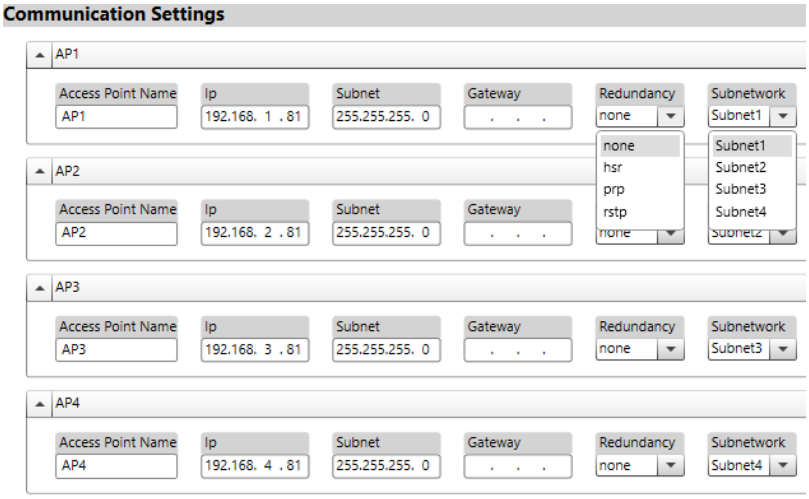


Figure E.2 AccessPoint Configuration.

Also, a new parameter will appear in the GOOSE Control Block configuration so that you can define to which AccessPoint the GCB will be associated with.

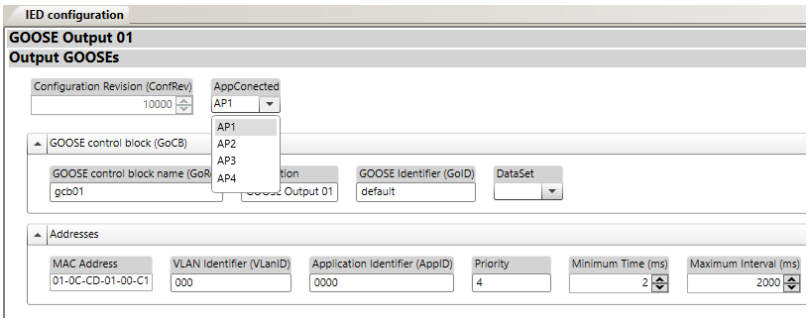


Figure E.3 AccessPoint Configuration inside the GCB.

If the user modifies the configuration of the AccessPoints once they have already been assigned to the different GCBs, and one AP that was been used disappears, automatically the tool will update the association of the GCB to the remaining AP (AP1/AP3). If later the AP configuration is changed again so that all of them are available again, the configuration tool will not proceed with any change and it will be the responsibility of the user to modify, if necessary, the assignation of the APs to the GCBs. On the other hand, the IED can receive GOOSE messages by any LAN port and therefore nothing specifically has to be configured.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.3.2 Logical Device

It will be allowed to rename, add or delete LDs from the predefined data model in the user defined data model (UDDM).

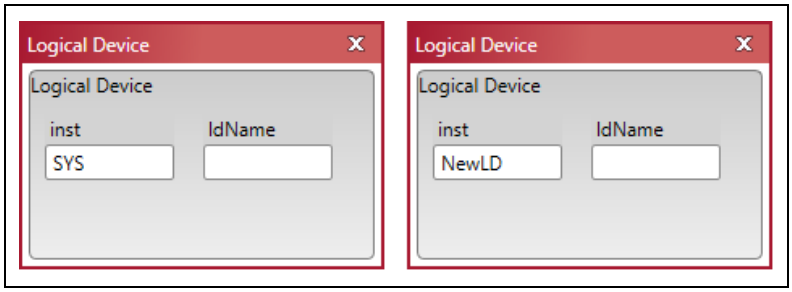


Figure E.4 Modification of LDs.

There will be a root LD where the LPHD LN will be located and the rest of LDs will have the *GrRef* DO to indicate the reference to the root LD which manages its behaviour.

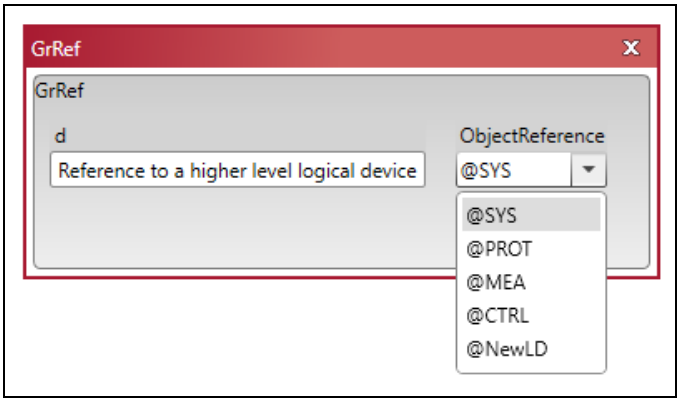


Figure E.5 Reference of LDs.

E.3.3 Logical Node

New LNs can be added selecting one *LNClass* available in the list shown by the configuration tool and defining the desired Prefix. Once added the user will have access to the DOs, being able to select the required optional DOs and with the possibility of adding new extended DOs if required. It is also possible to create new LNs with *LNClass* not defined in the standard.

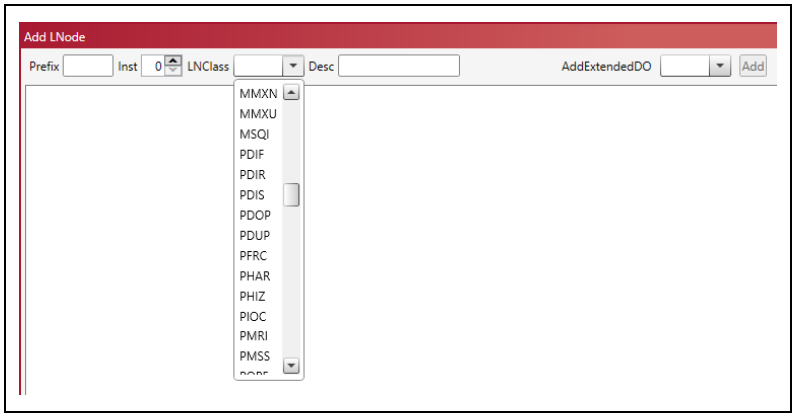


Figure E.6 New LN.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The LNs that appear in the UDDM can be deleted or modified (*Prefix*, *Instance*, *Remove* optional DOs, *Add* optional or *Extended DOs*).

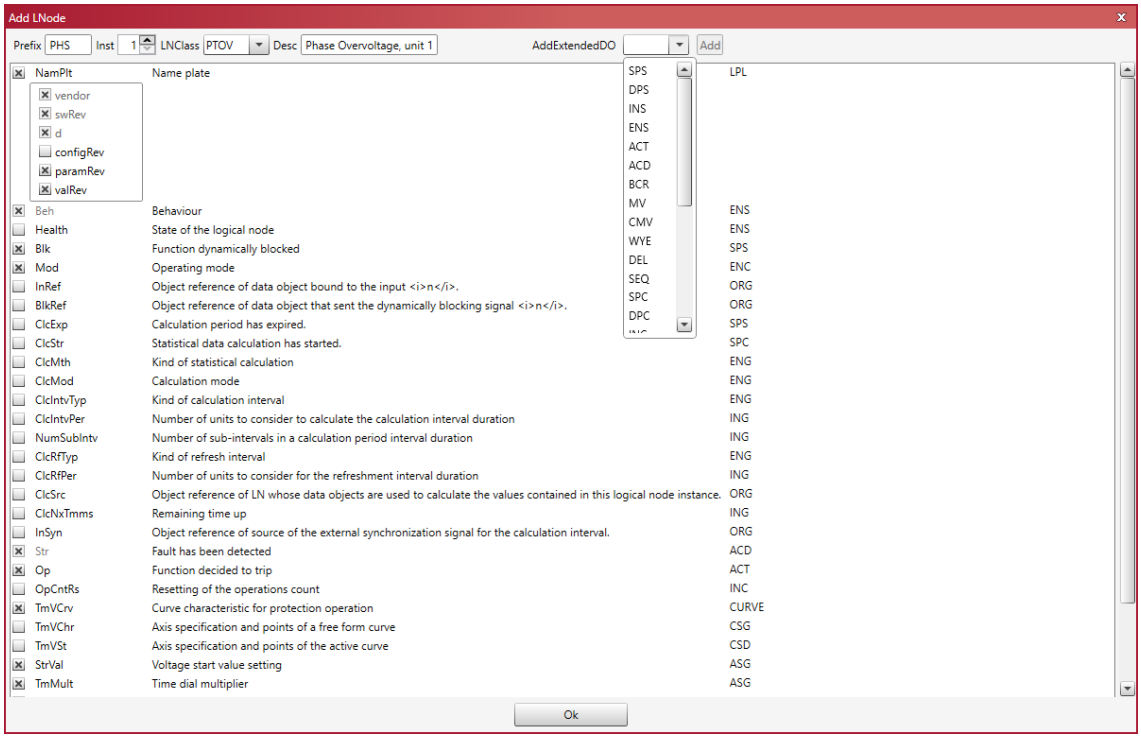


Figure E.7 Modification of LN.

It is also allowed moving one LN from one LD to another LD.

Once one DO is added inside a LN, the available resources of the IED will be used for the mapping.

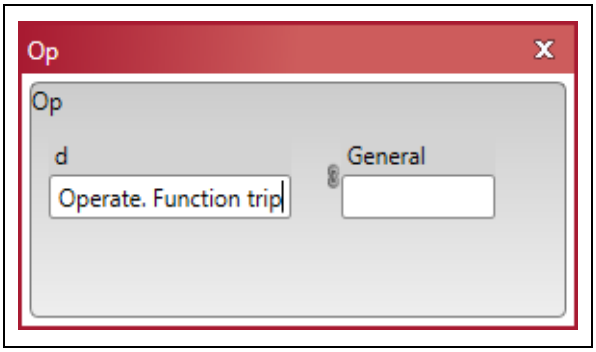
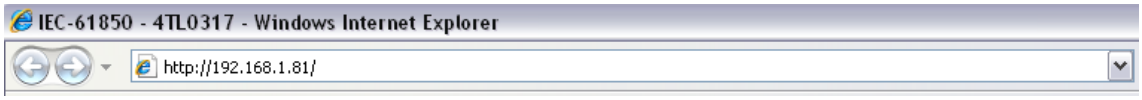


Figure E.8 Data Mapping.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.4 Web Server

Firmware versions, boot up status and useful relay data, can be accessed through the web server (using HTTP or HTTPS). To gain access, write the relay IP in a web browser:



Once authenticated (user admin, password Passwd@02 by default), the following data will be displayed:

- **Configuration**: relay identification data (hostname, location, contact, complete product model, firmware version, firmware reference and serial number) and access control data and certificates (see Cybersecurity Annex) are displayed. Additionally, it is allowed, only with the corresponding permission, to enable and disable Serial Log (option for analysis of internal anomalies by the manufacturer). Click ***Send*** and ***Apply*** to run this action.
- **Statistics**: this section shows the time the relay has been operating since the last boot up, the date and UTC time, the percentage of memory used and the percentage of CPU used. The relay date can be edit with permission to change settings.
  - **Routing**: traffic statistics can be accessed in case of using routers.
- **Log menu.** It is accessible with permission to manage logs. Shows the following information:
  - **System log:** register with boot up and system operation data that informs the user on the relay status where the reasons for CID rejection and other issues can be consulted. This register is stored in non-volatile memory. Click the button located at the top of the screen within section Download of System log, named Download File, to download the data into a text file.
  - **Security log**: see Cybersecurity Annex.
- **IEC-61850**. A number of data related to IEC 61850 standard are displayed.
  - **CID log**: register with loading data of new CID files. This register is stored in volatile memory since it stores data related to the last load. The history file may be obtained from System log.
  - **Analog signals list**: list of analog measurements available in IEC 61850 with the following data:
    - Description.
    - MMS path.
    - Value.
    - Quality: it consists of 3 fields:
      - Validity (**G**ood, **I**nvalid, **R**eserved, **Q**uestionable)
      - Quality Bit (**OV** overflow, **OR** out of range, **BR** bad reference, **OS** oscillatory, **FL** failure, **OD** old data, **ER** inconsistent, **IN** inaccurate)
      - Origin (**P** process, **S** substituted)/**T**est/Operator**B**locked.
    - Date of last update.
    - Information concerning maximum and minimum calculation (whether automatic or not).
    - Maximum value.
    - Minimum value.
    - Magnitude deadband setting.
    - Angle deadband setting.
  - **Digital signals list**: list of digital signals available in IEC 61850 with description, MMS path, value, quality and date of last update.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- **GOOSE subscription list**: list of subscriptions to GOOSE messages where the configured subscription data can be seen (MAC, APPID, GOID, etc.) and the subscription status:
  - NOT FOUND: The configured GOOSE has never been received. The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA. It is the initial state of subscriptions.
  - OK: The GOOSE has been received perfectly and has been received before the TAL (*TimeAllowedToLive*). The quality of the data subscribed to that GOOSE (node GIGGIO1) will be either that contained in the GOOSE if the data is subscribed to the quality or GOOD if it is not.
  - TIME OUT: The GOOSE has ever been perfectly received and is no longer received in the TAL (*TimeAllowedToLive*). The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA.
  - STRUCT ERROR: The GOOSE has been received but the type of data does not match the expected type or the information is not present in the GOOSE. The quality of the data subscribed to that GOOSE whose type does not match the expected type will be INVALID and without cause. If any of the information expected in the GOOSE mapped to the data does not match or that information does not travel in the GOOSE, the quality of the data will be marked as INVALID
  - NDSCOM ERROR: The received GOOSE comes with the *NdsCom* field to TRUE. The GOOSE is ignored and the quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA.
  - ERROR HOLD TIME: The received GOOSE has TAL=0. In this case, the GOOSE is ignored.
  - CONFREV ERROR: The GOOSE has been received perfectly, but with *ConfRev* different from that configured. The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately passed to QUESTIONABLE by OLDDATA.
  - DATSET ERROR: The GOOSE has been received perfectly, but with a different *DatSet* than the one configured. The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately transferred to QUESTIONABLE by OLDDATA.
  - INTERRUPTED: The IED has stopped/interrupted the subscription to this GOOSE (for example, because the computer switches to Off mode). The quality of the data subscribed to that GOOSE (node GIGGIO1) is immediately switched to QUESTIONABLE by OLDDATA.
  - WAITING: Indicates that, having received and processed GOOSEs correctly, a change of LPHD1.Sim=FALSE has been detected. The quality of the data subscribed to that GOOSE (node GIGGIO1) will be QUESTIONABLE by OLDDATA. This status will only be changed when a change in LPHD1.Sim=FALSE is detected and LGOS[X].SimSt=TRUE has just been obtained.
- **Download file:** the name of the active CID file that the relay is operating with is displayed to the top as title. Click the Download File button located under it to download the file.

- **Actions menu** (only with administrator access).
  - **Apply**. After having been changed and sent, the parameters are applied to the relay.
  - **Clear Statistics**. Deletes statistics stored in the relay.
  - **Reboot**. Resets the relay.
  - **Reflash**. Updates the relay with a new firmware version.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Taking into account the differences between the actions below (only available for administrator users) is very important.

- Send changed parameters to the relay. Click ***Send*** in the modified page to carry out this action.
- Once the desired parameters have been configured, the ***Apply*** action will activate these changes and the relay will commence to use the new applied configuration.
- Click ***Reboot*** to reset the relay.

E.5 Communications Port

The IEDs have two or four LAN ports for IEC 61850 communications. This LAN ports use the Ethernet network, using the TCP/IP protocol for MMS (standard used to pack the information in the network) communications, sending and receiving GOOSE messages, file transfer through FTP, etc. Therefore, regardless the physical media and the connection (fiber, copper, etc.), configuring the relay network IP configuration is necessary.

The relay can communicate in IEC 61850 with up to 10 clients and with 4 masters simultaneously, the port number and the protocol (PROCOME, DNP3 or MODBUS) being able to be configured. Also, the relay will always be able to communicate simultaneously with the manufacturer tool for relay remote management through the fixed port 32001.

The relay will therefore have a menu to configure the LAN ports:

- DHCP enable.
- IP address.
- Network mask.
- Routing configuration menu if required.
- Redundancy type.

And a menu to configure the TCP/IP protocols simultaneously enabled together with IEC 61850:

- PROCOME protocol: fixed connection to the TCP/IP 32001 port for remote relay management through the manufacturer tool.
- Protocols 1, 2, 3 and 4: settings to indicate protocol, TCP/IP port, etc. for simultaneous TCP/IP communications with the relay.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.6 File Transfer

File transfer access (using FTP or SFTP) will enable the availability of a number of relay folders. Different access levels will be obtained as a function of the user and password.

Accessing the equipment with user with visualization permission, read only access is gained to the following directories:

- COMTRADE: folder where the generated oscillograms are saved.
- SCL: folder containing the active CID that the relay is working with (SCL/active/).

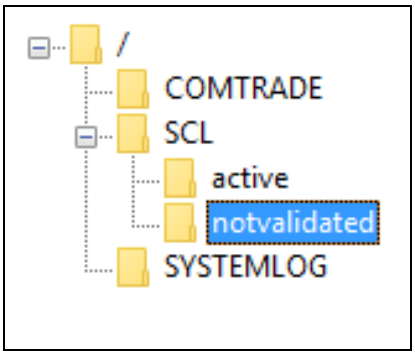


Figure E.9 Directory Structure for File Transfer.

Accessing the equipment with a user with permission to manage logs, you have read-only access to the following directory:

- **SYSTEM LOG**: folder containing *System.log* and *Security.log*.

Accessing the equipment with user with configuration loading permission, the equipment also offers write permission on the */SCL/notvalidated* folder, where the user can copy the new CID to load the equipment. When the new CID is copied to that location the equipment begins its validation.

In those cases where the relay is reset or has had a bad operation, the firmware automatically generates a file, *coredump,* where the status at the time of the failure is stored so as to be able to analyse the issue. Accessing by file transfer with a user with permission to manage logs, access to a read only folder with this information is gained.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.7 CID Configuration File

The standard defines the following files that will form part of the IED configuration process:

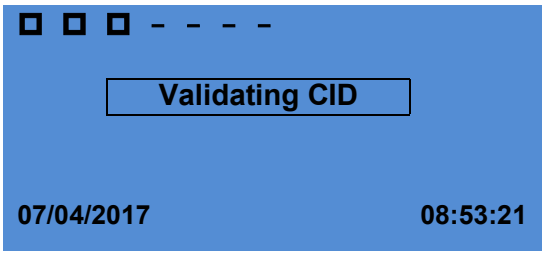
- ICD: file describing the IED capabilities. All nodes are extended and without configuration.
- CID: file containing a specific IED configuration at IED name, communications, Reports, etc. level

Both files allow knowing the relay data model in Logical Devices, Logical Nodes, Data and Attribute form. Once the relay has an IEC 61850 firmware, a basic file (**CID** with one LD and two LNs, LN0 and LPHD) will be available in the format proposed by the **IEC 61850** standard according to section 6 (SCL) that can be downloadable by file transfer, web server or FileTransfer service of IEC 61850. With the configuration tool, eNET Tool, a CID file can be generated with the complete predefined data model.

The CID file is used to configure send GOOSE message parameters, subscription to data of other GOOSE messages, create and allocate *datasets* to Report Control Blocks (RCBs) and GOOSE Control Blocks (GCBs), edit settings, control logic, descriptions, parameters etc.

The file can be edited using the program ***ZIV e-NET Tool***®. This program allows configuring the file that will later be sent to the relay through file transfer from the configuration tool. The starting CID file can be the file downloaded from the relay or a new file generated from the tool itself.

When a new CID file is loaded to the relay through file transfer (using a user with configuration loading permission), it is validated by the relay checking it is a correct SCL and that the configured IP in the file matches the IP configured in the relay, and the message **Validating CID** is displayed on the screen.



Once it has been validated, if the result is correct, the message **Validation SUCCESS** is displayed on the screen and the relay will be rebooted and reconfigured. The relay will be reset and will displayed the message **Configuring Device** and a progress bar on the screen. Upon completion of the reconfiguration process, the relay will be rebooted with the new configuration. The complete validation and reconfiguration process lasts about the minute.



© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Upon failed validation, the CID file will be rejected and deleted from the loading directory (non validated), the message **Validation ERROR** being displayed on the screen. In this case, web server logs can be accessed (through the web server, file transfer or File Transfer service of IEC 61850) in order to know the reasons for file rejection. Therefore, the relay will keep operating with the CID file that was active and communications will never be lost.



E.8 Mod/Beh

The standard defines the following values in the Logical Nodes for the Mod and Beh.

Value	Status	LN Behaviour
1	On	The application represented by the LN works. All communication services work and get updated values. DOs will be transmitted with a relevant quality. Control commands with Test=false will be accepted. Control commands with Test=true will be rejected.
2	Blocked	The application represented by the LN works. No (wired) output data will be issued to the process. All communication services work and get updated values. DOs will be transmitted with a relevant quality. Control commands with Test=false will be accepted. Control commands with Test=true will be rejected.
3	Test	The application represented by the LN works. All communication services work and get updated values. DOs will be transmitted with q.test=true, except Mod, Beh and Health that have q.test=false. Control commands with Test=false will be rejected. Control commands with Test=true will be accepted.
4	Test/Blocked	The application represented by the LN works. No (wired) output data will be issued to the process. All communication services work and get updated values. DOs will be transmitted with q.test=true, except Mod, Beh and Health that have q.test=false. Control commands with Test=false will be rejected. Control commands with Test=true will be accepted.
5	Off	The application represented by the LN does not work. All communication services work (output with quality.validity=invalid, except Mod, Beh and Health that will have q.validity=good). No process output will be done. Control commands to the process will be rejected. Only Mod accepts control command with Test=false. Settings and configuration attributes are still modifiable.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The IED (whether by LD or LN) supports the five modes.

It is implemented a hierarchy management for the LDs (*GrRef* of LLN0). The format for the *GrRef.setSrcRef* in the SCL is: "@<*LDinst*>" or "<*IEDname*><*LDinst*>" and in the on-line data model is: "<*IEDname*><*LDinst*>" or "<*LDname*>".

The "root" by default is **SYS** and therefore all the other LDs will contain the *GrRef* in their LLN0 with "**@SYS**" value, which will be read only, so that all the LDs will inherit the status of **SYS** LD. It is configurable.

The IED will provide the following features related to the test mode:

- All the information sent/available in the IED will have test indication (*q.test*=true) and the following inputs will be considered as valid:
  - Data received by GOOSE/SV message with *q*.test = true.
  - Commands received with Test=true attribute.
- Multicast signals used for simulation (GOOSE/SV):
  - Subscription: Sim is the data object used to change the status/behaviour. It is present just in LPHD1 LN of **SYS** LD and will indicate the behaviour of the GOOSE simulation for all the IED. When the IED is receiving the same GOOSE/SV in both ways, real (simulation bit=false) and simulated (simulation bit=true), the IED will take into account just to one of them depending on the value/status of *SYS/LPHD1.Sim.stVal.*
    - Real GOOSE/SV if SYS/LPHD1.Sim.stVal=false.
    - Simulated GOOSE/SV if *SYS/LPHD1.Sim.stVal=false*. In this case, the SimSt of SYS/LGOS and SYS/LSVS LN configured to monitor that GOOSE/SV message will go to TRUE, showing that the IED is receiving and processing a simulated GOOSE/SV message.
  - Publishing: The IED will have one setting that allows sending normal or simulated GOOSE messages (***LPHD1.GoTxSim***) and another one for the SV (***LPHD1.SVTxSim***). Therefore, depending on these settings, the IED will send all the GOOSE/SV messages with the simulated bit in TRUE or FALSE.

Moreover, the configuration tool will allow configurin the Beh of any LN manually, so that the user can define it as per any specific requirement:

- A user Beh can take On, Off and Blocked values base don the activation and blocking signals defined by the user.

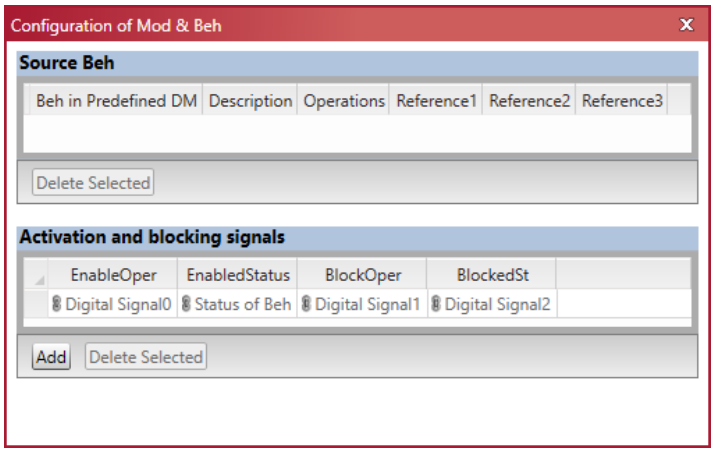


Figure E.10 Beh Configuration Depending on Signals.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- A user Beh can be calculated as a combination of Behs of different LNs of the predefined data model.

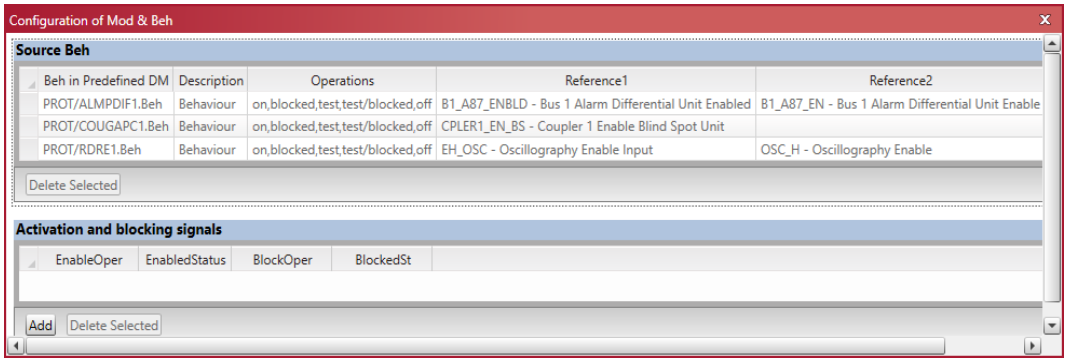


Figure E.11 Configuration of Beh as a Combination of Different LN Behs.

E.9 Data Set

The relay supports a maximum of 35 Data Sets, each containing a maximum of 500 FCDAs.

The FC allowed in a Data Set which will be assigned to a RCB are the following ones: ST, MX, SP, CF, DC, SG, SR, OR, BL and EX.

The FC allowed in a Data Set which will be assigned to a GCB are the following ones: ST, MX and SP.

Datasets can be located inside the LD and LN selected.



Figure E.12 Configuration of Datasets.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.10 GOOSE Messages Publishing

This service is defined in the standard and enables horizontal, fast and safe communications between IEDs. They are *multicast* messages and, thus, the emitter will place the data in the network and this will be received by any relay connected to the same. It has a message repeat algorithm, so that the data can be received by new relays connected to the network and, in this way, the receiving IEDs can detect communications or own emitter failures and act accordingly.

The type of the Performance class (according to IEC 61850-5 and IEC 61850-10) is P2/P3 performance class. The IEDs have 10 GCBs, so that they can be configured to send up to 10 different GOOSE messages. Each GCB has the following configurable parameters:

- MAC: send GOOSE message virtual MAC address
- VLAN ID: VLAN identifier
- AppID: application identifier. Parameter used to differentiate between GOOSE messages.
- VLAN Priority: message priority identifier.
- MinTime: minimum GOOSE message repeat time.
- MaxTime: maximum failure detection time on the part of the receiver (MaxTAL). The maximum GOOSE message repeat time will be MaxTime/2.
- GoID: string with a maximum size of 65 octets, which identifies the GOOSE message.
- GoRef: with a maximum size of 65 octets, which identifies the name of the GCB.
- Data Set: Data Set to be sent in the GOOSE message.
- Description: user-editable identifier to provide extra information.

Configuration version (*ConfRev*) is automatically calculated by the configuration tool and update at the time of generating the CID file.

Both *Data Attributes* and *Data Objects* (any FCD with a single FC ST/MX) can be sent through GOOSE and the same Data Set can be allocated to a GCB and a RCB. The relay can send both single and double digital signals, (SPS) and (DPS), integer data (INT) or analog measurements (FLOAT). When a measurement is allocated to a Data Set that will later be allocated to a GCB, it must be taken into account that, if the *deadband* associated to this measurement is configured to 0, this measurement will not be assessed, it will never generate a change and, therefore, will not cause GOOSE *trigger* by a change of value. If, otherwise, an instantaneous measurement is selected in the Data Set associated to a GOOSE message, every change of measurement will produce GOOSE sending.

In order to carry out the configuration, a Data Set must be first generated with the data to be sent in the GOOSE message. As a rule, attribute pairs (data, q) are sent but the relay can work with any type of Data Set. Later, this Data Set will be allocated to the desired GCB, any of the 10 existing in the relay model.

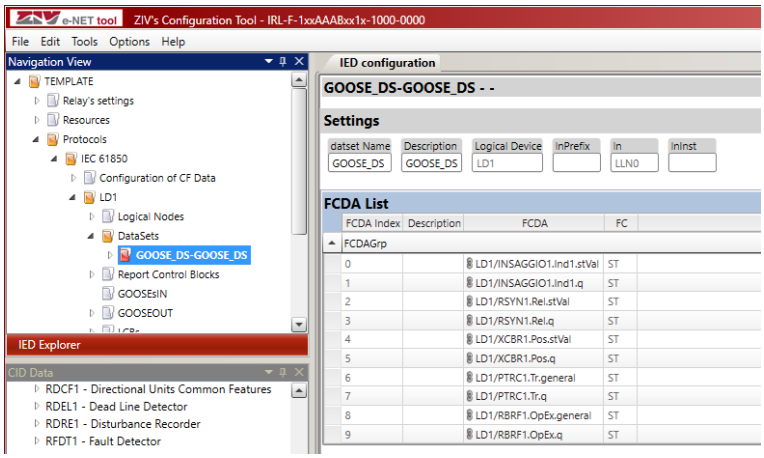


Figure E.13 Data Set Configuration for GOOSE.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

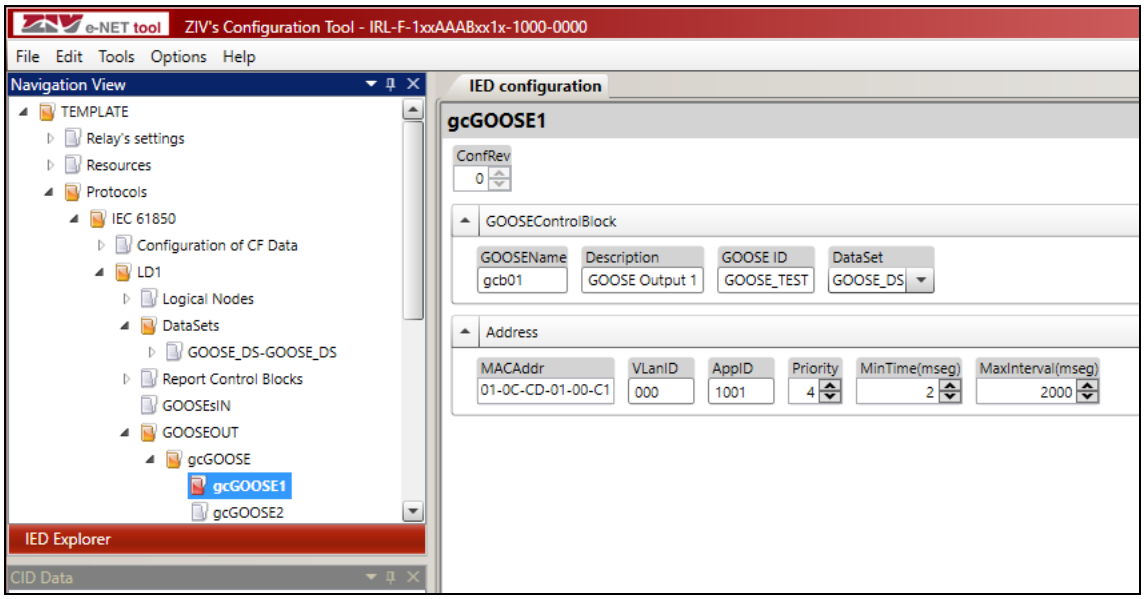


Figure E.14 GCB1 Configuration with Data Set Generated in Advance.

In this way, when a tool-generated CID is sent to the relay, after boot up, it will start sending a GOOSE message with the configured Data Set data.

The GCB can be added inside any LD.



Figure E.15 Configuration of GCBs in Different LDs.

If the Data Set allocated to the GCB is so large that the relay is not able to process and send, all relay services will be booted up normally, but the GOOSE message will not be sent, since it will have been disabled and the *NDSCom* attribute of that GCB set to TRUE. The *System Log* will display a message stating this condition:

ERR - [IEC61850ED1] Goose encoding error, setting GCB invalid (GoEna=False, NdsCom=True)

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.11 Subscription to GOOSE Message Data

Subscription to GOOSE message data is carried out through *ExtRef*, that can be located inside any LD and any LN.

You can subscribe to a total of 400 elements using the *ExtRefs*. Each subscribed element (value and / or quality) will occupy an independent *ExtRef*.

The device can receive GOOSEs containing both data (CDF) and attributes (FCDA), but the subscription has to be made only to final attributes of type boolean, *DbPos*, int, float and quality. For example, if an SPS data travels in the GOOSE, the equipment should subscribe to the *stVal* attribute and the *q* attribute (if desired), using two *ExtRefs*.

So, as defined before, the subscription is carried out through any LN in the data model, where it will be mapped to internal data where the data received through the GOOSE service will be stored. Because of this, at the time of configuring a subscription, the required user resources (digital and/or analogue signals) must be generated. Those user resources will be the ones where the data received through the GOOSE message will be stored.

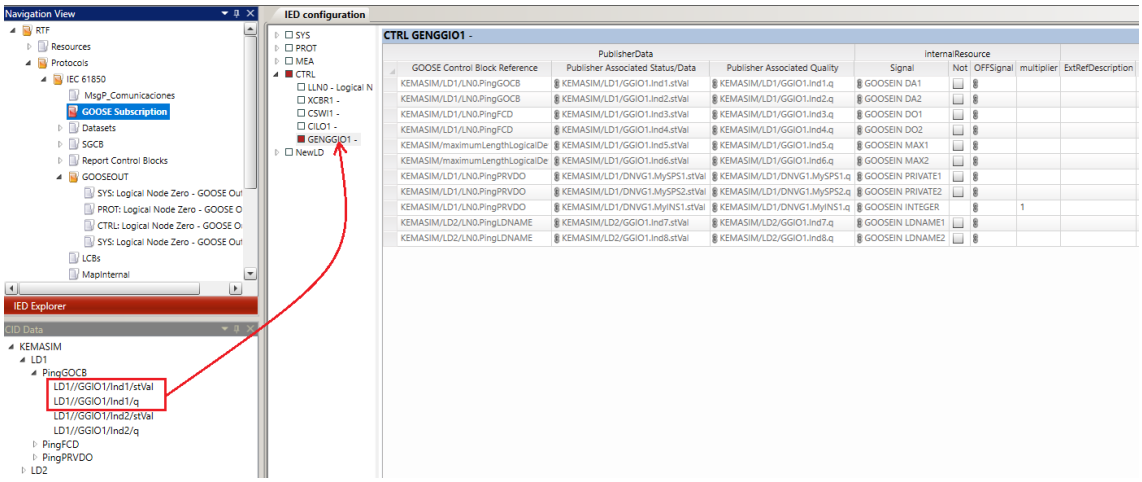


Figure E.16 Subscription to GOOSE Messages inside CTRL/GENGGIO1.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The tool also allows adding non-complete subscriptions so that the corresponding ExtRef will be added inside the desired LN just with the internal resource configured. This way the tool will generate one file (*.IID) that the SCT will use to complete all the information related to the publishers (later binding). For that purpose, the internal resource where the information of the subscribed element will be stored has to be selected and drag into the LN where the ExtRef will be added. The configuration tool will not allow generating a CID file this way, because the configuration of that type of subscriptions is not completed and the IED would reject it, but it allows generating one IID file so that the SCT will be the one in charge of finishing the configuration. Due to the fact that there is pending information related to the publisher, the tool will show the corresponding LN marked in grey instead of red.

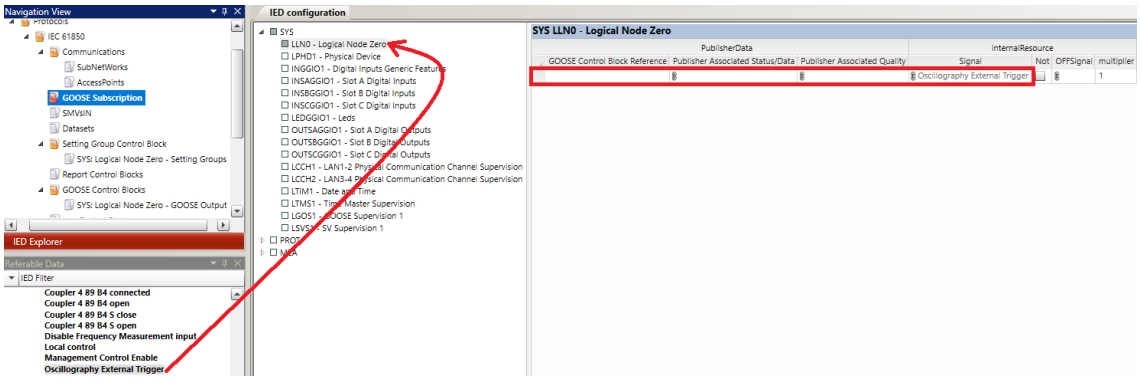


Figure E.17 GOOSE Subscription using Later Binding

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The Mod status of the IED (LD SYS.LLN0.Mod) will define the way the IED will process the GOOSE subscription elements.

GOOSE input value	on	blocked	test	test-blocked	off
value=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=false	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=false	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=good *detailQual*=0 *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Processed as valid** *value*=X *validity*=good *detailQual*=0 *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=quest *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Processed as questionable** *value*=X *validity*=quest *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=false	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
value=X *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Processed as invalid** *value*=latest valid value *validity*=invalid *detailQual*=Y *test*=true	**Not Processed** *value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false
GOOSE is no longer being received	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=false	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=false	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=true	*value*=latest valid value *validity*=quest *detailQual*=OD(*) *test*=true	*value*=latest valid value *validity*=invalid *detailQual*=0 *test*=false

Where:

(*) OD = *OldData*.
“Processed as valid” means that the application should react according to the quality and intended functionality of the LN.
“**Processed as invalid**” means the application should react as if the quality of the data had been invalid or as the data source has failed.
“**Processed as questionable**” means that the application should decide how to consider the status value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.12 Report Control Blocks (RCBs)

This method is used in the standard for an effective vertical communication between the IED (server) and the clients (central units, gateways, SCADAs, etc.). The IEDs have 20 indexed RCBs. The user will define per each RCB added the maximum number of indexed RCBs that will be available and per RCB it will be defined:

- Configuration revision.
- RCB:
  - Buffer time. (the buffer size is 30 kbytes).
  - Report Name.
  - Description.
  - Data Set associated to the RCB.
  - Report Identifier (*rptID*).
  - Integrity Period. The minimum configuration value is 500ms.
- Trigger Options:
  - Data Change (*Dchg*).
  - Quality Change (*Qchg*).
  - Data Update (*Dupd*): configurable but not supported by the IED.
  - Integrity.
  - General Interrogation.
- Optional fields: Sequence number, TimeStamp, ReasonCode, dataSet, Reference to Dataset, Entry ID, Configuration Reference y BufferOverflow.
- Client Reservation:
  - Max: number of indexed RCBs.
  - ClientAP and ClientLN per each indexed RCB to configure the reservation.

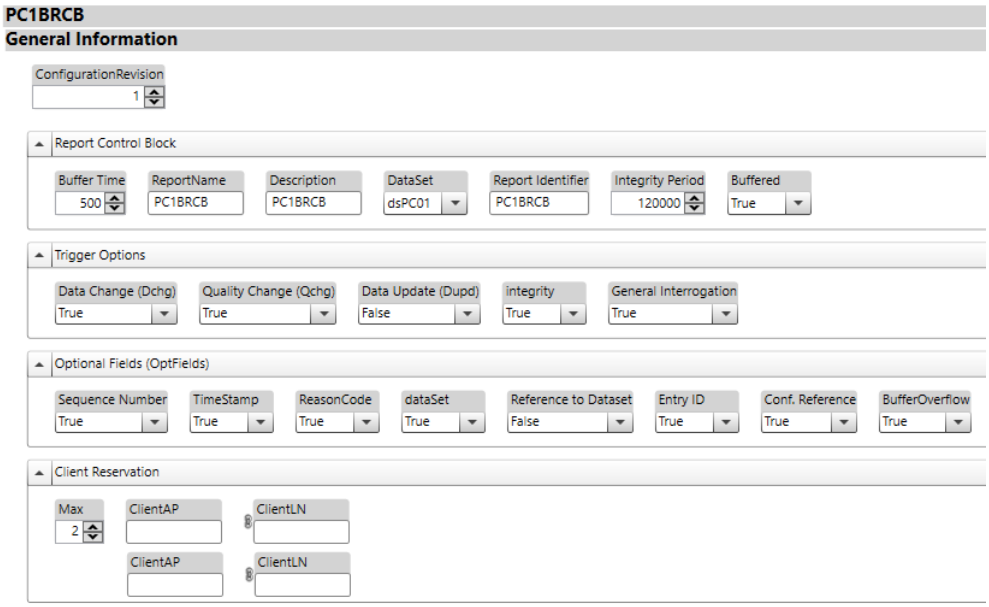


Figure E.18 Configuration of a BRCB.

The moment a client enables a RCB after having connected and associated with the relay, this RCB is then no longer available for other clients. Although all the configuration parameters are available in the tool, the client (once connected and prior to enabling the RCB) can edit the same according to its needs, except for the Data Set and ***Configuration Revision*** (***SqNum***, ***GI*** and ***TimeofEntry*** *cannot be edited either*).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The IED supports the following ***Trigger Options***, apart from ***General Interrogation***:

- ***Integrity***: the relay will send periodically a *Report* with all the information of the Data Set, according to ***Integrity Period*** setting configuration.
- ***Data Change***: the relay will send a *Report* when a change in a the value of any Data Set element is detected and only this changed data will be sent.
- ***Quality Change***: the relay will send a *Report* when a change in Data Set element quality is detected and only this changed data will be sent.

The IED allows preconfiguring RCBs to specific clients so that those RCBs can just be configured and enabled by the preconfigured clients. In order to carry out that configuration it is necessary having the ICD/IID/CID/SCD file where the information of the client appears. Clicking with the right button of the mouse over the ***Report Control Blocks*** it appears a menu (***Open SCL file***) from where you can select the SCL file of the client. The tool will extract from that file the necessary information to preconfigure the desired RCB (LN and *AccessPoint* of the corresponding IED). Once selected the SCL file, it will appear in the ***Tools*** window, when being selected ***CID Data***, the information of the SCL file which will be used to configure the ***ClientLN*** and ***ClientAP*** fields of the desired RCB.

It is necessary that the SCL file of the client contains the *Clientservices* of the *bufReport* and/or *unbufReport* enabled (true) into the *Services* section so that the tool can preconfigure the RCBs.

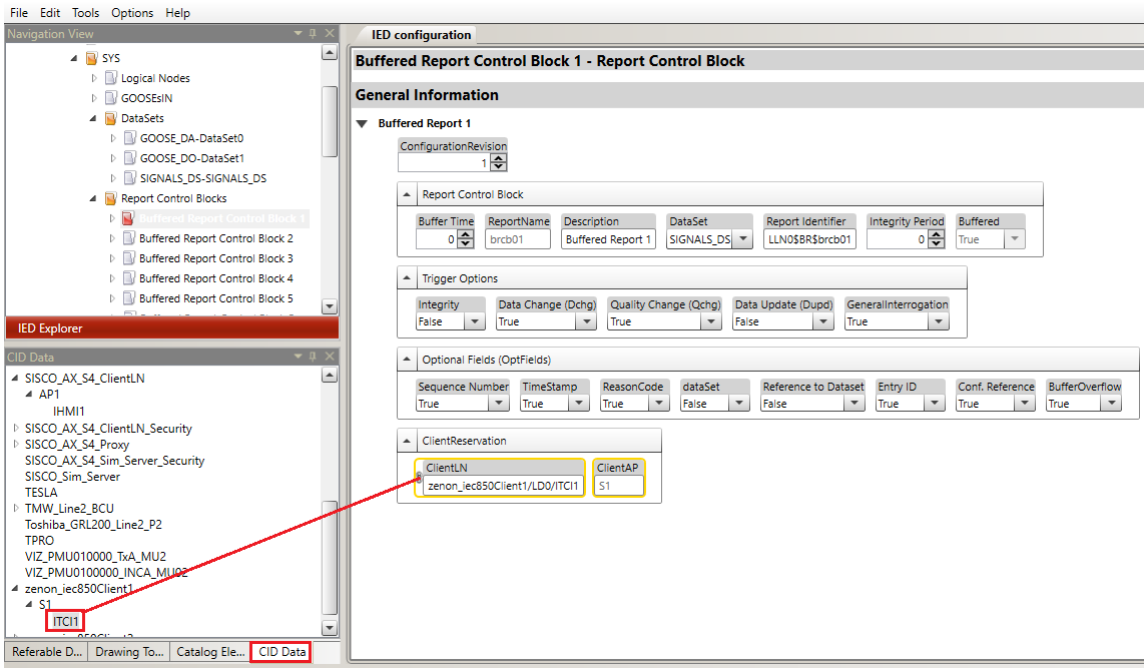


Figure E.19 Preconfiguration of a RCB.

In the hypothetical case in which a ***ClientLN*** has been configured without a ***ClientAp*** and the client IED has several *AccessPoints* with the same server (*ServerAt*), this is, when the tool can not determine the *AccessPoint* of the Logical Node selected of the client, the preconfiguration of the RCB will be refused. In this case, the ***ClientLN*** will be ignored and an error notification will be displayed. When performing a preconfiguration of a RCB, the tool will automatically add to the CID the information of the client IED (Communications field, *DataTypeTemplates*, etc.).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.13 Measurement Configuration (Data CF)

When the automatic measurement range calculation setting is enabled (*AutoRanMag* data located in the logic node LPHD), the relay will carry out the automatic calculation of the 6 elements of the measurements *rangeC*. In this case, these elements will be *read only* type. The automatic calculation will be as follows:

- max: will be calculated as a function of the measurement, its nominal and corresponding transformation ratios.
- hhLim = min + ((max-min) * 80 / 100)
- hLim = min + ((max-min) * 60 / 100)
- lLim = min + ((max-min) * 40 / 100)
- llLim = min + ((max-min) * 20 / 100)
- min: will be calculated as a function of the measurement, its nominal and corresponding transformation ratios.

When the setting is disabled, the user can configure these *rangeC* elements as deemed appropriate, either from the configuration tool or through MMS, although the following checks will be carried out:

- rangeC.max > rangeC.min
- max>=hhLim>=hLim>=lLim>=llLim>=min

Any change in the *rangeC* values will be updated in the CID file.

On the other hand, each measurement has its *deadband* (***db*** attribute). *Deadband* represents the difference percentage between maximum and minimum values of a measurement in 1 per thousand (0.001). This setting is present in the data model since the measurements consist of two data: "**instMag/instCVal**" representing the instantaneous and continuous measurement value and "**mag/cVal**". This "**mag/cVal**" data is updated when the instantaneous measurement value is subject to a certain change, defined in the ***db*** setting and it is this "**mag/cVal**" data that is subject to the Reports and LOGS (*data change*) assessment function, namely, the data that is sent through communications in Reports and is stored in the LOG files.

Regarding GOOSE messages, both the instantaneous and the *deadband* data generate change and, thereby, the GOOSE message change *trigger*, so that instantaneous data selection in the Data Set associated with GOOSE messages is not recommended. Below is a graph with the relation between instantaneous and deadband data.

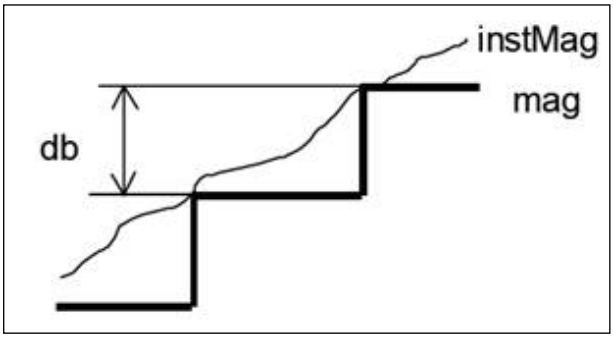


Figure E.20 Relation between Instantaneous and *Deadband* Measurement.

The measures contained in elements of Common Data Class: WYE, DEL or SEQ are a collection of simultaneous measurements in a three-phase system that represent phase to ground values, and their respective time stamps hold the same value "t". In addition, as indicated in the standard (IEC61850-7-3): *The actualization of one of the component due to a dead band calculation results in the actualization of all other components and a restart of the dead band calculation for all the components*.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

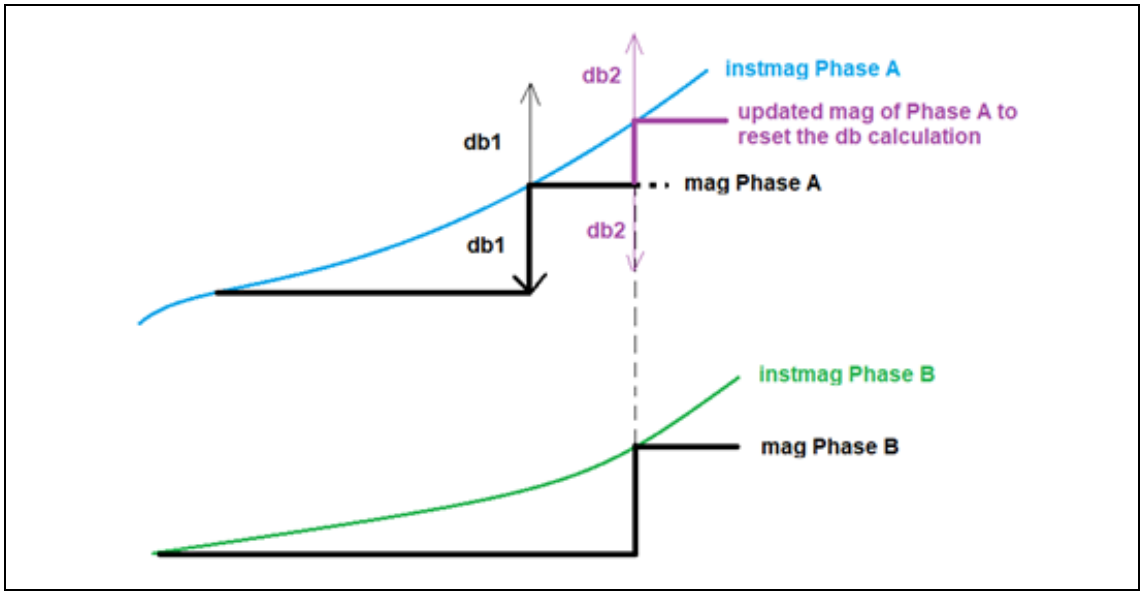


Figure E.21 Deadband actualization of simultaneous measurements.

So, in these cases, whenever a single phase is to be tested, it is recommended to set all db and zerodb parameters of the rest of phases to their highest possible values. In other words, when injecting and so when modifying the value of all phases, t and mag of all phases will be updated when the lowest db value between all phases has been reached or crossed (and then, the reference of all the rest of phases is modified too). It should also be tested, that whenever one changes the rest are updated (to do that, set db and zerodb to different values).

In the same way, the change in the angle will update the whole group of measurements. Therefore the dbAng must be also taken into account.

As an example, below is shown the influence of the ***db*** data in the generation of changes of the measurement to be reported.

RangeC setting values max=30326402.0 and min=-30326402.
max-min= 60652804 W

db = 1000
1% del max-min => 606,5 kW
When the measurement varies 606.5 kW, a change is detected and the report is sent. In the graph above, the steps would be 606.5 kW.

db=10
0,01% del max-min => 6,065 kW
When the measurement varies 6.065, a change is detected and the report is sent. In the graph above, the steps would be 6.065 KW.

db=1
0,001% del max-min => 606,5 W
When the measurement varies 606.5, a change is detected and the report is sent. In the graph above, the steps would be 606.5 W.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.14 Commands

IEDs support SBO and direct commands, with or without enhanced safety as a function of the ***ctlModel*** setting value present in every relay commanding data:

- ***ctlModel*** = 0: non commanding data.
- ***ctlModel*** = 1: direct command with normal safety, which can be run after writing the applicable *Oper* attribute.
- ***ctlModel*** = 2: SBO command with normal safety. Before running it, first select the data by reading the *SBO* attribute. The IED will return the *path* of the selected data as indication of a good operation and "null" in case of error. Once selected, the data can be run after writing the corresponding Oper before the time ***sboTimeout*** times out, after which time the element is not longer selected.
- ***ctlModel*** = 3: direct command with enhanced safety that can be run after writing the corresponding *Oper* attribute. The IED will send information on how the command has been run: execution of the command rejected, failed termination or successful termination, indicating the cause of the failure in the first two situations.
- ***ctlModel*** = 4: SBO command with enhanced safety. In order to run it, first select the data by writing the *SBOw* attribute. Once selected, the data can be run after writing the corresponding Oper with the same SBOw write parameters before the time ***sboTimeout*** times out, after which time the element is not longer selected. The IED will send information on how the command has been run: selection of the command rejected, execution of the command rejected, failed termination or successful termination, indicating the cause of the failure in the first three situations.

The device supports the *interlock-check* for any configurable command, so that, depending on the value of the mentioned *Check* attribute, the device will apply the information of the associated CILO Logical Node to the command to block it or to skip such blocking.

The commands hierarchy in the IEDs with dynamic data model has been defined at the level of the element which can receive commands (DO by DO independently) and following what it is declared in the standard. Each element can be associated to the LocKey, Loc and LocSta DOs at LN level. Depending on the value of them (plus the heritage of the LLN0 of the LD where it is located and the possible LDs that this LD belongs to) the element will calculate the hierarchy status. Logically, the value of the MltLev setting that allows working with several hierarchy levels at a time or just with one has to be taken into account and also the LocMntnc DO (device in maintenance) that will block any command except the ones generated with orCat 7 (maintenance).

Therefore, based on the status of those DOs, the commands will be accepted or rejected depending on the origin they are coming from. The combination is described in the following table which shows the same information of table B.1 of the 7-4 part of the IEC 61850 standard.

If those DOs are not appearing in the data model (from the point of view of the LN), the IED will use the internal signals (Local/Panel-Controlled/Remote) that were being used before with the previous models (check the Programmable Logic chapter).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

IED		Signal from each commandable element			IEC 61850 Origin							
					1	2	3	4	5	6	7	8
MltLev	Maintenance Control	Local Control	Station Control	Remote Control	Bay-ctrl	Station-ctrl	Remote-ctrl	Auto-bay	Auto-station	Auto-remote	maintenance	process
0	0	0	0	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK
0	0	0	0	1	BLOCK	BLOCK	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK
0	0	0	1	0	BLOCK	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK
0	0	0	1	1	BLOCK	PERM	PERM	BLOCK	PERM	PERM	BLOCK	BLOCK
0	1	0	0	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
0	1	0	0	1	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
0	1	0	1	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
0	1	0	1	1	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
0	0	1	0	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	0	1	0	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	0	1	1	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	0	1	1	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	1	1	0	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	1	1	0	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	1	1	1	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
0	1	1	1	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	0	0	0	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK
1	0	0	0	1	PERM	PERM	PERM	PERM	PERM	PERM	BLOCK	BLOCK
1	0	0	1	0	PERM	PERM	BLOCK	PERM	PERM	BLOCK	BLOCK	BLOCK
1	0	0	1	1	PERM	PERM	PERM	PERM	PERM	PERM	BLOCK	BLOCK
1	1	0	0	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
1	1	0	0	1	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
1	1	0	1	0	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
1	1	0	1	1	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	PERM	BLOCK
1	0	1	0	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	0	1	0	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	0	1	1	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	0	1	1	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	1	1	0	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	1	1	0	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	1	1	1	0	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK
1	1	1	1	1	PERM	BLOCK	BLOCK	PERM	BLOCK	BLOCK	BLOCK	BLOCK

Exceptions:

- If LockKey = True, commands received by communications will not be accepted no matter which is the status of the input signals “Local Control”, “Station Control”, “Remote control”, “Maintenance Control” or the value of the MltLev. Commands received by communications will be rejected with AddCause=Blocked-by-switching-hierarchy.
- All the internal commands with orCat “4” will be accepted.
- When being in orCat “1”, the IED will accept commands received by communications but only if they are coming from origin 1.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

E.15 SNTP Synchronization

The IED is able to synchronize through the communications network by SNTP protocol (*Simple Network Time Protocol*), as indicated by IEC 61850. The SNTP client of the equipment can be configured in *broadcast* or *unicast* mode: with one or two servers:

- *Broadcast*: the relay will wait to receive *broadcast* messages sent by the GPS clock for synchronizing.
- *Unicast*: the relay will send a date and time request to the GPS clock and will be synchronized with the message received.

The settings are detailed in the Physical Description section of the Description and Start-Up chapter.

E.15.1 SNTP Synchronism Status Calculation

The SNTP module recalculates its status every time any client (*unicast* or *broadcast*) calculates its own, which occurs with a change in its status (online/offline) due to timing, at the end of each interrogation cycle with response (correct structure) on the part of a server (*unicast client*) or with each received *broadcast* message (*broadcast* client).

The calculation method varies as a function of the ***Synchronism status calculation*** setting value:

- If the setting has been configured as ***Leap indicator***, the SNTP module status will be the latest status calculated by any of the *unicast* and *broadcast* clients.
- If the setting has been configured as ***Timing***, the SNTP module status will be a combined status of both *unicast* and *broadcast* clients, following two possible algorithms:
  - If ***broadcast error timing*** is set to 0, the SNTP module status is only a function of the *unicast* client status, except when the *broadcast* client switches from offline to online, at which time the SNTP module switches to the online status until a new *unicast* client status calculation.
  - If ***broadcast error timing*** is set to a value other than 0, the SNTP module status is a combination of the *unicast* and *broadcast* client statuses. In this mode, the SNTP module status will be:
    Synchronized if any client is in synchronized status.
    Non Synchronized if no client is synchronized and any client is not synchronized.
    Non calculated if all the clients are in non-calculated status.

E.15.1.a *Unicast* Client

A disabled *unicast* client does not make synchronization requests to servers. Therefore, when the IED client is enabled, it will interrogate the servers that have a configured IP address other than 0.0.0.0, which is the server identifier to be ignored.

Synchronization Period and ***Interval Between Retries*** settings define the time request interval to the servers when the client is in synchronized status and non-synchronized status respectively. The ***Number of Retries*** setting defines the maximum number of retries on a server if a valid response is not received. A 0 value indicates that retries will not be made, namely, only one connection attempt will be made. The ***SNTP Time Between Retries*** setting indicates the maximum waiting time between retries.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

As a function of these settings, the relay will send the appropriate messages and will wait for the answer on the part of the SNTP server. If ***Ignore leap indicator*** is set to **NO**, the received message will be process in terms of *leap indicator* field (less than 3), *stratum* field (from 0 to 16) and time difference between server and client (less than the ***Maximum Synchronization Time Difference*** *setting* except that the setting is 0), so that these received values must be within ranges in order to accept the synchronization, but when the ***Ignore leap indicator*** setting is set to **YES**, the message will be directly accepted. If the message is not accepted, the IED will interrogate the second server. The relay, in this way, will successively interrogate the servers until receiving a valid response from one of them. If, after going through all the servers, a correct response is not received, **non-synchronized** status will be shown. The relay will listen to NTP messages sent to its own IP address.

If the synchronized status calculation is set to timing, the ***Unicast Validity Timing*** setting specifies the time lapse from the first valid message received without receiving error messages or timeouts, so that the client switches to a synchronized Status. When the setting sets to 0, the waiting time is 0 seconds, so that the unicast client will switch to synchronized Status when the first correct message is received.

Unicast Error Timing enables selecting the time lapse from the last valid message received, so that the unicast client switches to non-synchronized Status. The timing also starts at the time when the client reaches the synchronized Status, since it could remain in this status without receiving any valid message.

E.15.1.b *Broadcast* Client

The *broadcast* client receives NTP synchronization *broadcast* messages, sets the time in accordance with the same, and calculates synchronism status at all times. When disabled, the IED will ignore the received synchronization messages. The synchronized status will be produced the moment a correct message is received, provided the time set in ***Broadcast Validity Timing,*** elapsed from the first correct message received, has run out, switching to non-synchronized when no valid messages are received within the time configured in ***Broadcast Error Timing***. The *broadcast* client will permanently be awaiting to receive NTP *broadcast* synchronization messages, listening to messages received with destination IP address 255.255.255.255 or *broadcast* address corresponding to the subnetwork that it belongs to. Listening to messages sent to its IP address in particular is also deemed correct.

Force unicast setting establishes whether a new *unicast* refresh must be sent at the time of receiving a *broadcast* message. The *unicast* client, when receiving the synchronization request, will cancel the refresh in progress if applicable and will immediately start a new refresh process with the servers.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Protocol Implementation Conformance Statement for the IEC 61850 interface in IRF/IDF/ZLF/DLF/RTF from ZIV Aplicaciones y Tecnología

Version 0.0, Date 15/05/2021

based upon UCAIug PICS Template version 3.0

UCA International Users Group
Testing Sub Committee

Date: January 19, 2021

1. General

The following ACSI conformance statements are used to provide an overview and details about IRF/IDF/ZLF/DLF/RTF, with firmware version 0.10.0:

- ACSI basic conformance statement,
- ACSI models conformance statement,
- ACSI service conformance statement

The statements specify the communication features mapped to IEC 61850-8-1 and IEC 61850-9-2.

2. ACSI basic conformance statement

The basic conformance statement is defined in Table A.1.

Table A.1 – Basic conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments	Client	Server
Client-Server roles						
B11	**Server** side (of TWO-PARTY-APPLICATION-ASSOCIATION)	N/A	Yes			C1
B12	**Client** side (of TWO-PARTY-APPLICATION-ASSOCIATION)	No	N/A		M	
SCSMs supported						
B21	**SCSM**: IEC 61850-8-1 used	No	Yes			
B22	**SCSM:** IEC 61850-9-1 used	N/A	N/A	Deprecated Ed2		
B23	**SCSM**: IEC 61850-9-2 used	No	No			
B24	**SCSM**: other					
Generic substation event model (GSE)						
B31	**Publisher** side	N/A	Yes			O
B32	**Subscriber** side	Yes	N/A		O	
Transmission of sampled value model (SVC)						
B41	**Publisher** side	N/A	No			O
B42	**Subscriber** side	No	N/A		O	
N/A = not applicable Yes = supported No or empty = not supported					M-Mandatory O-Optional	

3. ACSI models conformance statement

The ACSI models conformance statement is defined in Table A.2.

Table A.2 – ACSI models conformance statement

		Client/ Subscriber	Server/ Publisher	Value/ Comments	Client	Server
If **Server** side (B11) and/or **Client** side (B12) supported						
M1	**Logical device**	No	Yes		c2	c2
M2	**Logical node**	No	Yes		c3	c3
M3	**Data**	No	Yes		c4	c4
M4	**Data set**	No	Yes		c5	c5
M5	**Substitution**	No	Yes		O	O
M6	**Setting group control**	No	Yes		O	O
	Reporting					
M7	**Buffered report control**	No	Yes		O	O
M7-1	sequence-number	No	Yes			
M7-2	report-time-stamp	No	Yes			
M7-3	reason-for-inclusion	No	Yes			
M7-4	data-set-name	No	Yes			
M7-5	data-reference	No	Yes			
M7-6	buffer-overflow	No	Yes			
M7-7	entryID	No	Yes			
M7-8	BufTm	No	Yes			
M7-9	IntgPd	No	Yes			
M7-10	GI	No	Yes			
M7-11	conf-revision	No	Yes			
M8	**Unbuffered report control**	No	Yes		O	O
M8-1	sequence-number	No	Yes			
M8-2	report-time-stamp	No	Yes			
M8-3	reason-for-inclusion	No	Yes			
M8-4	data-set-name	No	Yes			
M8-5	data-reference	No	Yes			
M8-6	BufTm	No	Yes			
M8-7	IntgPd	No	Yes			
M8-8	GI	No	Yes			
M8-9	conf-revision	No	Yes			
	Logging	No	N		O	O
M9	**Log control**	No	N		O	O
M9-1	IntgPd	No	N			
M10	**Log**	No	N		O	O
M11	**Control**	No	Yes		O	O
M17	**File Transfer**	No	Yes		O	O
M18	**Application association**	No	Yes		c3	c3
M19	**GOOSE Control Block**	No	Yes		O	O
M20	**Sampled Value Control Block**	No	N		O	O

		Client/ Subscriber	Server/ Publisher	Value/ Comments	Client	Server
If **GSE** (B31/32) is supported						
M12	**GOOSE**	No	Yes		O	O
M13	**GSSE**			Deprecated Ed2	O	O
If **SVC** (B41/42) is supported						
M14	Multicast SVC	No	No		O	O
M15	Unicast SVC	No	No		O	O
For all IEDs						
M16	**Time**	No	Yes	Time source with required accuracy shall be available. Only Time Master are SNTP (Mode 4 response) time server. All other Client / Server devices require SNTP (Mode 3 request) clients	O	M
Yes = service is supported No or empty = service is not supported					c2 – shall be 'M' if support for logical-node model has been declared. c3 – shall be 'M' if support for data model has been declared. c4 – shall be 'M' if support for data-set, Substitution, Report, Log Control, or Time model has been declared. c5 – shall be 'M' if support for Report, GSE, or SV models has been declared. M – Mandatory O – Optional	

4. ACSI service conformance statement

The ACSI service conformance statement is defined in Table A.4 (depending on the statements in Table A.1 and in Table A.2).

Table A.3 – ACSI service Conformance statement

	Ed.	Services	AA: TP/MC	Client (C)	Server (S)	Comments	Client	Server
Server								
S1	1,2	GetServerDirectory (LOGICAL-DEVICE)	TP	No	Y		O	c12
							c12 - Mandatory if B11=Yes	
Application association								
S2-1	1,2	Associate_Request		No	Yes		M	O
S2-2		Associate_Response		No	Yes		O	M
S3-1	1,2	Abort_Request		No	Yes		c11	M
S3-2		Abort_Processing		No	Yes		M	M
S4-1		Release_Request		No	Yes		c11	O
S4-2	1,2	Release_Responde		No	Yes		M	M
		c11 – Either the Abort or the Release request shall be supported by the client. Additionaly, the client must understand the abort request delivered by the server.						
Logical device								
S5	1,2	GetLogicalDeviceDirectory	TP	No	Yes		O	c12
							c12 - Mandatory if B11=Yes	
Logical node								
S6	1,2	GetLogicalNodeDirectory	TP	No	Yes		O	c12
S7	1,2	GetAllDataValues	TP	No	Yes		O	M
							c12 - Mandatory if B11=Yes	
Data								
S8	1,2	GetDataValues	TP	No	Yes		O	M
S9	1,2	SetDataValues	TP	No	Yes		O	O
S10	1,2	GetDataDirectory	TP	No	Yes		O	M
S11	1,2	GetDataDefinition	TP	No	Yes		O	M
Data set								
S12	1,2	GetDataSetValues	TP	No	Yes		O	M
S13	1,2	SetDataSetValues	TP	No	No		O	O
S14	1,2	CreateDataSet	TP	No	No		O	O
S15	1,2	DeleteDataSet	TP	No	No		O	O
S16	1,2	GetDataSetDirectory	TP	No	Yes		O	M
Substitution								
S17	1	SetDataValues	TP	No	Yes		M	M
Setting group control								
S18	1,2	SelectActiveSG	TP	No	Yes		M	M
S19	1,2	SelectEditSG	TP	No	Yes		O	O
S20	1,2	SetEditSGValues	TP	No	Yes		O	O
S21	1,2	ConfirmEditSGValues	TP	No	Yes		O	O
S22	1,2	GetEditSGValues	TP	No	Yes		O	O
S23	1,2	GetSGCBValues	TP	No	Yes		O	M

	Ed.	Services	AA: TP/MC	Client (C)	Server (S)	Comments	Client	Server
Reporting								
Buffered report control block (BRCB)								
S24	1,2	Report	TP	No	Yes		c6	c6
S24-1	1,2	data-change (dchg)		No	Yes		-	M
S24-2	1,2	quality-change (qchg)		No	Yes		-	M
S24-3	1,2	data-update (dupd)		No	No		-	M
S25	1,2	GetBRCBValues	TP	No	Yes		c6	c6
S26	1,2	SetBRCBValues	TP	No	Yes		c6	c6
Unbuffered report control block (URCB)								
S27	1,2	Report	TP	No	Yes		c6	c6
S27-1	1,2	data-change (dchg)		No	Yes		-	M
S27-2	1,2	quality-change (qchg)		No	Yes		-	M
S27-3	1,2	data-update (dupd)		No	No		-	M
S28	1,2	GetURCBValues	TP	No	Yes		c6	c6
S29	1,2	SetURCBValues	TP	No	Yes		c6	c6

c6 – shall declare support for at least one (BRCB or URCB)

Logging								
Log control block								
S30	1,2	GetLCBValues	TP	No	No		M	M
S31	1,2	SetLCBValues	TP	No	No		O	M
Log								
S32	1,2	QueryLogByTime	TP	No	No		c7	M
S33	1,2	QueryLogAfter	TP	No	No		c7	M
S34	1,2	GetLogStatusValues	TP	No	No		M	M

c7 – shall declare support for at least one (QueryLogByTime or QueryLogAfter).

Generic substation event model (GSE)								
GOOSE								
S35	1,2	SendGOOSEMessage	MC	No	Yes		c8	c8
GOOSE-CONTROL-BLOCK								
S36	1,2	GetGoReference	TP	No	No		O	O
S37	1,2	GetGOOSEElementNumber	TP	No	No		O	O
S38	1,2	GetGoCBValues	TP	No	Yes		O	O
S39	1,2	SetGoCBValues	TP	No	Yes		O	O
GSSE								
S40	1	SendGSSEMessage	MC			Deprecated in Edition 2	c8	c8
GSSE-CONTROL-BLOCK								
S41	1	GetReference	TP			Deprecated in Edition 2	O	O
S42	1	GetGSSEElementNumber	TP			Deprecated in Edition 2	O	O
S43	1	GetGsCBValues	TP			Deprecated in Edition 2	O	O
S44	1	SetGsCBValues	TP			Deprecated in Edition 2	O	O

c8 – shall declare support for at least one (SendGOOSEMessage or SendGSSEMessage

	Ed.	Services	AA: TP/MC	Client (C)	Server (S)	Comments	Client	Server
Transmission of sampled value model (SVC)								
Multicast SV								
S45	1,2	SendMSVMessage	MC	No	No		c10	c10
Multicast Sampled Value Control Block								
S46	1,2	GetMSVCBValues	TP	No	No		O	O
S47	1,2	SetMSVCBValues	TP	No	No		O	O
Unicast SV								
S48	1,2	SendUSVMessage	TP	No	No		c10	c10
Unicast Sampled Value Control Block								
S49	1,2	GetUSVCBValues	TP	No	No		O	O
S50	1,2	SetUSVCBValues	TP	No	No		O	O

c10 – shall declare support for at least one (SendMSVMessage or SendUSVMessage).

Control								
S51	1,2	Select		No	Yes		M	O
S52	1,2	SelectWithValue	TP	No	Yes		M	O
S53	1,2	Cancel	TP	No	Yes		O	c13
S54	1,2	Operate	TP	No	Yes		M	M
S55	1,2	CommandTermination	TP	No	Yes		M	O
S56	1,2	TimeActivatedOperate	TP	No	No		O	O

c13 – shall declare support if either S51 (Select) or S52 (SelectWithValue) is Y.

File Transfer								
S57	1,2	GetFile	TP	No	Yes		M	M
S58	1,2	SetFile	TP	No	Yes		O	O
S59	1,2	DeleteFile	TP	No	No		O	O
S60	1,2	GetFileAttributeValues	TP	No	Yes		O	M
S61	1,2	GetServerDirectory (FILE-SYSTEM)	TP	No	Yes		M	M

Time								
T1	1,2	Time resolution of internal clock		xx	10 (1ms)	Nearest negative power of 2^{-n} in seconds (number 0 .. 24)		
T2	1,2	Time accuracy of internal clock		Tx	T1	TL (ms) (low accuracy), T3 < 7) T0 (ms) (<= 10 ms), 7 <= T3 < 10 T1 (µs) (<= 1 ms), 10 <= T3 < 13 T2 (µs) (<= 100 µS), 13 <= T3 < 15 T3 (µs) (<= 25 µS), 15 <= T3 < 18 T4 (µs) (<= 25 µS), 15 <= T3 < 18 T5 (µs) (<= 1 µS), T3 >= 20		
T3	1,2	Supported TimeStamp resolution	-	xx	10	Nearest value of 2^{-n} in seconds (number 0 .. 24)		
N/A = not applicable Yes = supported No or empty = not supported								

5. 61869-9 Communication Profile conformance statement

The A-Profile conformance statement shall be as defined in Table 912.

Table 912 – PICS for A-Profile support: 61869-9

	Ed.	Services	Client (C)	Server (S)	Comments	Conformance Classes			
						a	b	c	d
A0	2	Conformance class supported	No	No		a=only SV, b=+GOOSE, c=+MMS, d=+reports			
A1	2	Client/Server A-Profile	No	No		-	-	M	M
A2	2	GOOSE mgmt A-Profile	No	No		-	M	M	M
A3	2	GOOSE A-Profile	No	No		-	M	M	M
A4	2	TimeSync A-Profile	No	No		N1	N1	N1	N1
A5	2	Security for client/server A-Profile	No	No		-	-	-	-
A6	2	Security for GOOSE/GSE mgmt A-Profile	No	No		-	-	-	-
A7	2	SV A-Profile per IEC 61850-9-2:2011	No	No		M	M	M	M

The T-Profile conformance statement shall be as defined in Table 913.

Table 913 – PICS for T-Profile support: 61869-9

	Ed.	Services	Client (C)	Server (S)	Comments	Conformance Classes			
						a	b	c	d
T1	2	TCP/IP T-Profile per IEC 61850-8-1	No	No		-	-	M	M
T2	2	SV T-Profile per IEC 61850-9-2	No	No		M	M	M	M
T3	2	GOOSE T-Profile per IEC 61850-8-1	No	No		-	M	M	M
T4	2	GSSE T-Profile	No	No		-	-	-	-
T5	2	TimeSync T-Profile per IEC 61850-8-1	No	No		-	-	O	O

6. 61850-9-3 Clock Profile conformance statement

The capabilities and options supported by the PTP clock is shown in Table 22.

Table 22 – PICS for Clocks ~~A-Profile support~~: 61850-9-3

PICS proforma reference	Ed.	Capability	Client (C)	Server (S)	Comments	Value Range	Base	Condition	Example
CLOCK_TYPE_OC	2	clock is OC according to this base	Y	N		Y/N	M	c.1	Y
CLOCK_TYPE_TC	2	clock is TC according to this base	Y	N		Y/N	M	c.1	
CLOCK_TYPE_BC	2	clock is BC according to this base	N	N		Y/N	M	c.1	
NR_PORTS	2	number of clock ports (total)	2/4	N		Int>0	M	-	2
PORTS_STEP	2	1: all ports support 1-step on egress 2: all ports support 2-step on egress 3: all ports support both 1-step and 2	2	N		1.3	M	-	{1}
SLAVE_ONLY	2	all ports of the clock are slave-only	N	N		Y/N	M	c.2	
TIME_TRACEABLE	2	connectable to a time reference outside of PTP (e.g. GPS)	Y	N		Y/N	M	c.3	Y
FREQ_TRACEABLE	2	connectable to a frequency reference outside of PTP (e.g. GPS)	Y	N		Y/N	M	c.3	Y
DAC	2	doubly attached OC	Y	N		Y/N	O		Y
PORTS_PAIRED	2	paired clock ports for redundancy (e.g. {3-4})	{1-2},{3-4}	N		Port pair	O	c.4	Y
REDBOX_DATC	2	Redbox as Transparent Clock	N	N		Y/N	O	c.5	{0,1}
REDBOX_SLTC	2	Redbox as Stateless Transparent Clock	N	N		Y/N	O	c.5	
REDBOX_TWBC	2	Redbox as three-way Boundary Clock	N	N		Y/N	O	c.6	
REDBOX_DABC	2	Redbox as DAC BC	N	N		Y/N	O	c.6	
MIB_SNMP	2	supports MIB of IEC 62439-3 Annex E	N	N		Y/N	M	c.7	
MIB_61850	2	supports IEC 61859-90-4 Clock Objects	Y	N		Y/N	M	c.7	
MIB_OTHER	2	clock supports fixed values or a mechanism defined by the manufacturer. (If True, this list is appended to this PICS)	N	N		Y/N	M	c.7	Y, void list
ATOI	2	A master clock attaches the ALTERNATE_TIME_OFFSET_INDICATOR TLV as defined in IEC 61588 as set by its application. A slave clock makes this TLV information available to the application if it receives it. A BC forwards the ATOI TLV from the slave port to the master ports	N	N		Y/N	O	-	N
						c.1: at least one shall be supported (CLOCK_TYPE_OC and CLOCK_TYPE_TC may be both True) c.2: only if CLOCK_TYPE_OC = True c.3: only if SLAVE_ONLY = False c.4: shall be "m" (>1) if DAC = True c.5: support shall only be declared if CLOCK_TYPE_TC = True and DAC=True c.6: support shall only be declared if CLOCK_TYPE_BC = True and DAC=True c.7: at least one shall be supported			

Protocol Implementation eXtra Information for Testing (PIXIT) for the IEC 61850 Edition 2 server interface in IRF/IDF/ZLF/DLF/RTF from ZIV Aplicaciones y Tecnología

Version 0.0, Date: 15/05/2021

Based Upon UCAIug Server PIXIT Template version 20

UCA International Users Group
Testing Sub Committee

PIXIT template for Server Test Procedures
for Edition 1 and Edition 2
Revision 20

Date: July 02, 2020

PIXIT for server

Introduction

This document specifies the protocol implementation extra information for testing (PIXIT) of the IEC 61850 interface in IRF/IDF/ZLF/DLF/RTF with firmware version 0.10.0.

Together with the PICS and the MICS the PIXIT forms the basis for a conformance test according to IEC 61850-10. The PIXIT entries contain information, which is not available in the PICS, MICS, TICS documents or SCL file.

Each table specifies the PIXIT for applicable ACSI service model as structured in IEC 61850-10. The “Ed” column indicates if the entry is applicable for IEC 61850 Edition 1 and/or Edition 2. A hyphen (“-“) in the Ed column indicates the PIXIT entry is not applicable for any version.

PIXIT for Documentation

ID	Ed	Description	Value / Clarification
Do1	2	How to expose required firmware versions not present in the datamodel	

PIXIT for Association model

ID	Ed	Description	Value / Clarification
As1	1	Maximum number of clients that can set-up an association simultaneously	10
As2	1,2	TCP_KEEPALIVE value. The recommended range is 1..20s	Configurable 20 seconds by default
As3	1,2	Lost connection detection time	Configurable: number of retries and time between retries 40 seconds by default
As4	-	Authentication is not supported yet	
As5	1,2	What association parameters are necessary for successful association Called values: Calling values:	Transport selector N Session selector N Presentation selector N AP Title N AE Qualifier N other Transport selector N Session selector N Presentation selector N AP Title N AE Qualifier N other
As6	1,2	If association parameters are necessary for association, describe the correct values e.g.	Association parameters are not necessary for association

ID	Ed	Description	Value / Clarification
As7	1,2	What is the maximum and minimum MMS PDU size	Max MMS PDU size 65000 Min MMS PDU size Is determined by the size of the request.
As8	1,2	What is the maximum start up time after a power supply interrupt	50 seconds in normal situation (when no control configuration needs to be loaded)
As9	1,2	Does this device function only as test equipment? (test equipment need not have a non-volatile configuration; but it cannot be part of the substation automation system)	No. It has non-volatile configuration.

PIXIT for Server model

ID	Ed	Description	Value / Clarification
Sr1	1,2	Which analogue value (MX) quality bits are supported (can be set by server)	Validity: Y Good, Y Invalid, N Reserved, Y Questionable Detail Quality: Y Overflow Y OutofRange Y BadReference Y Oscillatory Y Failure Y OldData Y Inconsistent Y Inaccurate Miscellaneous: Y Source Y Test N OperatorBlocked If no user configuration is done, by default the measurements support: OutOfRange and OldData.

ID	Ed	Description	Value / Clarification
Sr2	1,2	Which status value (ST) quality bits are supported (can be set by server)	Validity: Y Good, Y Invalid, N Reserved, Y Questionable Detail Quality Y BadReference Y Oscillatory Y Failure Y OldData Y Inconsistent Y Inaccurate Miscellaneous: Y Source Y Test N OperatorBlocked If no user configuration is done, by default the signals support: Oscillatory, Failure and OldData.
Sr3	-	What is the maximum number of data object references in one GetDataValues request	Deprecated
Sr4	-	What is the maximum number of data object references in one SetDataValues request	Deprecated
Sr5	1	Which Mode values are supported [1]	On Y [On-]Blocked Y Test Y Test/Blocked Y Off Y The supported Mode values are indicated by using different enumeration types for each case. Control LNs (CSWI, GAPC…) just support On and Test.

[1] IEC 61850-6:2009 clause 9.5.6 states that if only a subrange of the enumeration value set is supported, this shall be indicated within an ICD file by an enumeration type, where the unsupported values are missing

PIXIT for Data set model

ID	Ed	Description	Value / Clarification
Ds1	1	What is the maximum number of data elements in one data set (compare ICD setting)	Fixed in ICD to 500
Ds2	1	How many persistent data sets can be created by one or more clients (this number includes predefined datasets)	0
Ds3	1	How many non-persistent data sets can be created by one or more clients	0

PIXIT for Substitution model

ID	Ed	Description	Value / Clarification
Sb1	1	Are substituted values stored in volatile memory	Yes

PIXIT for Setting group control model

ID	Ed	Description	Value / Clarification
Sg1	1	What is the number of supported setting groups for each logical device	8
Sg2	1,2	What is the effect of when and how the non-volatile storage is updated (compare IEC 61850-8-1 $16.2.4)	If values are updated in a CID, these changes take effect after starting up. If values are updated by MMS services, these changes take effect immediately
Sg3	1	Can multiple clients edit the same setting group	N
Sg4	1	What happens if the association is lost while editing a setting group	The EditSG is reset to 0
Sg5	1	Is EditSG value 0 allowed	Y
Sg6	2	When ResvTms is not present how long is an edit setting group locked	ResvTms is present. Its default value is 3600 seconds

PIXIT for Reporting model

ID	Ed	Description	Value / Clarification
Rp1	1	The supported trigger conditions are (compare PICS)	integrity Y data change Y quality change Y data update N general interrogation Y
Rp2	1	The supported optional fields are	sequence-number Y report-time-stamp Y reason-for-inclusion Y data-set-name Y data-reference Y buffer-overflow Y entryID Y conf-rev Y segmentation Y
Rp3	1,2	Can the server send segmented reports (when not supported, it is allowed to refuse an association with a PDU smaller than the supported minimum PDU size)	Y
Rp4	1,2	Mechanism on second internal data change notification of the same analogue data value within buffer period (Compare IEC 61850-7-2 Ed2 $17.2.2.9)	The DUT behaves as if BufTm has expired and sends the report immediately, restarts the timer with BufTm value and processes the second change
Rp5	1	Multi client URCB approach (compare IEC 61850-7-2:2003 $14.2.1)	Each URCB is visible to all clients
Rp6	-	What is the format of EntryID	Deprecated
Rp7	1,2	What is the buffer size for each BRCB or how many reports can be buffered	30 Kbytes
Rp8	-	Pre-configured RCB attributes that are dynamic, compare SCL report settings	Deprecated
Rp9	1	May the reported data set contain: - structured data objects - data attributes	 Y Y
Rp10	1,2	What is the scan cycle for binary events Is this fixed, configurable	2 ms Fixed
Rp11	1	Does the device support to pre-assign a RCB to a specific client in the SCL	Y

ID	Ed	Description	Value / Clarification
Rp12	2	After restart of the server is the value of ConfRev restored from the original configuration or retained prior to restart	Restored from original CID configuration
Rp13	1,2	Does the server accept any client to configure/enable a BRCB with ResvTms=-1? What fields are used to do the identification?	N Client's IP Address
Rp14	2	When BRCB.ResvTms is exposed, what is default value for BRCB.ResvTms if client does not write (must be > 0) or When BRCB.ResvTms is not exposed, what is the internal reservation time (must be >= 0)	10 seconds N/A
Rp15	2	Is data model db=0 supported	Yes
Rp16	1,2	Each RCB should be configured with a different Data Set. In case of configuring the same Data Set in different RCBs those RCBs must be configured with the same trigger options and integrity period.	

PIXIT for Logging model

ID	Ed	Description	Value / Clarification
Lg1	1,2	What is the default value of LogEna (Compare IEC 61850-8-1 $17.3.3.2.1, the default value should be FALSE)	FALSE
Lg2	-	What is the format of EntryID	Deprecated
Lg3	1,2	Are there are multiple Log Control Blocks that specify the Journaling of the same MMS NamedVariable and TrgOps and the Event Condition (Compare IEC 61850-8-1 $17.3.3.3.2)	Single Journal Entry
Lg4	1	Pre-configured LCB attributes that cannot be changed online	Deprecated, the information is already available in SCL
Lg5		Which TrgOps are supported for logging (note Ed2 and up requires support for all TrgOps)	data change Y quality change Y data update N integrity Y

PIXIT for GOOSE publish model

ID	Ed	Description	Value / Clarification
Gp1	1,2	Can the test (Ed1) / simulation (Ed2) flag in the published GOOSE be set	Y
Gp2	1	What is the behaviour when the GOOSE publish configuration is incorrect	If goose pdu is too large NdsCom=True and DUT keeps GoEna=False If no DatSet is configured NdsCom=True and DUT keeps GoEna=False CIDs with incorrect goose publish configuration are rejected
Gp3	1,2	Published FCD supported common data classes are	Any FCD with FC=ST/MX/SP Arrays are not supported
Gp4	1,2	What is the slow retransmission time Is it fixed or configurable	Max value: 2.147.483.647 ms Configured by GoCB MaxTime Default value: 2000 ms
Gp5	1,2	What is the fastest retransmission time Is it fixed or configurable	Min value: 2ms Configured by GoCB MinTime Default value: 2ms
Gp6	-	Can the GOOSE publish be turned on / off by using SetGoCBValues(GoEna)	Deprecated See PICS - SetGoCBValues
Gp7	1,2	What is the initial GOOSE sqNum after restart	1
Gp8	1	May the GOOSE data set contain: - structured data objects (FCD) - timestamp data attributes	 Y Y
Gp9	1,2	Does Server or ICT refuse GOOSE payload dataset length greater than SCSM supports?	No

PIXIT for GOOSE subscribe model

ID	Ed	Description	Value / Clarification
Gs1	1,2	What elements of a subscribed GOOSE message are checked to decide the message is valid and the allData values are accepted? If yes, describe the conditions. Notes: • the VLAN tag may be removed by a ethernet switch and shall not be checked • the simulation flag shall always be checked (Ed2)	Y destination MAC address Y APPID Y gocbRef Y timeAllowedtoLive Y datSet Y goID N t Y stNum Y sqNum Y simulation / test Y confRev Y ndsCom Y numDatSetEntries sqNum greater than expected: Not detected (check Gs4) sqNum less than expected: Detected Data-type mismatch in data set elements: Detected N out-of-order dataset members When Y (except datSet, confRev, simulation, ndsCom and numDatSetEntries): the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the GOOSE message indicating it by changing the quality (questionable-old data). When receiving a subscribed GOOSE with the simulate bit or the ndsCom flag activated or an incorrect dataset or confRev, the DUT will discard the GOOSE message without indicating it by changing the quality. In these cases, as soon as received a subscribed GOOSE with a data value change, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the message indicating it by changing the quality (questionable-old data).

ID	Ed	Description	Value / Clarification
			When receiving a subscribed GOOSE with numDatSetEntries less than expected or data-type mismatch, the DUT will discard the GOOSE message without indicating it by changing the quality. In these cases, as soon as received a subscribed GOOSE with a data value change, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and the DUT will discard the GOOSE message indicating it by changing the quality (invalid). When receiving a subscribed GOOSE with an incorrect confRev, the DUT will use the latest value received when the goose was correct before identifying that the new subscription data is invalid and immediatly the DUT will discard the GOOSE message indicating it by changing the quality (invalid).
Gs2	1,2	When is a subscribed GOOSE marked as lost (TAL = time allowed to live value from the last received GOOSE message)	Message does not arrive prior to TAL
Gs3	1,2	What is the behaviour when one or more subscribed GOOSE messages isn't received or syntactically incorrect (missing GOOSE)	If the TAL is expired the quality of the attribute in the database will be set to Questionable and Old Data and it will keep the last received value

ID	Ed	Description	Value / Clarification
Gs4	1,2	What is the behaviour when a subscribed GOOSE message is out-of-order	To protect the system against out-of-order GOOSE messages the IED uses a combination of TAL and a time association setting (LPHD1.GoAsLosTms). The time used to invalidate one association will be the biggest one between them. By default, LPHD1.GoAsLosTms=10 seconds. While one association is in active status, the IED will only accept GOOSE messages where stNum+sqNum are incrementing (integer of 32 bits). If the increment is bigger than 2^31, the GOOSE is discarded and the IED will wait to receive a correct GOOSE message inside the TAL. If no GOOSE message arrives, then the IED sets the quality to questionable-old data. Once the IED has marked one GOOSE as lost, it will wait for the association time to reactivate the subscription accepting the first GOOSE (stNum+sqNum) that arrives and using those values as the new reference.
Gs5	1,2	What is the behaviour when a subscribed GOOSE message is duplicated	The DUT ignores the duplicated message.
Gs6	1	Does the device subscribe to GOOSE messages with/without the VLAN tag	Y, with the VLAN tag Y, without the VLAN tag
Gs7	1	May the GOOSE data set contain: - structured data objects (FCD) - timestamp data attributes	 Y N
Gs8	1,2	Subscribed FCD supported common data classes are	SPS, DPS, INS, ENS, ACT, ACD, SEC, MV, CMV, WYE, DEL, SPC, DPC, INC, ENC, BSC, ISC, APC, BAC, SPG, ING, ENG, ASG, CURVE, CSG. Arrays are not supported

ID	Ed	Description	Value / Clarification
Gs9	1,2	Are subscribed GOOSE with test=T (Ed1) / simulation=T (Ed2) accepted in test/simulation mode	Y
Gs10	1,2	Max number of dataset members	Unlimited
Gs11	1	Is Fixed-length encoded GOOSE supported	No
Gs12	1	Is IEC 62351-6 security supported	No

PIXIT for GOOSE performance

ID	Ed	Description	Value / Clarification	
Gf1	1,2	Performance class	P1 = 3ms	
Gf2	1,2	GOOSE ping-pong processing method	¿? Event driven based OR SCAN CYCLE BASED	
Gf3	1,2	Application logic scan cycle (ms)	Max	20ms
			Min	2ms
Gf4	1	Maximum number of data attributes in GOOSE dataset (value and quality has to be counted as separate attributes)	Maximum number of 1265 bytes. (Around 421 DAs if they are stVal)	

PIXIT for Control model

ID	Ed	Description	Value / Clarification
Ct1	1	What control models are supported (compare ICD file enums for Ed2)	DOns: Y SBOns: Y DOes: Y SBOes: Y
Ct2	1,2	Is the control model fixed, configurable and/or dynamic	Dynamic
Ct3	-	Is TimeActivatedOperate supported (compare PICS or SCL)	Deprecated
Ct4	-	Is “operate-many” supported (compare sboClass)	Deprecated, see sboClass in datamodel (ICD)
Ct5	1	Will the DUT activate the control output when the test attribute is set in the SelectWithValue and/or Operate request (when N test procedure Ctl2 is applicable)	N
Ct6	-	What are the conditions for the time (T) attribute in the SelectWithValue and/or Operate request	Deprecated
Ct7	-	Is pulse configuration supported (compare pulseConfig)	Deprecated

ID	Ed	Description	Value / Clarification
Ct8	1	What is the behaviour of the DUT when the check conditions are set Is this behaviour fixed, configurable, online changeable	N synchrocheck Y interlock-check DUT ignores synchrocheck value. DUT uses interlock-check to perform or not the check. Fixed
Ct9	1,2	Which additional cause diagnosis are supported	Y Unknown Y Not-supported Y Blocked-by-switching-hierarchy Y Select-failed Y Invalid-position Y Position-reached Y Step-limit (just in RTF model) Y Blocked-by-Mode Y Blocked-by-process Y Blocked-by-interlocking N Blocked-by-synchrocheck Y Command-already-in-execution N Blocked-by-health Y 1-of-n-control N Abortion-by-cancel N Time-limit-over N Abortion-by-trip Y Object-not-selected **Edition 1 specific values:** N Parameter-change-in-execution (PCIE Ed1 semantics) **Edition 2 specific values:** Y Object-already-selected N No-access-authority N Ended-with-overshoot N Abortion-due-to-deviation N Abortion-by-communication-loss N Blocked-by-command N None Y Inconsistent-parameters Y Locked-by-other-client N Parameter-change-in-execution (PCIE Ed2 semantics)

ID	Ed	Description	Value / Clarification
Ct10	1,2	How to force a “test-not-ok” respond with SelectWithValue request	Invalid orCat value, orCat >= 9
Ct11	1,2	How to force a “test-not-ok” respond with Select request	The control is selected
Ct12	1,2	How to force a “test-not-ok” respond with Operate request	Invalid orCat value, orCat >= 9 DOns, SBOns, DOes: Operate value and actual position are the same SBOes: Operate values are different than selected
Ct13	1,2	Which origin categories are supported / accepted	Y bay-control Y station-control Y remote-control N automatic-bay Y automatic-station Y automatic-remote Y maintenance Y process
Ct14	1,2	What happens if the orCat value is not supported or invalid	DOns: command rejected SBOns: command rejected DOes: command rejected SBOes: command rejected The DUT sends reponse– with AccessResult=Object_access_denied and it sends, for enhanced security, CommandTermination with AddCause= Not-supported
Ct15	1,2	Does the IED accept a SelectWithValue / Operate with the same control value as the current status value Is this behaviour configurable	DOns: N SBOns: N DOes: N SBOes: Y/N Configurable N The DUT sends reponse– with AccessResult=Object_access_denied and it sends, for enhanced security, CommandTermination with AddCause= Position-reached

ID	Ed	Description	Value / Clarification
Ct16	1,2	Does the IED accept a select/operate on the same control object from 2 different clients at the same time	DOns: N SBOns: N DOes: N SBOes: N The DUT sends reponse– with AccessResult=temporarily-unavailable and it sends, for enhanced security, CommandTermination with AddCause= Object-already-selected / Command-already-in-execution
Ct17	1	Does the IED accept a Select/SelectWithValue from the same client when the control object is already selected (Tissue #334)	SBOns: N SBOes: N
Ct18	1,2	Is for SBOes the internal validation performed during the SelectWithValue and/or Operate step	The validation is performed during the Operate step
Ct19	-	Can a control operation be blocked by Mod=Off or [On-]Blocked (Compare PIXIT-Sr5)	Deprecated
Ct20	1,2	Does the IED support local / remote operation	Y
Ct21	1,2	Does the IED send an InformationReport with LastApplError as part of the Operate response-for control with normal security	SBOns: N DOns: N
Ct22	2	How to force a “parameter-change-in-execution”	N/A
Ct23	1,2	How many SBOns/SBOes control objects can be selected at the same time?	SBOns: multiple SBOes: multiple
Ct24	1,2	Can a controllable object be forced to keep its old state e.g. Internal Controllable Objects may not be accessible to force this, whereas a switch like Circuit Breaker outside the DUT can?	Y
Ct25	1,2	When CDC=DPC is supported, is it possible to have DPC (Controllable Double Point) go to the intermediate state? (00)	Y
Ct26	1,2	Name a DOes point (if any) with a finite operate timeout and specify the timeout (in milliseconds)	CTRL/CSWI1.Pos Timeout is configurable
Ct27	2	Does the IED support control objects with external signals?	DOns: Y SBOns: Y DOes: Y SBOes: Y

PIXIT for Time synchronisation model

ID	Ed	Description	Value / Clarification
Tm1	1	What time quality bits are supported (may be set by the IED)	Y LeapSecondsKnown N ClockFailure Y ClockNotSynchronized
Tm2	1,2	Describe the behaviour when the time server(s) ceases to respond What is the time server lost detection time	Wait for a configurable number of connection retries (unicast mode) or wait a configurable period of time (multicast mode). After that "Clock-not-synchronized" will be set. Configurable. Tested value: 10 seconds after the first request send to the time server without response.
Tm3	1,2	How long does it take to take over the new time from time server	Configurable Tested value: as soon as the new time from the time server is received.
Tm4	1,2	When is the time quality bit "ClockFailure" set	N/A
Tm5	1,2	When is the time quality bit "Clock not Synchronized" set	When connection to all time servers are lost (see PIXIT-Tm2)
Tm6	-	Is the timestamp of a binary event adjusted to the configured scan cycle	Deprecated
Tm7	1	Does the device support time zone and daylight saving	Y
Tm8	1,2	Which attributes of the SNTP response packet are validated	Y Leap indicator not equal to 3 N Mode is equal to SERVER N OriginateTimestamp is equal to value sent by the SNTP client as Transmit Timestamp N RX/TX timestamp fields are checked for reasonableness Y SNTP version 3 and/or 4 N other (describe)
Tm9	1,2	Do the COMTRADE files have local time or UTC time and is this configurable	Local Time Not configurable

PIXIT for File transfer model

ID	Ed	Description	Value / Clarification
Ft1	1	What is structure of files and directories Where are the COMTRADE files stored Are comtrade files zipped and what files are included in each zip file	/COMTRADE/ /SCL/active/ /SCL/notvalidated /SYSTEMLOG/ /COMTRADE/ Not zipped
Ft2	1,2	Directory names are separated from the file name by	"/"
Ft3	1	The maximum file name size including path (recommended 64 chars)	255 chars
Ft4	1,2	Are directory/file name case sensitive	Case sensitive
Ft5	1,2	Maximum file size for SetFile	N/A
Ft6	1	Is the requested file path included in the MMS fileDirectory respond file name	(Ed2: always complete path)
Ft7	1	Is the wild char supported MMS fileDirectory request	No
Ft8	1,2	Is it allowed that 2 clients get a file at the same time	Y same file Y different files
Ft9	1,2	Which files can be deleted	N/A

TISSUES Implementation Conformance Statement for the IEC 61850 Ed2 interface in IRF/IDF/ZLF/DLF/RTF

Version 0.0, Date: 15/05/2021

UCA International Users Group
Testing Sub Committee

TICS Template Ed2 for TPCL 1.2.6

Introduction

This document provides a template for the Tissues conformance statement. According to the UCA IUG QAP the Tissue conformance statement is required to perform a conformance test and is referenced on the certificate.

This document is applicable for IRF/IDF/ZLF/DLF/RTF with firmware version 0.10.0.

Mandatory Edition 2 Tissues

Below tables give an overview of the applicable mandatory Tissues.
Items in *italic* are brief interpretations provided by the UCA International Users Group to aid in interpretation and is not normative.
The original TISSUE should be consulted for details of changes.

Part 6 Tissue	Description	Implemented Y/na
658	Tracking related features *EntryID and CST missing, these are checked by schema*	Y
1324	FCDA element cannot be a "functionally constrained logical node" *doName now mandatory in FCDA element, SCT: refuse to make empty doName? ICT: Refuse SCD*	Y
668	Autotransformer modeling *Autotransformer model in substation section has changed*	Y
687	SGCB ResvTms *SettingControl has added attribute resvTms see also TISSUE 845*	Y
719	ConfDataSet - maxAttributes definition is confusing *maxAttributes now means max count of FCDA in dataset*	Y
721	Log element name *LN0/Log now has optional attribute "name"*	Y
768	bType VisString65 is missing *VisString65 added as SCL BasicType*	na
779	object references *"@" as first character in object references now allowed*	Y
788	SICS S56 from optional to mandatory *SICS S56="Interpret IED capabilities and prohibit unsupported usage"*	na
789	ConfLdName as services applies to both server and client *Many changes made to Services section*	Y
804	valKind and IED versus System configuration *valImport missing/false DAI means ICT shall ignore value in SCD and SCT shall not change from ICD/IID value. Instance section inherits from DA/BDA element.*	Y
806	Max length of log name inconsistent between -6 and -7-2 *LogControl.logName and Log.name restricted to 32 chars*	Y
807	Need a way to indicate if "Owner" present in RCB *Services/ReportSettings@owner added*	Y
823	ValKind for structured data attributes *valKind is prohibited on structured attributes*	Y

Part 6 Tissue	Description	Implemented Y/na
824	Short addresses on structured data attributes *sAddr is now allowed for structured attributes*	Y
825	Floating point value *Server shall support <Val> with exponential notation*	Y
845	SGCB ResvTms *Services/SettingGroups/SGEdit added attribute resvTms Services/SettingGroups/ConfSG added attribute resvTms See also TISSUE 687*	Y
853	SBO and ProtNs *DA[@name=SBO] element shall have ProtNS element*	Y
855	Recursive SubFunction *Substation section extension must be tolerated*	na
856	VoltageLevel frequency and phases *Substation section extension must be tolerated*	na
857	Function/SubFunction for ConductingEquipment *Substation section extension must be tolerated*	na
886	Missing 8-1 P-types *"tP_IP_UDP_PORT" and "tP_IP_TCP_PORT" added*	na
901	tServices as AP or as IED element *Rules for contents of AP/Server/Services are now defined*	Y
936	SupSubscription parameter usage is difficult *SupSubscription "max" replaced by "maxGo" and "maxSv"*	Y
1147	tServices - FileHandling not consistent with -7-2 *Services/FileHandling now means only support for GetFile and GetFileAttributeValues and NOT SetFile/DeleteFile*	Y
1185	Valkind value Conf for EX FC data *valKind=Conf is allowed for dataNs*	N
1284	SCSM mapping may require a communication section in an ICD file *Server IEDs supporting client/server associations to 61850-8-1 shall include a <Communication> section*	Y
1328	Limitation on the size of data type templates identifiers *Identifer now limited to 255 characters*	N
1395	Client LN attributes *ReportControl/RptEnabled/ClientLN@ldInst shall be "LD0" for pure clients (without any Logical Devices)*	Na
1402	ExtRef during engineering *an ExtRef.intAddr attribute value unequal to empty string (prescribed or filled by the IED tool) is the flag indicating that the ExtRef shall not be deleted by the system tool. The system tool can however remove the link to the source IED* <<applicable for SCL tool test>>	Y
1415	SICS-S110 IID import mandatory for Edition2 *only the import of data model modifications and CF value changes is mandatory for system tool* <<applicable for SCL tool test>>	na
1419	Support of ldName on other IEDs *SICS I212 is now mandatory*	Y
1444	Need to support fixed and SCT controlled Datasets *Services/xxxSetttings@datSet=fix now means "data set pointed by Control Block cannot be altered from ICD/IID* value <<applicable for SCL tool test>>	na
1445	ConfReportControl and a fixed ReportSettings *Control block capabilities must be consistent <<applicable for SCL tool test>>*	Y

Part 6 Tissue	Description	Implemented Y/na
1450	originalSclXxx computation rules *Ed2 ICD/IID files specifying SCL@version=2007 SHALL include originalSCLVersion=2007 and originalSCLRevision as attributes of the <IED>element*	Y
1485	Need to supercede Tissue 1398 to clarify SCT behavior *Same as TISSUE 1450 <<applicable for SCL tool test>>*	na

Part 7-1 Tissue	Description	Implemented Y/na
828	Data model namespace revision IEC 61850-7-4:2007[A]	Y
948	Enumeration (string) values format *Enums are limited to 127 characters from Basic-Latin and Latin-1 character sets*	Y
1151	simulated GOOSE disappears after 1st appearance when LPHD.Sim = TRUE *New LGOS state machine defined, but TISSUE is not IntOp2, therefore TISSUE is optional if LGOS is used*	Y
1396	The use and configuration flow of LGOS and LSVS is unclear *If Services/SupSubscription@maxGo > 1 then at least 1 LGOS must exist. Same for maxSv/LSVS. If maxGo > count(LGOS) then SCT can create additional LGOS. Same for maxSv/LSVS*	Y
1447	Restriction on ENUMtypes in SCL *If a ENUM DA limits write or configuration to a subset, then that subset must be declared.*	Y
1457	Multiple DOI nodes with the same name. *LN can have no more than one DOI with same name.*	Y
1468	Re-use DO from other LN *allow standard or private dataNs*	Y
1491	CmdBlk blocks itself? *The data CmdBlk shall have no effect on the controllable data Mod or CmdBlk.*	na

Part 7-2 Tissue	Description	Implemented Y/na
728	BRCB: could PurgeBuf be set when RptEna=TRUE? *PurgeBuf while RptEna=true is prohibited.*	Y
778	AddCause values – add value not-supported *Align 7-2 with 8-1 (nothing new to 8-1)*	Y
780	What are unsupported trigger option at a control block? *All control blocks must support all trigger options.*	Y
783	TimOper Resp- ; add Authorization check *Clarifies Time-Operated Controls.*	Y
786	AddCause values 26 and 27 are switched *Annex B.2 has wrong AddCause values.*	Y
820	Mandatory ACSI services (use for PICS template) *Model entries M18 (Application Association), M19 (GCB), M20 (SVCB) are new. Services S17 (Substitution) and S61 (GetServerDirectory) are new. Services S1, S3, S4, S5, S6, S8, S16, S18, S23, S36, S37, S41, S42 are changed.*	Y
858	typo in enumeration ServiceType *Tracking serviceType now has GetLogicalNodeDirectory*	Y

Part 7-2 Tissue	Description	Implemented Y/na
861	dchg of ConfRev attribute *Clarifies (tracking) BTS.confRev is AFTER BRCB change.*	na
1050	GTS Phycomaddr definition in SCL *(Tracking) GTS needs a special structure for SCL.*	na
1071	Length of DO name *Private DO name length shall be <=12 including instance.*	Y
1127	Missing owner attribute in BTS and UTS *NSD files for 61850-7-3 show owner in (tracking) BTS/UTS.*	na
1202	GI not optional *GI support is mandatory for both URCB and BRCB*	Y
1232	EntryID needs clarification *Segments of a report shall have same identifiers*	Y
1242	NTS definition *NTS.resv have been added*	na
1307	Segmented report with Buffer overflow *Segments of a report shall have identical buf-overflow value*	Y
1428	MTS and NTS should use svOptFlds *MTS.optFlds and NTS.optFlds now have bType=SvOptFlds*	na
1630	Attributes in CDC=LTS do not match 8-1 definition *Order of attributes in LTS changed to: logEna, logRef, datSet, oldEntrTm, newEntrTm, oldEnt, newEnt, trgOps, intgPd*	Y

Part 7-3 Tissue	Description	Implemented Y/na
697	persistent command / PulseConfig *PulseConfig adds enum "persistent-feedback"* *DPC.cmdQual==”persistent” is conditionally allowed*	na
698	Wrong case is BAC.dB attribute *attribute renamed from "dB" to "db"*	Y
711	blkEna freeze data update while setting its quality to operaterBlocked *Mode=Blocked shall not cause q.operatorBlocked*	na
722	Units for 'h' and 'min' not in UnitKind enumeration. *New unit enums 84=hours, 85=minutes*	Y
919	Presence Condition for sVC *svC may be valKind=Conf in ICD file*	na
925	Presence of i or f attribute - Problem with writing *New constructed attribute class "AnalogueValueCtl"*	Y
926	Presence Conditions within RangeConfig *All or none of hhLim+hLim+lLim+llLim shall be present*	Y
954	Data attributes with FC=CF should have trgOp=dchg *Some INS and HST and CSG attributes missing dchg*	y
1078	CMV.t update if rangeAng changed *Add rangeAng to"reasons-to-update-timestamp-of-CMV"*	na
1565	db = 0 behaviour *db=0 not longer suppresses reporting*	Y
1578	dataAttribute NameSpace content *Attributes with FC=EX must be initialized in ICD/IID file*	Y

Part 7-4 Tissue	Description	Implemented Y/na
671	mistake in definition of Mod & Beh *Beh=on, q=test should be "Processed as valid"*	Y
674	CDC of ZRRC.LocSta is wrong *ZRRC LocSta should be CDC=SPC*	na
676	Same data object name used with different CDC *LCCH.Fer renamed to FerCh, LCCH.RedFer to RedFerCh*	Y
677	MotStr is used with different CDC in PMMS and SOPM LN classes *Rename SOPM.MotStr to MotStrNum*	na
679	Remove CycTrMod Enum *Enum is no longer used, use TrMod instead*	na
680	SI unit for MHYD.Cndct *Change unit from S/cm2 to S/m*	na
681	Enum PIDAlg *Typographical error, invalid XML syntax*	na
682	ANCR.ParColMod *ParColMod enum values text have changed*	na
683	Enum QVVR.IntrDetMth *IntrDetMth enum values text have changed*	na
685	Enum ParTraMod *ParTraMod enum values text have changed*	na
686	New annex H - enums types in XML *Many changes have been made to enumeration names*	Y
694	Data object CmdBlk *CmdBlk semantics have changed*	na
696	LSVS.St (Status of subscription) *LSVS.St is now mandatory*	na
712	interpretation of quality operatorBlocked *Mode and Behavior semantics have changed*	na
713	DO Naming of time constants in FFIL *Many DO names in FFIL have changed*	na
714	Enums for ShOpCap and SwOpCap *Type for YPSH.ShOpCap and XSWI.SwOpCap have changed*	Y
715	RBDR.ChNum1 *RBDR.ChNum1 changes from optional to conditional*	na
716	TAXD text for condition *TAXD.SmRte condition for inclusion has changed*	na
724	ANCR.Auto *ANCR.Auto changes from mandatory to optional*	Y
725	Loc in LN A-group *Loc changes to optional, LocKey/LocSta conditions change*	na
734	LLN0.OpTmh vs. LPHD.OpTmh *LLN0.OpTmh deleted, LPHD.OpTmH added as conditional*	na
736	PFSign *MMXU.PFSign enum's 1 = IEC and 2 = EEI*	na
742	GAPC.Str, GAPC.Op and GAPC.StrVal *Objects have instance indicator removed (ex, Str1 to Str)*	Y
743	CCGR.PmpCtl and CCGR.FanCtl *Object have instance indicator added (ex:PmpCtl to PmpCtl1)*	na
744	LN STMP, EEHealth and EEName *Removed STMP.EEHealth and STMP.EEName*	na
772	LPHD.PwrUp/PwrDn should be transient *These objects are now transient*	N

Part 7-4 Tissue	Description	Implemented Y/na
773	Loc, LocKey and LocSta YPSH and YLTC *Add Loc, LocKey and LocSta in YLTC and YPSH (optional)*	na
774	ITCI.LocKey *Add ITCI.LocKey as optional*	na
776	LPHD.OutOv/InOv and LCCH.OutOv/InOv *Clarified: stays true until buffer space again available*	na
800	Misspelling in CSYN *CSYN.VInvTmms renamed to CSYN.VIntvTmms*	na
802	CCGR and Harmonized control authority *Add Loc, LocKSta to every controllable LN (e.g. FSPT)*	na
808	Presence condition of ZMoT.DExt and new DOs *Change ZMOT.DExt to optional; add TotThmSt and MotSt*	na
831	Setting of ConfRevNum in LGOS *Add RxConfRevNum to LGOS and LSVS*	na
838	Testing in Beh=Blocked *Change sematic of Beh=Blocked to allow controls to be acknowledged even when LN is blocked*	na
844	MFLK.PhPiMax, MFLK.PhPiLoFil, MFLK.PhPiRoot DEL->WYE *Change these NFLK objects from cdc=DEL to cdc=WYE*	na
877	QVUB -settings should be optional	na
908	ARIS.StrSeq – transient *Change ARIS.StrSeq to transient*	na
909	Remove ANCR.ColOpR and ColOpL	na
912	Clarification of PwrRtg/VARtg *Change many DOs in YPTR, and ZGEN, see name space 2007A nsd for final result*	Y
920	Resetable Counter is NOT resetable	na
932	Rename AVCO.SptVol to AVCO.VolSpt	na
933	Presence of LCCH.RedFerCh and RedRxCnt *Change the presence condition of LCCH.RedChLiv*	na
939	Change CDC for ANCR.FixCol *Change ANCR.FixCol from APC to ASG*	na
991	LGOS: GoCBRef (as well as LSVS.SvCBRef) should be mandatory *LGOS.GoCBRef and LSVS.SvCBRef are now both mandatory*	na
1007	PTRC as fault indicator - Update of description required *PTRC.Tr and Op and Str conditional (at least 1 of group)*	na
1044	TapChg in AVCO *AVCO.TapChg is now optional*	na
1077	Rename DOnames within LTIM *LTIM.TmChgDayTm, changed to TmChgDay;* *LTIM.TmChgStdTm changed to TmChgStd*	Y
1256	New DO for LTIM to set time "manually" *Add LTIM.TmSet*	N
1331	Mod, Beh and Health with q=TEST, client can't receive their states *Mod while in Blocked will always be processed*	Y
1426	Add two DO for leap seconds in LTIM *LTIM.Leap added*	na
1456	Annex A and Mod/Beh/Health *Mod.stVal writes always igore test bits in controls*	N

Part 7-4 Tissue	Description	Implemented Y/na
1568	ISAF.AlmReset ->transient *Change ISAF.AmlReset to transient*	na

Note: Tissues 675, 735, 772, 775, 776, 878 are not relevant for conformance testing

Part 8-1 Tissue	Description	Implemented Y/na
770	GoID type mitmatch 18.1.1 and 18.1.2.5.2 *GoID string length is now 129*	Y
784	Tracking of control (CTS) *Tracking CTS has been added*	na
817	Fixed-length GOOSE float encoding *GOOSE float is encoded Tag-0x87, length=5, first octet=8*	na
827	Mandatory ACSI services (Part of 7-2 TISSUE resolution) *Change Table 111 (ServicesSupported): Add initiate, abort, and release. Change conditions for defineNamedVariables.*	Y
834	File dir name length 64 *Filename length changed from 32 to 64*	Y
951	Encoding of Owner attribute *xRCB.owner is encoded as 4 octets(IPv4) or 16 octets(IPv6)*	Y
1040	More associate error codes *3 additional associate error codes added*	Y
1178	Select Response+ is non-null value *Response to SBO read should be <CO_CtrlObjectRef>*	Y
1324	The response- for DeleteNamedVariableList is not defined *numDeleted=0; error=service/object-constraint-conflict*	na
1345	Fixed-length GOOSE ASN.1 length encoding *GOOSE publisher shall always encode minimum size legth field*	na
1441	Optonal fields in buffered reports *Writing BRCB.optFld shall not cause a purgeBuf operation*	Y
1442	Journal variableTag for ReasonCode *Example in the standard is incorrect*	Y
1453	Purge buffer on write to BRCB *PurgeBuf only occurs if different value is written*	Y
1454	Reports can be transmitted before write(RptEna=true) is confirmed	Y
1495	GetVariableAccessAttributes error code *Return MMS error access/object-non-existent if the object does not exist*	Y
1500	the response for DeleteNamedVariableList with a non-existent LN is not specified *CreateDataSet/DefineNamedVariableList specifying a non-existing LD/LN shall fail with access/object-non-existent*	na
1626	PICS for Information Report is incorrect *MMS ServicesSupported "informationReport" should be optional for servers because they never receive InformationReport requests. It is only required for clients which process reports or control command-termination*	Y

Compare the TISSUE database for more details: www.tissues.iec61850.com

F. Cybersecurity

F.1 Introduction F-3
F.2 Ports and Communications Services F-4
F.3 Role Based Access Control (RBAC) F-6
F.3.1 Users, Roles and Permissions F-7
F.3.2 User and Role Management F-12
F.3.2.a User and Role Management from the Web F-12
F.3.2.b User and Role Management from CLI F-16
F.3.2.c User and Role Management from *ZIV e-NET Tool*® F-18
F.3.3 Session Concurrency F-23
F.3.4 Local Access F-24
F.3.4.a Password Authentication F-27
F.3.4.b User and Password Authentication F-29
F.3.5 Automatic Logout F-31
F.4 Remote User Authentication F-32
F.4.1 RADIUS (Remote Authentication Dial In User Service) F-33
F.4.2 LDAP (Lightweight Directory Access Protocol) F-35
F.4.3 Remote User Authentication Configuration F-39
F.4.3.a Remote User Authentication Configuration from the Web F-39
F.4.3.b Remote User Authentication Configuration from CLI F-41
F.4.3.c Remote User Authentication Configuration from *ZIV e-NET Tool*® F-42
F.5 Communication with Configuration Tool using PROCOME F-51
F.6 Secure Sockets F-52
F.6.1 SSH (Secure Shell) F-52
F.6.2 SFTP (SSH File Transfer Protocol) F-53
F.6.3 TLS / SSL (Transport Layer Security / Secure Socket Layer) F-53
F.6.4 HTTPS (Secure Web Server) F-54
F.6.5 Mutual Authentication F-54
F.7 Credential Management F-56
F.7.1 Devices with Basic Cybersecurity F-56
F.7.2 Devices with Enhanced Cybersecurity F-58
F.8 Digital Firmware Securization F-63
F.8.1 Devices with Basic Cybersecurity F-64
F.8.2 Devices with Enhanced Cybersecurity F-64
F.8.3 Firmware Upload Methods F-66

F.9 Registration of Activities F-68
F.9.1 Syslog Format F-68
F.9.2 Events F-68
F.9.3 Storage File F-73
F.9.4 Viewing and Downloading the File F-74

F.1 Introduction

In the past, substation networks were traditionally isolated, and the protocols and data formats used to transmit information between devices were often proprietary.

Because of this, the substation environment was very safe from cyberattacks. The terms used for this type of inherent security are:

- Security by isolation (if the substation network is not connected to the outside world, it cannot be accessed from the outside world).
- Security by obscurity (if data formats and protocols are proprietary, they are difficult for a third party to interpret).

The increasing sophistication of protection devices, together with the advancement of technology and the requirement for interoperability between manufacturers, have resulted in a standardization of networks and data exchange in substations. Today, devices within substations use standardized protocols for communications. In addition, substations can connect to open networks, such as the Internet and vast corporate networks, which employ standardized protocols for communications. This introduces a greater security risk, making the network vulnerable to cyberattacks, which could result in a higher electrical failure rate. Clearly there is now a need to secure communications and devices in substations.

Cybersecurity provides protection against unauthorized disclosure, transfer, modification or destruction of information or information systems, whether accidental or intentional. To achieve this, there are several security requirements:

- Confidentiality (avoid unauthorized access to information).
- Integrity (avoid modification of unauthorized information).
- Availability (avoid denial of service).
- Non-repudiation (avoid denying that an action was taken or asserting that it was done when it was not done).
- Traceability / Detection (monitoring and logging of activity to detect intrusions and analyze incidents).

Cybersecurity threats can be unintentional (natural disasters, human error) or intentional (cyber-attacks by hackers).

Some examples of vulnerabilities are:

- Indiscretions on the part of the staff (users keep the keys on their computers).
- Bad practices (users do not change passwords by default, or everyone uses the same password to access all substation devices).
- Circumvention of control (users deactivate security measures).
- Inadequate technology (no firewalls are installed in the substation).

Some examples of availability problems are:

- Device overload resulting in poor or even no performance.
- Expiration of the certificate preventing access to the device.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To help solve these problems, standardization organizations have developed several standards/norms. Compliance with these standards significantly reduces the threats associated with a lack of cybersecurity.

The cybersecurity measures implemented in the device include the following:

- Disabling of ports and communications services.
- Role-based access control (RBAC).
- Remote user authentication (LDAP and RADIUS).
- Use of secure sockets.
- Digital firmware securization.
- Cybersecurity audit log.

F.2 Ports and Communications Services

It is important to be able to guarantee that a device has active only those physical ports and logical ports (services) strictly necessary to comply with the required functionality. Therefore, it is essential to be able to enable or disable physical ports and services. These physical ports and services are managed through the configuration tool and the HMI of the device.

Depending on the model, the device may have the following physical ports:

- Local port.
- Remote port 1.
- Remote port 2.
- LAN 1.
- LAN 2.
- LAN 3.
- LAN 4.
- USB (pendrive).

By default, all ports on the device are disabled except the local port and the LAN ports. This means that remote ports 1 and 2 and USB (pendrive) will not be operational until they are enabled.

The user must initially enable the ports and services to be used, either by connecting to the configuration tool or by accessing the corresponding HMI menus.

When a port is disabled, it means that both transmission and reception are blocked.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The device has the following settings for enabling and disabling physical ports:

Port Enabling				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
Local Port	Local Port	Inactive / Active		Active
Remote Port 1	Remote Port 1	Inactive / Active		Inactive
Remote Port 2	Remote Port 2	Inactive / Active		Inactive
LAN 1 Port	LAN 1 Port	Inactive / Active		Active
LAN 2 Port	LAN 2 Port	Inactive / Active		Active
LAN 3 Port	LAN 3 Port	Inactive / Active		Active
LAN 4 Port	LAN 4 Port	Inactive / Active		Active
USB Port	USB Port	Inactive / Active		Inactive

If network redundancy (PRP, HSR, RSTP) is configured on a pair of ports (LAN1-2 or LAN3-4), enabling/disabling the second port (LAN2 or LAN4) has no effect on the device. Enabling/disabling the first port (LAN1 or LAN3) enables/disables both ports (LAN1-2 or LAN3-4).

The communication services supported by the device are the following:

- HTTP.
- HTTPS.
- Telnet.
- SSH.
- FTP.
- SFTP.
- MMS (IEC 61850).
- PROCOME Protocol.
- TCP/IP 1 Protocol (PROCOME, DNP3 or MODBUS).
- TCP/IP 2 Protocol (PROCOME, DNP3 or MODBUS).
- TCP/IP 3 Protocol (PROCOME, DNP3 or MODBUS).
- TCP/IP 4 Protocol (PROCOME, DNP3 or MODBUS).
- Syslog Client.

By default, all services are disabled except those which use secure sockets (HTTPS, SSH, SFTP and PROCOME). When a service is disabled, the socket associated with the service may appear as open (in listen state), but does not support connections, filtering is done by software.

The device has the following settings for enabling and disabling logical ports (services):

Service Enabling				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
HTTP	HTTP	Inactive / Active		Inactive
HTTPS	HTTPS	Inactive / Active		Active
SSH	SSH	Inactive / Active		Active
SFTP	SFTP	Inactive / Active		Active
Telnet	Telnet	Inactive / Active		Inactive
FTP	FTP	Inactive / Active		Inactive
MMS (IEC 61850)	MMS (IEC 61850)	Inactive / Active		Inactive
PROCOME	PROCOME	Inactive / Active		Active
TCP/IP Protocol 1	TCP/IP Protocol 1	Inactive / Active		Inactive
TCP/IP Protocol 2	TCP/IP Protocol 2	Inactive / Active		Inactive
TCP/IP Protocol 3	TCP/IP Protocol 3	Inactive / Active		Inactive
TCP/IP Protocol 4	TCP/IP Protocol 4	Inactive / Active		Inactive
Syslog Client	Syslog Client	Inactive / Active		Inactive

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To disable other services such as synchronization by SNTP or by PTP (IEEE 1588), see Chapter 1, **Description and Start-Up**, **Synchronization Settings** section.

As an additional security measure, the device offers the possibility of changing the logical ports assigned to the services. The device has the following settings for changing service ports:

Service Ports				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
HTTP	HTTP	1 - 65535	1	80
HTTPS	HTTPS	1 - 65535	1	443
Telnet	Telnet	1 - 65535	1	23
FTP	FTP	1 - 65535	1	21
SSH/SFTP	SSH/SFTP	1 - 65535	1	22

The logical ports corresponding to the PROCOME, DNP3 and MODBUS protocols can be modified as described in Chapter 1, **Description and Start-Up**, **Communications Settings** section.

The logical port of the MMS protocol corresponding to IEC 61850 communications is 102 and cannot be modified.

All the services must have different port numbers assigned to them.

F.3 Role Based Access Control (RBAC)

The concept of **R**ole **B**ased **A**ccess **C**ontrol (RBAC) is used.

RBAC is not a new concept, many operating systems use it to control access to system resources.

RBAC is an alternative to the total access (superuser) or read-only model.

RBAC complies with the principle of minimum privilege security, which states that no user should be granted more rights than are necessary to perform that user's work.

RBAC allows an organization to separate the different capabilities and group them into special user accounts called roles for assignment to specific individuals according to the needs of their work.

RBAC carries implicitly the concepts of *users*, *roles* and *permissions* that will be developed next.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.3.1 Users, Roles and Permissions

RBAC intrinsically carries the concepts of *users*, *roles* and *permissions*. A *user* has an associated *role*. Each *role* has one or more associated *permissions*.

Some examples that can help to understand the concept of roles and permissions would be the following:

Role	Permissions
VIEWER	Visualization
OPERATOR	Visualization, Command execution
ENGINEER	Visualization, Setting change, Configuration change
INSTALLER	Visualization, Setting change, Configuration change, Firmware change
RBACMNT	Visualization, User management
SECAUD	Visualization, Audit log
ADMINISTRATOR	All

The device allows the creation of up to **20 users**. Each user has associated a username, a password and a role.

The device allows the creation of up to **10 roles**. At the same time, each role can be associated with a series of permissions, in addition to a name and an identifier (used to univocally relate the user with a role).

Each access to the device by a user or application by remote access to console (Telnet / SSH), web (HTTP / HTTPS), file transfer (FTP / SFTP) and configuration tool (PROCOME), must be authenticated (login) through the introduction of user and password.

Access through other protocols, such as DNP3, MODBUS and MMS (IEC 61850), is still free of username and password.

The following permissions have been defined in the device:

- *Visualization* permission. With this permission it is possible to visualize states, measurements, settings, etc., as well as to collect oscillographs, events and fault reports, configuration files and log files (except for the cybersecurity event file).
- *Command execution* permission. With this permission it is possible to execute commands (e.g., date/time change).
- *Setting change* permission. With this permission it is possible to change the value of the settings, as well as to change the active table of settings and load the settings file.
- *Configuration change* permission. With this permission it is possible to load configuration files.
- *Firmware change* permission. With this permission it is possible to load the firmware to the device.
- *User management* permission. With this permission it is possible to manage users (add, delete or modify a user or a role), configure authentication methods and manage credentials.
- *Audit log* permission. With this permission it is possible to view/collect the cybersecurity event file.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

By default, there is a single *admin* user with password *Passwd@02* associated with a role with identifier *-1*. This role is configured by default with all the permissions.

As a minimum, the visualization permission must be active. A user who does not have visualization permission will not have permission to do anything and therefore the device will reject his/her authentication attempts.

There must always be a user with user management permission.

To configure users and roles a user with *user management* permission must be used and next procedures can be used:

- From a website, via HTTP (not recommended because the data is not encrypted) or HTTPS, by accessing the ***Configuration→Access*** menu.
- From command line interface (CLI), via Telnet (not recommended because the data is not encrypted) or SSH.
- From the ***ZIV e-NET Tool***® configuration tool, using *LocalRBAC* and *DevicePreferences* files.

The following parameters are configured for each user:

Users					
Website	**CLI**	**LocalRBAC**	**Range**	**Step**	**Default**
Login	*main/access/user[x]/login*	name	char[32]		admin
Password	*main/access/user[x]/pwd*	pwd	char[32]		Passwd@02
Role Id	*main/access/user[x]/roleid*	role	-32768… 32767	1	-1

where *x* goes from 1 to 20, depending on the number of users that have been created.

Name. It supports up to 32 characters and its default value is *admin*. If it is empty, it means that the user does not exist. The username is unique (no two users with the same name can exist) and is case sensitive (i.e., "Admin" and "admin" are two different users).

Password. Users' passwords are strong. They allow a minimum length of 8 characters and a maximum of 32, are case sensitive and contain:

- At least one uppercase letter.
- At least one lowercase letter.
- At least one number.
- At least one non-alphanumeric character from ASCII 33 to ASCII 126 (both included). Blank space (ASCII character 32) is not a valid character to be used as part of passwords.

Passwords are never shown in clear and are stored encrypted on the device. Its default value is *Passwd@02*.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Role. An existing role identifier is configured.

The following parameters are configured for each role:

Roles					
Website	**CLI**	**DevicePreferences**	**Range**	**Step**	**Default**
Name	*main/access/role[y]/name*	name	char[32]		admin
Id	*main/access/role[y]/id*	id	-32768… 32767	1	-1
View	*main/access/role[y]/rview*	rightMsk (bit 0x01)	NO / YES		YES
Control	*main/access/role[y]/rctrl*	rightMsk (bit 0x02)	NO / YES		YES
Settings	*main/access/role[y]/rchset*	rightMsk (bit 0x04)	NO / YES		YES
Config	*main/access/role[y]/rchcfg*	rightMsk (bit 0x08)	NO / YES		YES
Firmware	*main/access/role[y]/rchfw*	rightMsk (bit 0x10)	NO / YES		YES
Users	*main/access/role[y]/rusrmgmt*	rightMsk (bit 0x20)	NO / YES		YES
Audit	*main/access/role[y]/raudit*	rightMsk (bit 0x40)	NO / YES		YES
Global role concurrency	*main/access/global_conc*	global_conc	NO / YES		YES
Priority	*main/access/role[y]/priority*	priority	1…10		5
Concurrency	*main/access/role[y]/concurrency*	concurrency	NO / YES		NO

where *y* goes from 1 to 10, depending on the number of roles that have been created.

Name. It supports up to 32 characters and its default value is *admin*. It cannot be empty. The role name is unique (there cannot be two roles with the same name) and is case sensitive (i.e., "Admin" and "admin" are two different roles).

This is the text used to check the role returned by remote authentication services (AAA) when they return a text.

Identifier. It uniquely identifies the role and is used on the user to indicate its associated role.

This is the number used to check the role returned by remote authentication services (AAA) when they return a number.

According to the IEC 62351-8 standard, negative numbers will be used for private roles, since this standard reserves positive numbers. The user can assign the desired value within the range -32768...32767, but by default the identifier -1 is assigned to comply with IEC 62351-8 standard.

Permissions. These are the different permissions that a role can have.

A role without associated permissions is not allowed to do anything and the device will reject authentication attempts from users who have that role associated with them.

The characters supported for usernames and roles are those indicated in the POSIX standard (Portable Operating System Interface for Unix) (IEEE Standard 1003.1 2008), with the exception that the hyphen character '-' cannot be used as the first character of the username or role:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 . _ -
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The last three parameters are related to **Role Concurrency**:

Access Priority. This is a numeric setting indicating the access priority of that role. There will be as many priorities as roles (10). The lowest number (1) indicates the lowest priority and the highest number (10) indicates the highest priority. The default value is 5.

When the session limit has been reached (see **Session Concurrency** section), the access of a user with a higher priority role will cause the session of a user with a lower priority role to be automatically closed without any warning. The criterion will be to close the session of the user with a lower priority role and who has been connected for the longest time.

This priority will become clearer later when the different configuration possibilities are explained.

Concurrent Access. This is a Boolean setting that indicates whether concurrency is allowed for that role. Concurrency is when a role is authenticated more than once. The value **YES** indicates concurrency, **NO** indicates non-concurrency (a role can only be authenticated once). The default value will be **NO**.

Once there is an authenticated user with a certain non-concurrent role, authentication of another user with that role is prevented. The exceptions to this general rule are explained in detail below.

Apply non-concurrent roles together. If selected (value **YES**) it means that non-concurrency is additionally checked among all roles marked as non-concurrent, i.e., only one non-concurrent role can be authenticated at any given time. For example, if the roles ENGINEER, INSTALLER and SECADM are configured as non-concurrent and this setting is set to YES, only a user with role ENGINEER, INSTALLER or SECADM can be active (if a user with role ENGINEER is authenticated, a second user with role INSTALLER or SECADM will not be able to access). The default value is YES.

Always taking the criterion of facilitating access to users with priority roles (non-concurrent):

- In case there are authenticated users with non-priority (concurrent) roles, the user with the lowest priority role and who has been logged in the longest is logged out automatically and without warning.
- In case there is another authenticated user with priority (non-concurrent) role, the new user is asked if he/she wants to log out the user with priority role who is currently authenticated. This option is only available via website and HMI.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The following shows how the device behaves in the different cases of role concurrency configuration:

Case in which the *Apply Non-Concurrent Roles Together* parameter is set to YES

- If the accessing user has a concurrent role:
  - If there are available sessions in that service, the access is granted.
  - If there are no available sessions in that service, a check is made to see if there is an authenticated user with less priority role:
    - If there is, the session of the longest authenticated user is automatically closed, access is granted to the new user and the **Logout - session closed by other user** event is generated with the user that has just been expelled.
    - If not, access is denied and the event **Login failed - too many user sessions** is generated.

- If the accessing user has a non-concurrent role:
  - A check is made to see if there is any other authenticated user with non-concurrent role:
    - If there is and it is higher priority than the user trying to access, access is denied and the event **Login failed - user rejected due to role concurrency** is generated.
    - If there is and it is equal or lower priority than the user trying to access and the service is not a website or HMI, access is denied and the event **Login failed - user rejected due to role concurrency** is generated.
    - If there is and it is equal or lower priority than the user trying to access and the service is a website or HMI, a warning is displayed that there is another authenticated privileged user and is offered to the user the possibility of expelling it:
      - If the user accepts, the other user with non-concurrent role is logged out, access is granted to the new user and the **Logout - session closed by other user** event is generated with the user that was just expelled.
      - If the user cancels, access is denied and the event **Login failed - user rejected due to role concurrency** is generated.
    - If there is not, a check is made to see if there are available sessions in that service:
      - If there are available sessions, access is granted.
      - If there are no available sessions, a check is made to see if any user with a lower priority role is authenticated:
        - If there is, the session of the user who has been logged in the longest is automatically closed, access is granted to the new user and the **Logout - session closed by other user** event is generated with the user who has just been expelled.
        - If not, access is denied and the event **Login failed - too many user sessions** is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Case where the *Apply Non-Concurrent Roles Together* parameter is set to NO

- If the accessing user has a concurrent role:
  - If there are available sessions in that service, the access is granted.
  - If there are no available sessions in that service, a check is made to see if there is an authenticated user with less priority role:
    - If there is, the session of the user with the lowest priority role who has been logged in the longest is automatically closed, access is granted the new user and the **Logout - session closed by other user** event is generated with the user who has just been expelled.
    - If not, access is denied and the event **Login failed - too many user sessions** is generated.

- If the accessing user has a non-concurrent role:
  - A check is made to see if there is any other authenticated user with the same role:
    - If there is, and the service is not a website or HMI, access is denied and the event **Login failed - user rejected due to role concurrency** is generated.
    - If there is and the service is a website or HMI, a warning is displayed that there is another authenticated privileged user and is offered to the user the possibility of expelling it:
      - If the user accepts, the other user with the same role is logged out, access is granted to the new user and the **Logout - session closed by other user** event is generated with the user that was just expelled.
      - If the user cancels, access is denied and the event **Login failed - user rejected due to role concurrency** is generated.
    - If there is not, a check is made to see if there are available sessions in that service:
      - If there are available sessions, access is granted.
      - If there are no available sessions, a check is made to see if any user with a lower priority role is authenticated:
        - If there is, the user with the lowest priority role who has been logged in the longest is automatically logged out, access is granted to the new user and the **Logout - session closed by other user** event is generated with the user who has just been logged out.
        - If not, access is denied and the event **Login failed - too many user sessions** is generated.

F.3.2 User and Role Management

User and role management must be performed by a user with *user management* permission. It is managed from several interfaces:

- Web interface (HTTP / HTTPS).
- CLI Command Line Interface (Telnet / SSH).
- ***ZIV e-NET Tool***® Configuration Tool, using *LocalRBAC* and *DevicePreferences* files.

F.3.2.a User and Role Management from the Web

In order to manage users from the web interface, some LAN ports and HTTP or HTTPS services need to be enabled. It is recommended to use the HTTPS connection instead of HTTP because the data is encrypted.

- The website of the device is accessed through a browser, entering the IP address configured in the LAN adapter of the device. Initially, a login web page appears where the user's name and password must be entered (*admin* is the default user).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

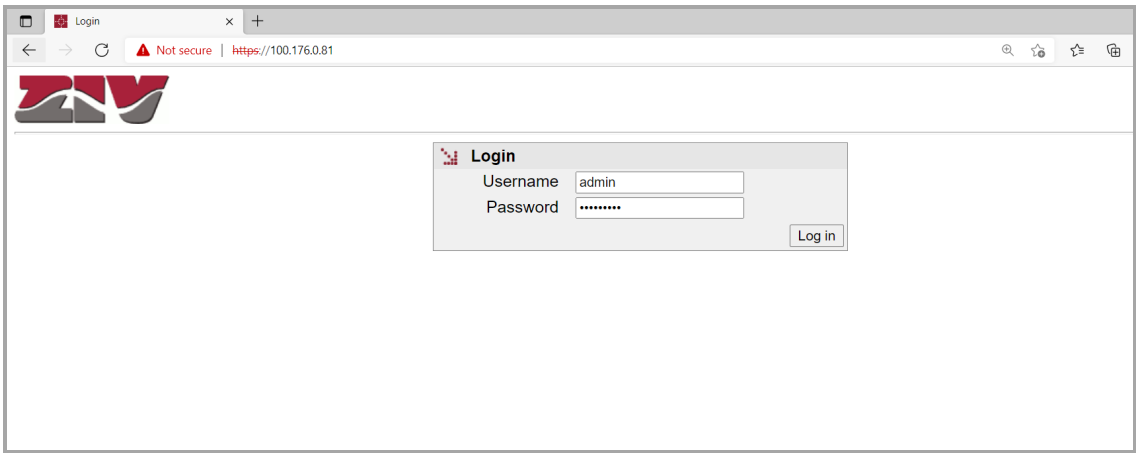


Figure F.1 User Authentication on Website.

- The ***Configuration→Access*** menu is accessed to manage user configuration.

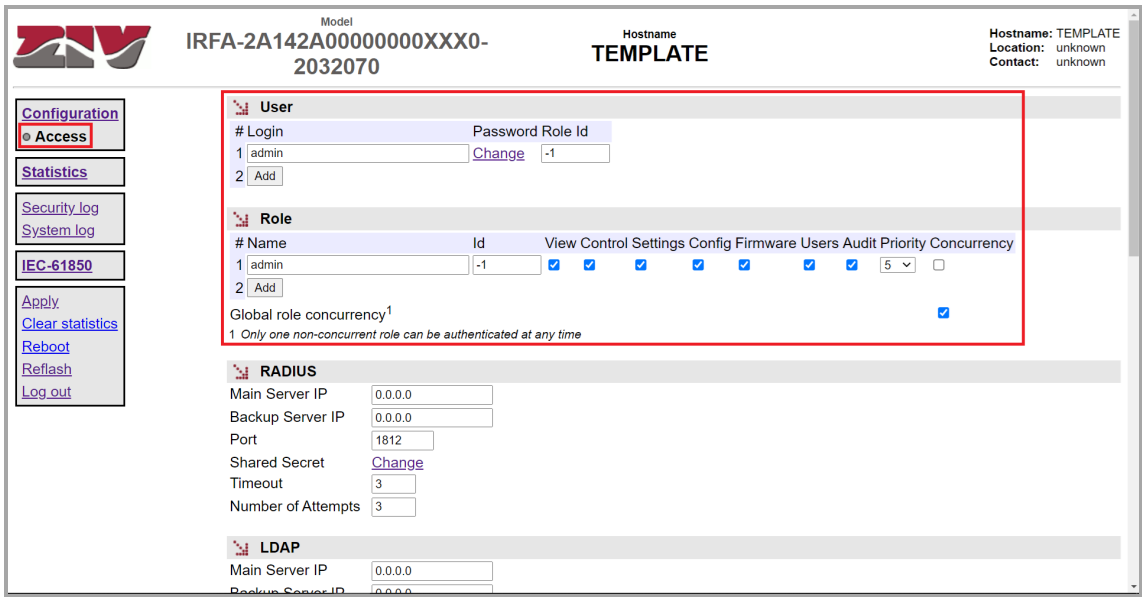


Figure F.2 Users and Roles Configuration in Website.

To add a new role, click on the ***Add*** button in the ***Role*** section and enter a name (cannot be repeated), a role identifier (cannot be repeated), select the permissions assigned to the role, adjust the priority if desired and configure its concurrency. In the following example, the *guest* role is created with identifier '-2' and only *visualization* permission, priority 5 and concurrent.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

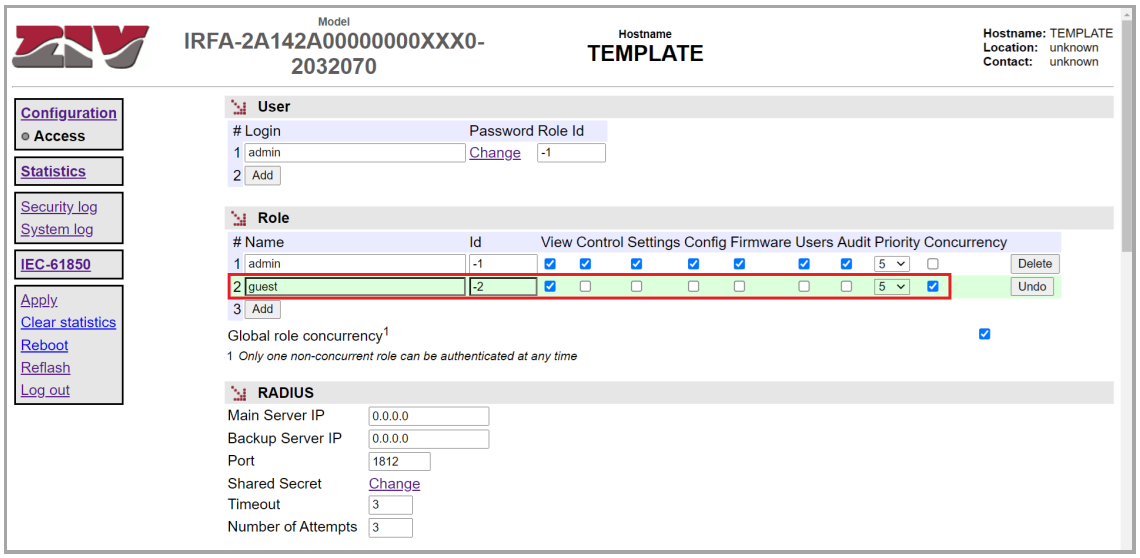


Figure F.3 Adding a Role on a Website.

To add a new user, press the ***Add*** button in the ***User*** section and enter the username (cannot be repeated) and the associated role identifier. In the example, a *guest* user is created and assigned the role with identifier -2.

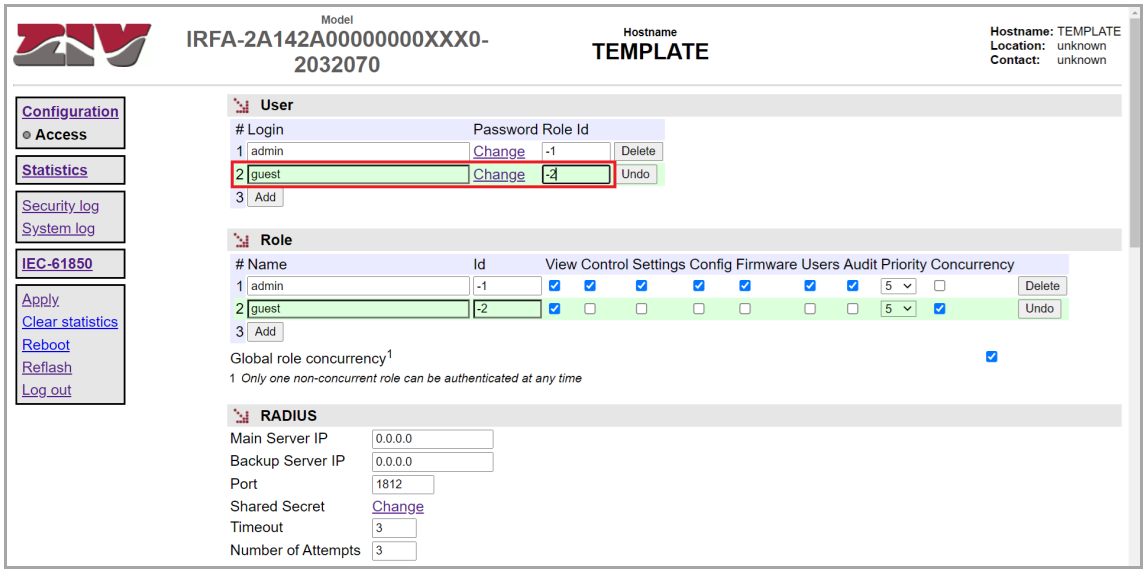


Figure F.4 Adding a User on a Website.

You can then change the password of the new user by clicking on the ***Change*** link.

*Before changing your password, validate the above data by clicking on the **Send** button located at the bottom of the web page (scroll down to the bottom of the web page). Otherwise, the data entered will be lost.*

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

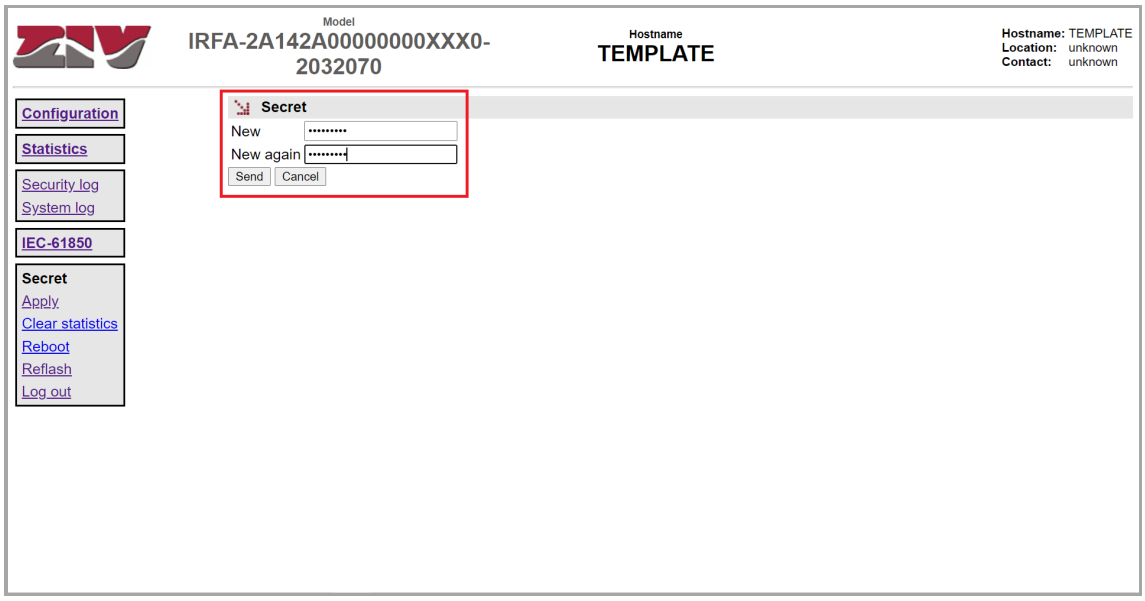


Figure F.5 Changing User Password on Website.

On the password change web page, enter the new password twice and click ***Send***.

For new users to take effect, click on the ***Apply*** menu, click ***OK*** and wait for the message *'Configuration applied successfully'* to appear.

If you wish to temporarily disable a role, and therefore the users that include it, you can deactivate the *visualization* permission of a role.

To delete a user or role, press the corresponding ***Delete*** button and then press ***Send*** and ***Apply***. In the following example the user 'Dummy' and the role '-1234' will be deleted.

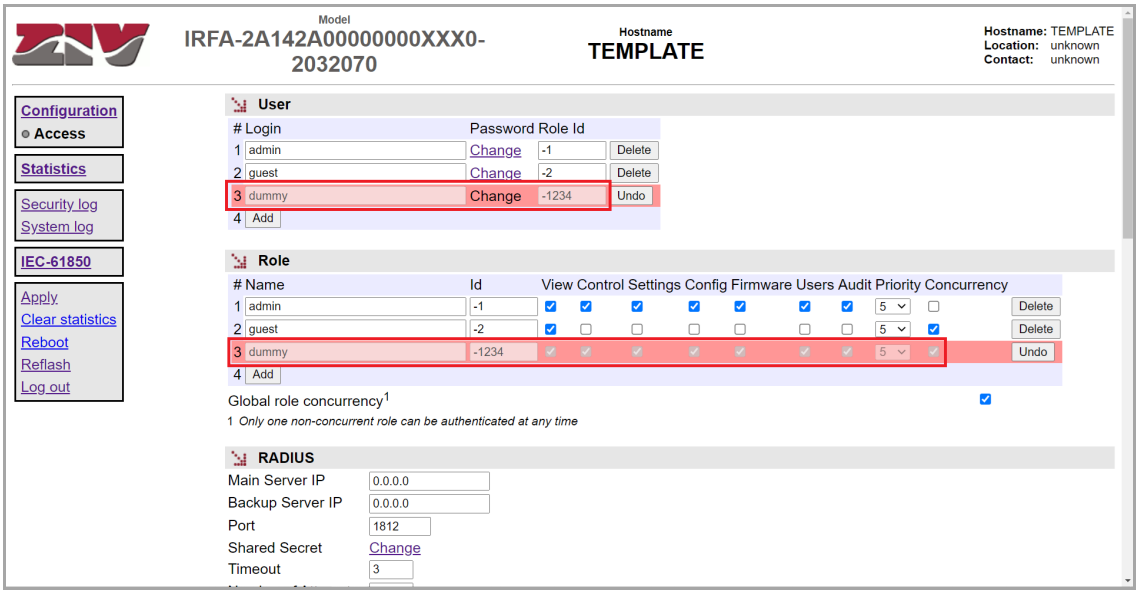


Figure F.6 Delete User and Role on Website.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

*Before changing your password, validate the above data by clicking on the **Send** button located at the bottom of the web page (scroll down to the bottom of the web page). Otherwise, the data entered will be lost.*

F.3.2.b User and Role Management from CLI

To manage users and roles from the CLI command line interface, some LAN ports and Telnet or SSH services need to be enabled. It is recommended to use the SSH connection instead of Telnet because the data is encrypted.

The CLI of the device is accessed by launching the Telnet or SSH application from a host and entering the login of the user who has *user management* permission.

The CLI of the device is automatically accessed. You can see the parameters tree with the ***get*** command. The corresponding user settings are in the ***main/access*** node.

```
TEMPLATE /> get
/
   main/
      hostname       = TEMPLATE
      location       = unknown
      contact        = unknown
      product        = any
      model          = IRFA-2A142A00000000XXX0-2032070
      iedInfo        = ZIV   IRFA-2A142A00000000XXX0-2032070   0.10.0-0C03-00
      fw_version     = 0.10.0-0C03-00
      fw_reference   = unknown
      serialnumber   = 160538
      config_version = 00.00
      time           = 2021/06/29,10:25:11
      localtime      = 2021/06/29,10:25:11
      access/
         global_conc = on
         user[]/
            [user] login pwd      roleid
            ---------------------------
            1      admin ******** -1
         role[]/
            [role] name  id rview rctrl rchset rchcfg rchfw rusrmgmt raudit priority concurrency
            ------------------------------------------------------------------------------------
            1      admin -1 on    on    on     on     on    on       on     5        off
         radius/
            server1_ip = 0.0.0.0
            server2_ip = 0.0.0.0
            port       = 1812
            secret     = ********
            timeout    = 3
            attempts   = 3
```

Figure F.7 User and Role Settings in CLI.

To add a new role, first add a new element in the ***role[]*** table with the command ***add/main/access/role***. A new role is created with index 2 in the table and with the default values.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

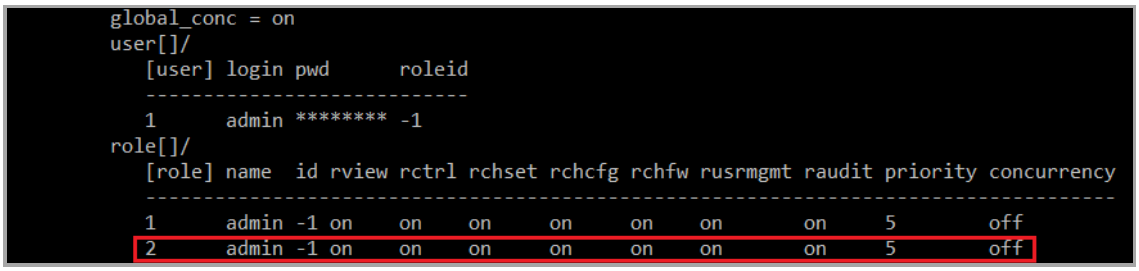


Figure F.8 Adding a Role in CLI.

The new role is now modified with the desired name, identifier, permissions, priority and concurrency. It can be done interactively executing the command ***set main/access/role[2]*** where each one of the fields will be asked to complete the role, or directly executing the set of the field to modify, for example:

- ***set /main/access/role[2]/name guest***
- ***set /main/access/role[2]/id -2***
- ***set /main/access/role[2]/rview on***
- ***set /main/access/role[2]/rctrl off***
- ***set /main/access/role[2]/rchset off***
- ***set /main/access/role[2]/rchcfg off***
- ***set /main/access/role[2]/rchfw off***
- ***set /main/access/role[2]/rusrmgmt off***
- ***set /main/access/role[2]/raudit off***
- ***set /main/access/role[2]/priority 5***
- ***set /main/access/role[2]/concurrency on***

To add a new user, you must perform a similar process to the previous one but in the ***user[]*** table.

- ***add main/access/user***

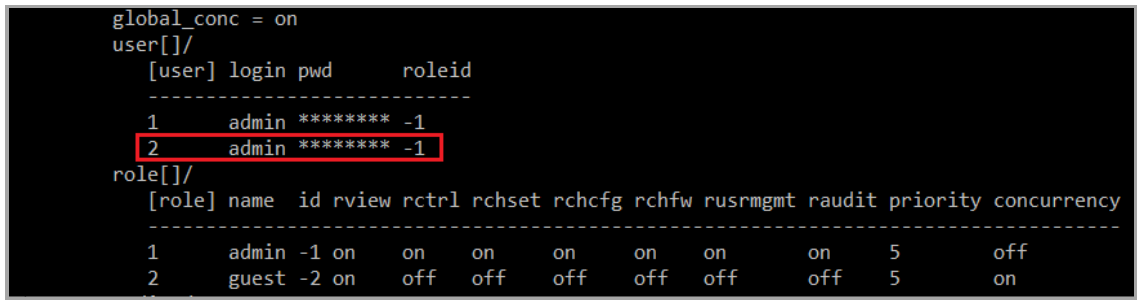


Figure F.9 Adding a User in CLI.

- ***set main/access/user[2]/login guest***
- ***set main/access/user[2]/roleid -2***
- ***set main/access/user[2]/pwd*** (by entering the key value twice).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

```
global_conc = on
user[]/
   [user] login pwd      roleid
   ---------------------------
   1      admin ******** -1
   2      guest ******** -2
role[]/
   [role] name  id rview rctrl rchset rchcfg rchfw rusrmgmt raudit priority concurrency
   ------------------------------------------------------------------------------------
   1      admin -1 on    on    on     on     on    on      on     5        off
   2      guest -2 on    off   off    off    off   off     off    5        on
```

Figure F.10 Modified User and Role in CLI.

Once the new user and/or role has been created, the data is saved with the ***save*** command and the changes in the device are made effective with the ***apply*** command.

F.3.2.c User and Role Management from *ZIV e-NET Tool*®

To manage users and roles from ***ZIV e-NET Tool***® it is necessary that some of the LAN ports and the SSH and SFTP services are enabled.

A distinction is made between users and roles, as they are configured in different configuration files. The operation is as follows: first the roles are created (they are stored as part of the *DevicePreferences* file), then the local users are created (they are stored in the *LocalRBAC* file) and finally both files are transferred to the device. When collecting information from the device, only the complete *DevicePreferences* file can be collected (this includes the roles). Local users cannot be retrieved from the device, as the *LocalRBAC* file contains the device passwords, it is considered a file only for input to the device.

To configure local users, in the ***Navigation View*** go to the ***Preferences→Security→Local Users*** option.

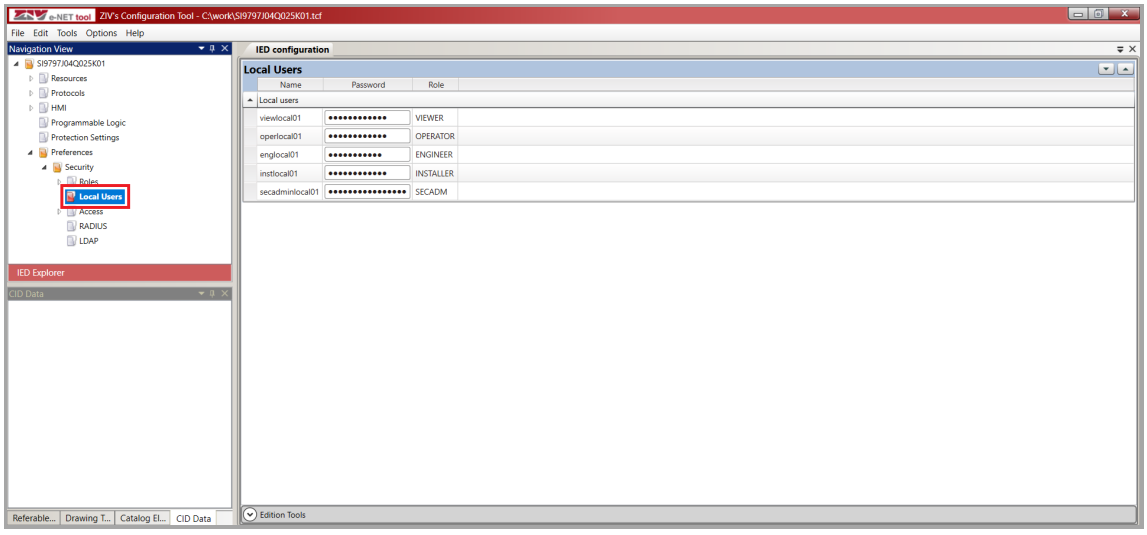


Figure F.11 Configuration of Local Users with Configuration Tool.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Following the usual philosophy of the tool, local users can be added or deleted (using the ***Edition Tools*** tab), as well as modifying the current local users. For each user, its name, password and associated role must be configured (therefore the roles must be created previously).

By right-clicking on this option ***Preferences→Security→Local Users***, you can export the users to a *LocalRBAC* file or import them from a previously configured *LocalRBAC* file.

The *LocalRBAC* file is an XML file with the following format:

Node	Description	Child nodes	Attributes
RBACtemplate	Root node.	**device**	-
device	Main node.	**LOCALUSRDB**	**name**: name of the device. **IP**: IP address of the device.
LOCALUSRDB	Local users.	**LocalUsr**	-
LocalUsr	Definition of a local user: name, password and assigned role.	-	**name**: name of the user. **pwd**: user password. **role**: numeric identifier of the role assigned to the user.

Example of a *LocalRBAC* file:

```
<?xml version="1.0" encoding="utf-8"?>
<RBACtemplate>
 <device name="TEMPLATE" IP="192.168.1.81">
  <LOCALUSRDB>
   <LocalUsr name="viewlocal" pwd="PwdView@01" role="7"/>
   <LocalUsr name="operlocal" pwd="PwdOper@01" role="8"/>
   <LocalUsr name="englocal" pwd="PwdEng@01" role="9"/>
   <LocalUsr name="instlocal" pwd="PwdInst@01" role="10"/>
   <LocalUsr name="secadmlocal" pwd="PwdSecadm@01" role="15"/>
  </LOCALUSRDB>
 </device>
</RBACtemplate>
```

To transfer local users to the device, go to the menu ***Tools→Device access***. In this window, check that SFTP + SSH is selected in ***Protocol***, configure the IP address of the device and port (it must match the SSH/SFTP port of the device) and enter the user's credentials (user and password). In the ***Transfer Files*** tab, check the ***LRBAC*** option and click ***Transfer*** to upload the *LocalRBAC* file to the device. The upload progress is indicated in the ***Information*** window. If the *LocalRBAC* file is successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if any error occurs in the validation of the *LocalRBAC* file by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

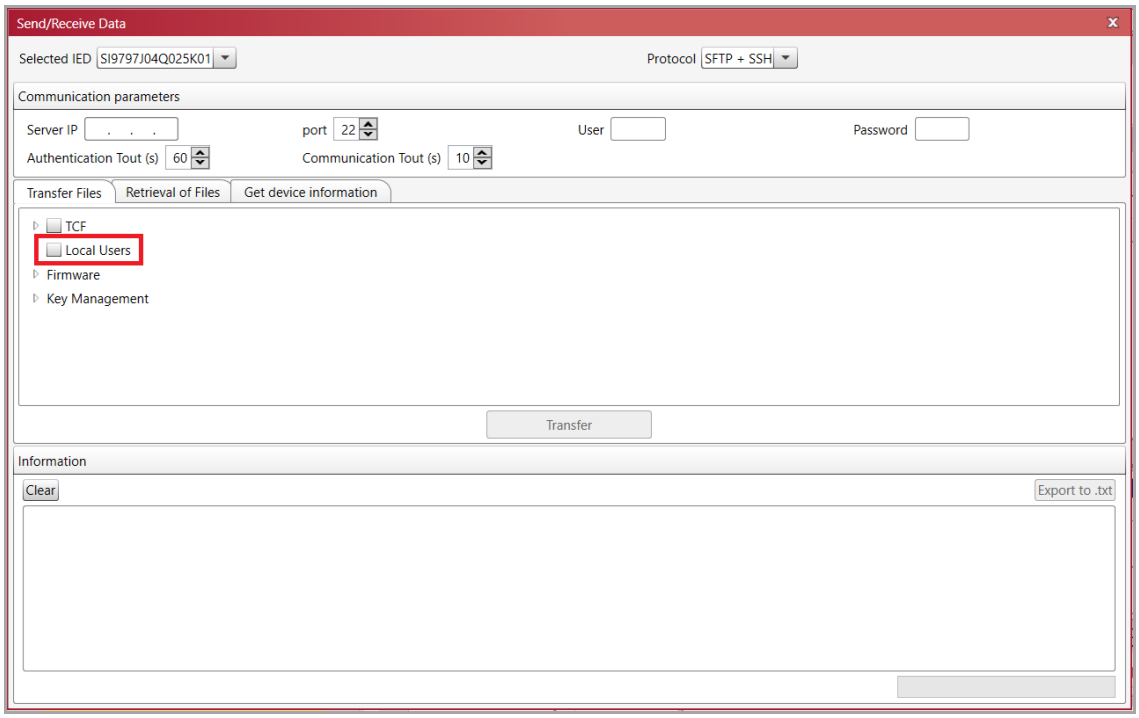


Figure F.12 Sending Local Users with Configuration Tool.

To configure the roles, in the Navigation View go to the ***Preferences→Security→Roles*** option.

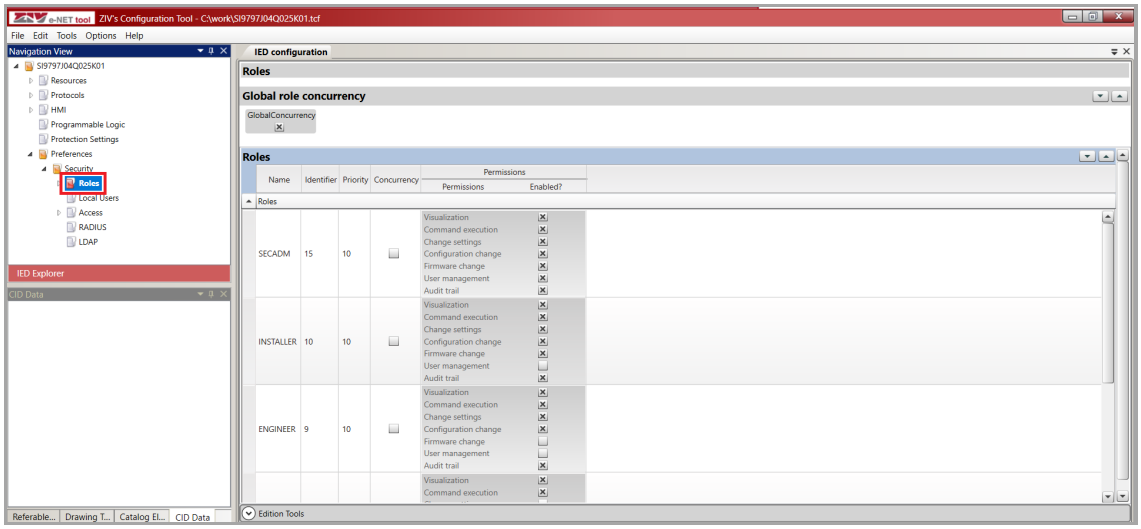


Figure F.13 Role Configuration with Configuration Tool.

Following the usual philosophy of the tool, roles can be added or deleted (using the ***Edition Tools*** tab), as well as modifying the current roles. For each role, its name, identifier, priority, concurrency and associated permissions must be configured.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

By right-clicking on this option ***Preferences→Security→Roles***, you can export the roles to a *DevicePreferences* file or import them from a previously configured *DevicePreferences* file.

The roles are part of the *DevicePreferences* file. This is an XML file whose roles section has the following format:

Node	Description	Child nodes	Attributes
device	Root node.	**ROLES**, RADIUS, LDAP, ACCESS	**tversion**: file version. **filetype**: file type ("DevicePreferences").
ROLES	Roles.	**Role**	**global_conc**: indicates whether only one or more non-concurrent roles can be authenticated at the same time.
Role	Role definition: name, identifier, permission mask, priority and concurrency.	-	**name**: name of the role. **id**: numerical identifier of the role. **rightMsk**: permissions mask, where: - 0x01: *Visualization* permission. - 0x02: *Command execution* permission. - 0x04: *Setting change* permission. - 0x08: *Configuration change* permission. - 0x10: *Firmware change* permission. - 0x20: *User management* permission. - 0x40: *Audit log* permission. **priority**: role priority. **concurrency**: indicates whether the role is concurrent or not.

Example of *DevicePreferences* file (only with roles section):

```
<?xml version="1.0" encoding="utf-8"?>
<device tversion="0.1" fileType="DevicePreferences">
  <ROLES global_conc="Yes">
    <Role name="SECADM" id="15" rightMsk="127" priority="10" concurrency="No" />
    <Role name="INSTALLER" id="10" rightMsk="95" priority="10" concurrency="No" />
    <Role name="ENGINEER" id="9" rightMsk="79" priority="10" concurrency="No" />
    <Role name="OPERATOR" id="8" rightMsk="3" priority="1" concurrency="Yes" />
    <Role name="VIEWER" id="7" rightMsk="1" priority="1" concurrency="Yes" />
  </ROLES>
</device>
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To transfer the roles to the device, go to the menu ***Tools→Device access***. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the IP address and port data of the device (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Transfer Files*** tab, check the option ***TCF→Preferences*** (if you want to transfer the complete *DevicePreferences* file) or the option ***TCF→Preferences→Roles*** (if you want to transfer only the roles) and click ***Transfer*** to upload the complete *DevicePreferences* file or only the roles to the device. The upload progress is indicated in the ***Information*** window. If it has been successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if there is any error in the validation by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

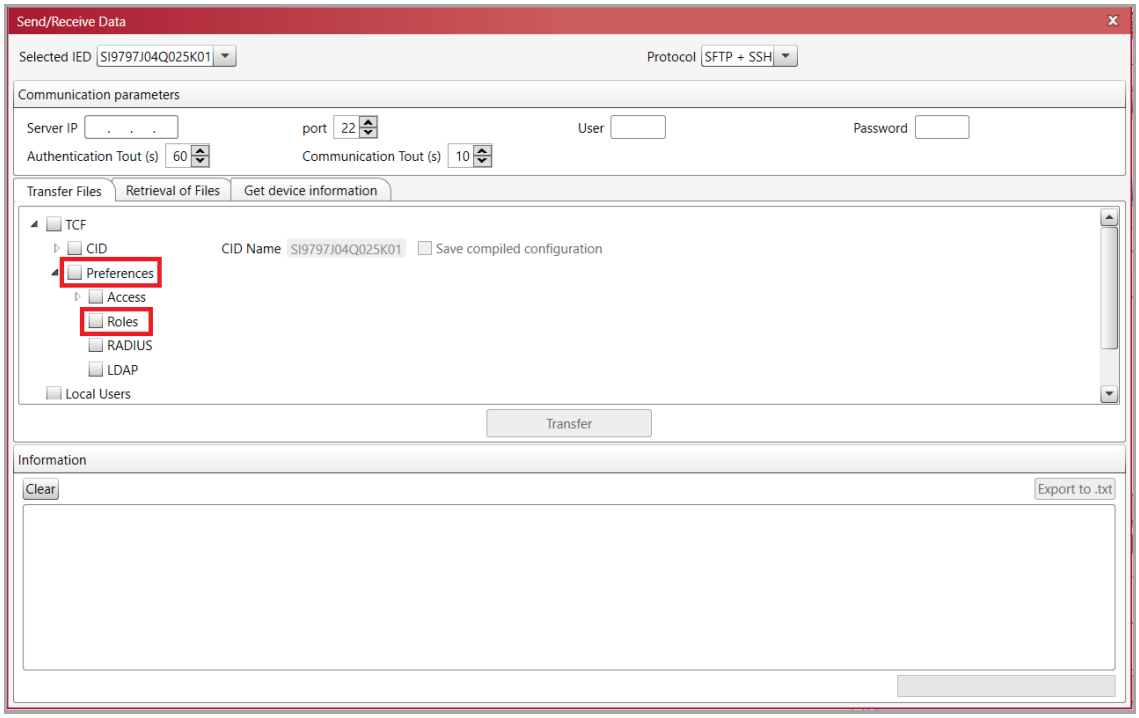


Figure F.14 Sending Roles with Configuration Tool.

To collect the roles from the device, access the menu ***Tools→Device access***. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the IP address of the device and port (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Retrieval of Files*** tab, check the ***Preferences*** option (only the complete *DevicePreferences* file can be downloaded) and click ***Retrieval*** to download the *DevicePreferences* file. The download progress is displayed in the ***Information*** window. Once the file has been downloaded, the **Configuration downloaded** cybersecurity event is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

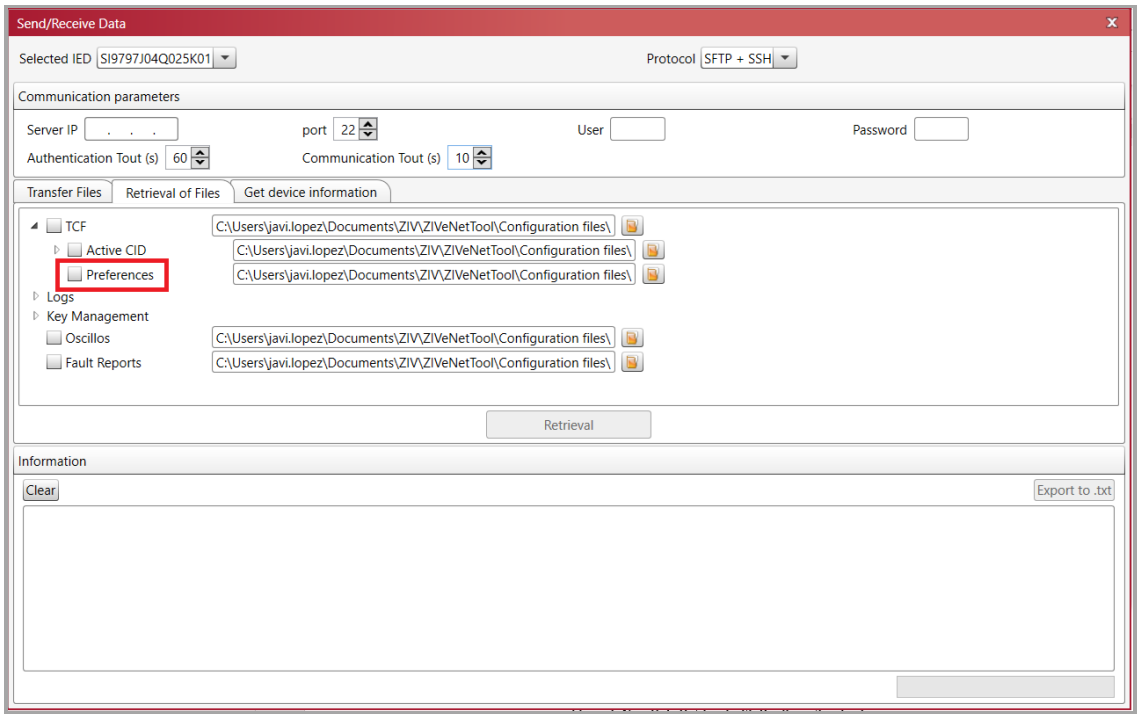


Figure F.15 Role Retrieval with Configuration Tool.

F.3.3 Session Concurrency

In order to control the resources used by the device, it was decided to limit the number of authenticated concurrent sessions per type of service available in the device.

The device has the following settings, which can be modified from the configuration tool and from the HMI:

Concurrent sessions				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
The same user can occupy all available sessions	`Same usr all sess`	YES / NO		YES
Telnet	`Telnet`	1 – 5	1	2
FTP	`FTP`	1 – 5	1	2
HTTP	`HTTP`	1 – 5	1	2
SSH/SFTP	`SSH/SFTP`	1 – 10	1	4
HTTPS	`HTTPS`	1 – 5	1	2

Some clients wish to prevent the same user from being able to occupy all available sessions of a service, preventing others from authenticating. For this purpose, the setting ***The same user can occupy all available sessions*** is used as follows:

- If the setting takes the value **YES**, all sessions of a service can be occupied by the same user and an attempt to open a new session when all of them are occupied will mean that the session is not accepted, generating the **Login failed - too many user sessions** cybersecurity event.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- If the setting is set to **NO**, all sessions of a service may be occupied by the same user and an attempt to open a new session when all of them are occupied will mean that:
  - If the session is of another user, this is accepted and the oldest (longest running) session of the other user who had all sessions occupied is closed without any warning. The **Logout - session closed by other user** cybersecurity event is generated.
  - If the session is of the same user who has all other sessions occupied, this new connection is rejected and the **Login failed - too many user sessions** cybersecurity event is generated.

F.3.4 Local Access

Local accesses correspond to accesses via HMI and USB (pendrive). As these are face-to-face accesses, which take place within the physical security perimeter of the electrical installations (considered secure), it is generally enough for them to be protected by a numerical password. Even under these conditions, there are customers who require all accesses to be protected with a username and password, and the HMI is no exception.

The device is able to operate in both ways depending on the following setting, which can be modified from the website, command line (CLI) or ***ZIV e-NET Tool***® configuration tool (using the *DevicePreferences* file).

User required for HMI authentication					
Website	**CLI**	**DevicePreferences**	**Range**	**Step**	**Default**
User required for HMI authentication	*main/access/hmi/ usrauthhmi*	usrauthhmi	NO / YES		NO

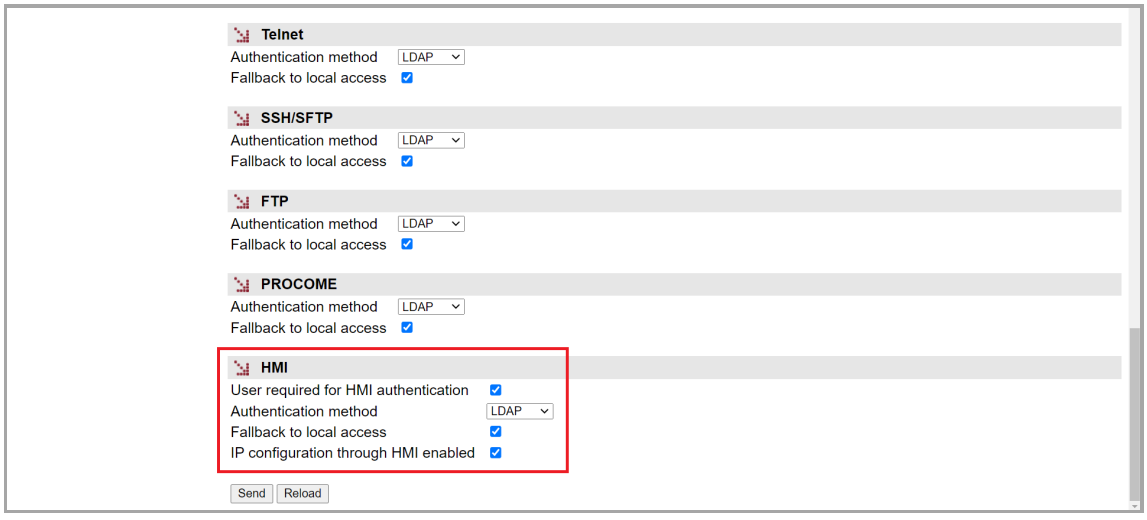


Figure F.16 Setting to Require User for HMI Authentication on Website.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

```
main/
   access/
      hmi/
         usrauthhmi  = off
         pwdconfig   = ********
         pwdcontrol  = ********
         pwdsettings = ********
         method      = LDAP
         local       = on
         confiphmi   = on
```

Figure F.17 Setting to Require User for HMI Authentication on CLI.

To change this setting via website or CLI, it is necessary that, after modifying the setting, the ***Send*** and ***Apply*** buttons/commands are pressed/executed in website/CLI.

To change this setting by ***ZIV e-NET Tool***® it is necessary that some of the LAN ports and the SSH and SFTP services are enabled. In the ***Navigation View***, go to the ***Preferences→Security→Access→HMI*** option.

By right-clicking on this option ***Preferences→Security→Access→HMI***, you can export the HMI settings (the present one plus others explained in other sections) to a *DevicePreferences* file or import them from a previously configured *DevicePreferences* file.

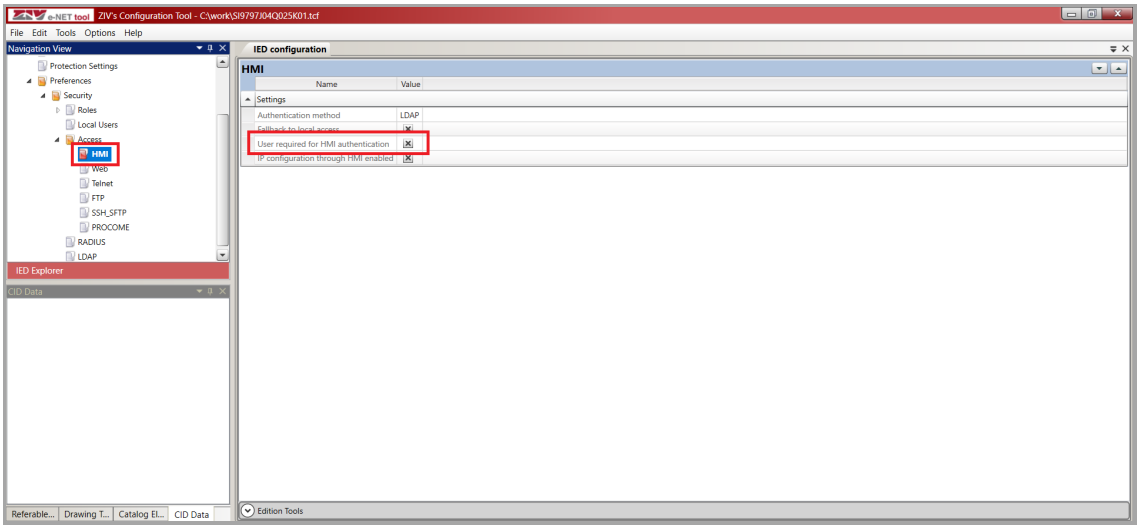


Figure F.18 Setting to Require User for HMI Authentication on Configuration Tool.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

This setting is part of the *DevicePreferences* file. It is an XML file and this setting is located inside the HMI section (highlighted):

Node	Description	Child nodes	Attributes
Device	Root node.	ROLES, RADIUS, LDAP, **ACCESS**	**tversion**: file version. **filetype**: type of file ("DevicePreferences").
ACCESS	Parameters to control access	**HMI**, WEB, TELNET, FTP, SSH_SFTP, PROCOME	-
HMI	HMI access parameters.	**Setting**	-
Setting	One **Setting** node for each HMI access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for HMI access (local, LDAP or RADIUS). - **local**: alternative use of local users for HMI access. - **userauthhmi**: name of the role. - **confiphmi**: it is allowed to change the IP via HMI. **value**: setting value.

Example of *DevicePreferences* file (with complete HMI section, the setting of require user for HMI authentication is highlighted):

```
<?xml version="1.0" encoding="utf-8"?>
<device tversion="0.1" fileType="DevicePreferences">
  <ACCESS>
    <HMI>
      <Setting name="method" value="LDAP" />
      <Setting name="local" value="Yes" />
      <Setting name="usrauthhmi" value="Yes" />
      <Setting name="confiphmi" value="Yes" />
    <HMI>
  </ACCESS>
</device>
```

To transfer the setting to the device, access the ***Tools→Device access*** menu. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the IP address data of the device and port (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Transfer Files*** tab, check the option ***TCF→Preferences*** (if you want to transfer the complete *DevicePreferences* file), the option ***TCF→Preferences→Access*** (if you want to transfer the complete access section) or the option ***TCF→Preferences→Access→HMI*** (if you want to transfer the complete HMI access section, this is the minimum section that can be sent) and press ***Transfer*** to upload the information to the device. The upload progress is indicated in the ***Information*** window. If it has been successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if there is any error in the validation by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

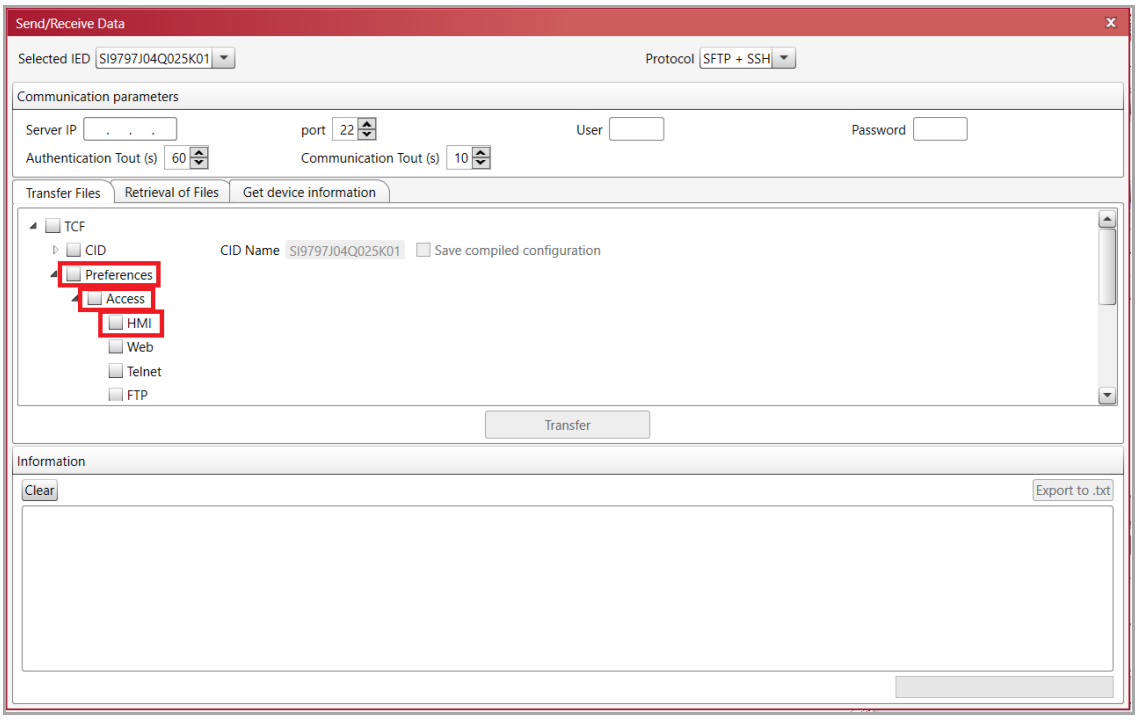


Figure F.19 Sending Setting to Require User for HMI Authentication with Configuration Tool.

To collect this setting from the device, proceed as indicated in the **User and Role Management from ZIV e-NET Tool®** section for the roles, as it is only possible to collect the complete *DevicePreferences* file.

Depending on this setting, the device behaves as follows:

- The value **NO** will indicate that the HMI authentication is performed using only a 4-number password.
- The value **YES** indicates that the HMI authentication is performed using user and password.

Both authentication modes are explained below.

F.3.4.a Password Authentication

The device has three passwords to access different levels of HMI management:

- *Configuration*: used to change parameters in the HMI configuration menu, as well as to download information to the USB pendrive.
- *Operations*: used to perform operations (commands) from HMI.
- *Settings*: used to change settings, including changing the active settings table.

The default value of the three passwords is 2140.

Two procedures can be used to change the value of these passwords:

- From HMI, by accessing the ***Configuration→Passwords*** menu.
- From the command line interface (CLI), through Telnet (not recommended because the data is not encrypted) or SSH.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The settings corresponding to the three local passwords are as follows:

Local Passwords				
CLI	**HMI**	**Range**	**Step**	**Default**
main/access/hmi/pwdconfig	Configuration	0 - 9999	1	2140
main/access/hmi/pwdcontrol	Operations	0 - 9999	1	2140
main/access/hmi/pwdsettings	Settings	0 - 9999	1	2140

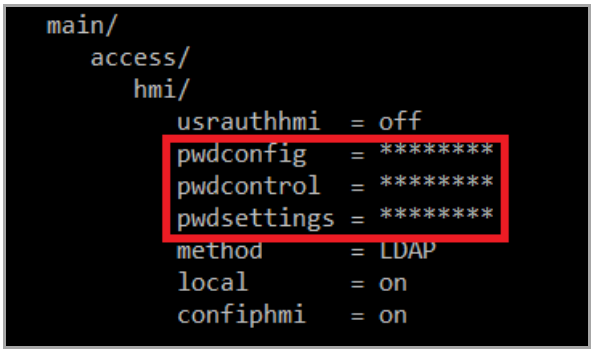


Figure F.20 HMI Passwords in CLI.

The remote change of local passwords via CLI facilitates the integration of device into centralized cybersecurity systems, allowing them to meet one of their main requirements: to periodically update device passwords.

When entering the password value, leading zeros are not entered. If, for example, the password is '0012', the digits to be entered will be '12'.

The menu options that are available with each of the passwords are listed below:

Password	HMI Menu Option
No password	*Information* menu. *USB* menu (if USB port activated and pendrive inserted): *Eject USB*. Access to *CLR* key to reset LEDs, trips, etc. Access to the *commandable objects* of the graphic display (accessible with SEL and executable with the O and | buttons). Access to *push buttons P1 to P12*.
Configuration	*Configuration* menu. *USB* menu (if USB port activated and pendrive inserted): *Storage dump*.
Operations	*Operations* menu.
Settings	*Activate Group* menu. *Change Settings* menu.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.3.4.b User and Password Authentication

When username/password use is required, the entered users are validated against the users available on the device, i.e., remote users (when using remote authentication methods such as LDAPS or RADIUS) and/or local users (when not using remote authentication methods or, if using remote authentication methods, they are not available and you have configured to use local users alternatively).

This user and password authentication option is only available on devices with enhanced cybersecurity.

Only access to the following menus will be possible without authentication:

- *Information*:
  - *Relay information*.
  - *Status*.
  - *Measurements*.
  - *Records*.

To access the rest of the menus it will be necessary to authenticate with username and password.

To log in or log out a user by HMI, one of the following two ways must be used:

- When in the default screen, pressing ENTER will take you to the first menu option:
  - When there is no user authenticated by HMI, the first menu option is **Login** and when you enter that option the login screen explained below is displayed.
  - When there is a user authenticated by HMI, the first menu option is **Logout** and when that option is entered, the logout screen explained below is displayed.
- If there is no HMI authenticated user and an attempt is made to access an area that requires a user, the login screen is automatically displayed.

The **login** screen initially has the focus on the user line.

Initially the character 'a' is displayed, with ↑ the next character option ('b') is displayed, with ↓ the previous character option is displayed, with → you advance to the next character, with ← you go back to the previous character (the current character is deleted). Pressing and holding down the ↑ or ↓ arrow speeds up the search for the desired character.

The possible character options are as follows (shown in order of appearance):

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . _ -
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Press ENTER to enter the password; the focus moves to the password field.

The way of entering the characters of the password is equivalent to that of the user. The order of displaying characters is: lowercase, uppercase, numbers and special characters in the order of the ASCII table:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 ! " # $ % & ' ( ) * + , - . / @
: ; < = > ? [ \ ] ^ _ ` { | } ~
```

Each character of the confirmed password (when ➔ is pressed) is graphically replaced by the '*' character to prevent the password from being seen.

Pressing ENTER completes the user and password entry and the device proceeds to authenticate the user. While the user is being authenticated, the message LOGIN IN PROGRESS is displayed.

If the user authentication is accepted by the device, an "L" character (login) is displayed on the HMI in the upper right corner. This allows to clearly identify when there is a user authenticated by HMI ("L" character present) or not ("L" character absent).

If the user authentication is rejected by the device, the message LOGIN FAILED / PRESS ANY KEY appears. When any key is pressed, the login screen is displayed again.

The **logout** screen requires confirmation: YES (➔) confirms the logout and NO (➔) or ESC cancels it and the user remains authenticated by HMI. While the user is being logged out, the message LOGOUT IN PROGRESS is displayed.

If ESC is pressed at any time within the login or logout screen, the login/logout window closes (in the case of logout the user would still be authenticated).

To log out (close user session) there are two options:

- A timeout after inactivity (no key presses, see **Automatic Logout** section): in this case the user returns to the main screen automatically.
- The user selects the option from the menu and confirms the logout.

A user authenticated by HMI counts as any other access for role concurrency (see **Users, Roles and Permissions** section). Therefore, a user by HMI can:

- Be expelled by another user (e.g., by web). In this case, the user is returned to the main screen, the HMI authenticated user indication is removed ("L" character in the display) and the **Logout - session closed by other user** cybersecurity event is generated with the user that has just been expelled.
- Expel another user. If the HMI user can expel a user and confirmation is required to do so (because it is about expelling another privileged user), after the login screen and confirmation that the user exists and is valid, a screen is presented to be able to expel the other user. This screen requires confirmation. If YES (➔) is chosen, the other user will be expelled and this HMI user will be authenticated. If NO (➔) is chosen or ESC is pressed, the HMI user authentication process is aborted and the **Login failed - user rejected due to role concurrency** cybersecurity event is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The menu options that are available with each of the permissions are listed below:

Permission	HMI menu option
Visualization	*Information* menu. *USB* menu (if USB port activated and pendrive inserted): *Eject USB*.
Command execution	*USB* menu (if USB port activated and pendrive inserted): *Storage Dump*. *Operations* menu. Access to *CLR* key to reset LEDs, trips, etc. Access to the *commandable objects* of the graphic display (accessible with SEL and executable with the O and | buttons). Access to *push buttons P1 to P12*.
Setting change	*Configuration* menu. *Activate Group* menu. *Change Settings* menu.
Configuration change	-
Firmware change	-
User management	-
Audit log	-

When a NOT allowed operation/option is selected, a PERMISSION DENIED message is displayed for a few seconds.

Examples where the PERMISSION DENIED message is displayed:

- A user without *command execution* permission presses P1.
- A user without *command execution* permission presses CLR.
- A user without *configuration change* permission tries to access *the Activate Group* menu.

F.3.5 Automatic Logout

A user's session is automatically logged out by the device after a period of inactivity. The concept of inactivity varies depending on the access:

- Communications: absence of communications messages (keep-alive in case of sockets are not taken into account). It affects HTTP, HTTPS, Telnet, SSH, FTP, SFTP and PROCOME services.
- HMI: no user interaction (keystrokes).
- USB (pendrive): no user interaction (key presses causing file download operations).

The device has the following setting, which can be modified from the configuration tool and from the HMI:

Configuration Tool	HMI	Range	Step	Default
Inactivity Timeout	`Inactivity Timeout`	1 – 60 min	1	5

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.4 Remote User Authentication

As described above, there is the possibility of local user authentication in the device. A series of local users and a series of roles with permissions are defined and a role is associated to each user. When a user authenticates, the device validates it against these local users.

Clients do not usually use local authentication on the device. They usually use centralized repositories where they configure their users with their associated roles. The device must authenticate users against these remote repositories using different standards. These repositories will return to the device, in case of positive user/password authentication, the user's role. In this way, the device will check internally if such role is defined in the device, the permissions assigned to such role in the device and will allow such user to perform the actions associated to such permissions.

The definition of users, roles and permissions using remote authentication is deployed as follows:

- Outside the device, in the remote repository, users are defined and their roles are associated with them.
- On the device, the roles and their associated permissions are defined (and additionally the local users with their roles).

This remote authentication option is only available on devices with enhanced cybersecurity.

As a general rule, the device can be configured to use remote or local authentication (local users of the device) and, in case of remote authentication, which remote authentication method to use (RADIUS or LDAP).

In addition, in case of using remote authentication, you can configure whether you want to use local users (local authentication) as an alternative source of authentication in case of impossibility to access the configured remote authentication repositories. If this option is chosen, the user/password authentication will be done locally (taking into account the local users defined in the device) when the requests to the remote repositories fail.

The following settings are defined for these two functionalities:

Authentication					
Website	**CLI**	**DevicePreferences**	**Range**	**Step**	**Default**
Authentication method	*main/access/xxxx/method*	method	local RADIUS LDAP		Local
Fallback to local access	*main/access/xxxx/local*	local	on (Yes) / off (No)		on (Yes)

where *xxxx* is the service name: web, telnet, ssh_sftp, ftp, procome and hmi.

These settings can be adjusted individually for each of the services requiring authentication: web access, telnet access, SSH/SFTP access, PROCOME access and HMI access.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

*If all **Fallback to local access** settings are set to **No** and the authentication methods for all services are set to a value other than **local**, the device will not be able to authenticate if the device is taken to the factory for repair or diagnostics, as it will not be possible to connect to the remote authentication servers and there will be no possibility of alternative use of local users.*

*It is therefore recommended that at least the HMI access be configured with **Fallback to local access** set to **Yes**.*

The device uses two remote authentication methods which are explained in detail below: RADIUS and LDAP.

F.4.1 RADIUS (Remote Authentication Dial In User Service)

The device acts as a RADIUS client to authenticate the user/password against up to two RADIUS servers (primary and secondary).

The device uses the RADIUS UDP client version specified by RFC 2865. The password is encrypted, but not the user. If more security is desired for RADIUS, alternative bump-in-the-wire methods, such as the use of VPN, should be employed.

For role notification by the server, the device processes the *Management-Privilege-Level* attribute (Type=136), explained in RFC 5607. This attribute contains the following fields:

- Type (1 byte): takes the value 136.
- Length (1 byte): takes the value 6.
- Value (4 bytes): this is an integer indicating the user's role. As private roles not predefined in IEC 62351-8 must take a negative value, this value is interpreted by the device as a signed integer (INT32).

When the device receives an Access-Accept message, it takes the role of this *Management-Privilege-Level* attribute and checks it against the list of roles it has defined:

- If it does not match any role or matches any role, but this one does not have *Visualization* permission, it shall refuse to authenticate the user.
- Otherwise, it must accept the user's authentication, take note of the permissions associated with that role and allow the user to execute only the operations associated with the permissions available to that role.

The RADIUS client settings are as follows:

RADIUS					
Website	**CLI**	**DevicePreferences**	**Range**	**Step**	**Default**
Main Server IP	*main/access/radius/server1_ip*	server1_ip	XXX.XXX.XXX.XXX		0.0.0.0
Backup Server IP	*main/access/radius/server2_ip*	server2_ip	XXX.XXX.XXX.XXX		0.0.0.0
Port	*main/access/radius/port*	port	1 – 65535	1	1812
Shared Secret	*main/access/radius/secret*	secret	8 – 128 chars		ziv12345
Timeout	*main/access/radius/timeout*	timeout	1 – 30 s	1	3
Number of Attempts	*main/access/radius/attempts*	attempts	1 – 10	1	3

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The meaning of the settings is as follows:

- *Main Server IP*: IP address of the primary RADIUS server. If **0.0.0.0** (default value) is set, it means that this server will not be used.
- *Backup Server IP*: IP address of the secondary RADIUS server. If **0.0.0.0** (default value) is configured, it means that this server will not be used.
- *Port*: Port on which the RADIUS servers operate. The default value is **1812** (UDP), which is the one reserved by RFC 2865.
- *Shared Secret*: Shared secret key between client and RADIUS server for password encryption. The default value is **ziv12345**. The length will range from 8 to 128 characters.
- *Timeout*: Maximum waiting time (in seconds) for obtaining the response from the RADIUS server. The default value is **3 seconds**.
- *Number of Attempts*: Number of attempts (not retries) to authenticate against a server before deciding that the server could not be accessed. The default value is **3 attempts**.

If both IPs are set to 0.0.0.0, it means that the RADIUS is disabled and therefore tries to validate the incoming user against local users, even if the *Authentication Method* setting is set to **RADIUS** and the *Fallback to Local Access* setting is set to **Off**.

For all other cases, upon receiving a login from a user, the device executes the following process if the *Authentication Method* setting is set to **RADIUS**:

1) Send an *Access-Request* to the primary server (or go to step 2 if the primary's IP is 0.0.0.0.0):

   1.1) If it replies, it no longer tries the secondary:
   - If the response is *Access-Reject*, the user is rejected and the process is terminated.
   - If the answer is *Access-Accept*:
     - And the role does not exist on the device, the user is rejected and the process is terminated.
     - And the role does not have *visualization* permission assigned, the user is rejected and the process is terminated.
     - Otherwise, the user is accepted and the permissions associated to the role received from the server are granted and the process ends.

   1.2) If the user does not answer in the *Timeout* setting:
   - If it has tried less than *Number of Attempts* times, go to step 1.
   - If it has tried *Number of Attempts* times, go to step 2 and the **RADIUS server not accessible** cybersecurity event is generated.

2) Repeat step 1, but now with the secondary server.
   If the IP of the secondary is 0.0.0.0, continue to step 3.

3) If the *Fallback to Local Access* setting is set to:
   - **On**, it attempts to validate the user and password against the local users of the device and terminates the process.
   - **Off**, the user is rejected and the process is terminated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.4.2 LDAP (Lightweight Directory Access Protocol)

The device acts as an LDAP client to authenticate the user/password against up to two LDAP servers (primary and secondary).

Authentication is performed by validating the user's credentials on the LDAP server. The LDAP client used is OpenLDAP 2.4.50. Simple synchronous authentication is supported according to the following summary procedure:

- Anonymous bind to LDAP server using anonymous authentication ("*Anonymous Authentication Mechanism of Simple Bind*" according to RFC 4513).
- Verification by the LDAP server of the username and password entered when opening a session via web, file transfer (FTP/SFTP), console access (Telnet/SSH), configuration tool (ICT) or other means, verifying that the username/password pair is correct.
- Reading the attribute defining the user's role (defined below), to apply the appropriate permissions to the user before granting access to the device by limiting, according to the role, the actions that the user can perform on the device.

The LDAP client settings are as follows:

LDAP					
Website	**CLI**	**DevicePreferences**	**Range**	**Step**	**Default**
Main Server IP	*main/access/ldap/ server1_ip*	IpAuth	XXX.XXX.XXX.XXX		0.0.0.0
Backup Server IP	*main/access/ldap/ server2_ip*	IpAuth2	XXX.XXX.XXX.XXX		0.0.0.0
Port	*main/access/ldap/ port*	port	1 – 65535	1	389
Timeout	*main/access/ldap/ timeout*	tRetryAuth	1 – 600 s	1 s	3 s
Number of Attempts	*main/access/ldap/ attempts*	NRetryAuth	1 – 10	1	3
Base DN	*main/access/ldap/ base_dn*	base_dn		0-100 chars	ou=users,dc=ziv,dc=es
Search Filter	*main/access/ldap/ search_filter*	search_filter		0-100 chars	objectClass=equiposSAS
Role Attribute	*main/access/ldap/ role_attribute*	role_attribute		0-60 chars	perfil-usu
Version	*main/access/ldap/ version*	version	2 – 3	1	3
Secure Connection	*main/access/ldap/ secure_cx*	secure_cx	Yes / No		Yes
Secure Protocol	*main/access/ldap/ secure_protocol*	secure_protocol	LDAPS / StartTLS		StartTLS

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The meaning of the settings is as follows:

- *Main Server IP*: IP address of the primary LDAP server. If **0.0.0.0** (default value) is set, it means that this server will not be used.
- *Backup Server IP*: IP address of the secondary LDAP server. If **0.0.0.0** (default value) is configured, it means that this server will not be used.
- *Port*: Port on which the LDAP servers operate. The default value is **389** (TCP), which is the one reserved according to RFC 4511.
- *Timeout*: Maximum waiting time (in seconds) for obtaining the response from the LDAP server. The default value is **3 seconds**.
- *Number of Attempts*: Number of attempts (not retries) to authenticate against a server before deciding that the server could not be accessed. The default value is **3 attempts**.
- *Base DN*: organizational unit (OU) in which users are stored in the LDAP server. The default value is **ou=users,dc=ziv,dc=en**. The length will range from 0 to 100 characters.
- *Search Filter*: additional search filter for the user, obviously together with the username (this will be done by the firmware by default). The default value is **objectClass=equiposSAS**. If no such filter is found, the user will not be validated. If an empty value is set, it means that the device will not perform this filter check to validate the user. The length will be between 0 and 100 characters.
- *Role Attribute*: name of the attribute that will contain the role of the user belonging to *Base DN* and that complies with the *Search Filter*. The default value is **perfil-usu**. If this attribute is not found on the server, the user will not be validated. If an empty value is set, the user will never be validated. The length will range from 0 to 60 characters.
- *Version*: version of LDAP to be used. The default value is **3** (LDAPv3).
- *Secure Connection*: indicates whether the connection to the LDAP server is secure or not. By default, a secure connection is used (**Yes**).
- *Secure Protocol*: secure protocol used if *Secure Connection* = **Yes**. The options are **LDAPS** or **StartTLS**. As the use of StartTLS is reserved for LDAPv3, if *Secure Connection* = **Yes** and *Version* = **2** are chosen, the LDAPS secure protocol (LDAP over SSL/TLS) will always be used regardless of the *Secure Protocol* parameter. The default value is **StartTLS**.

If both IPs are set to 0.0.0.0, it means that LDAP is disabled and therefore tries to validate the incoming user against local users, even if the *Authentication Method* setting is set to **LDAP** and the *Fallback to Local Access* setting is set to **Off**.

For all other cases, upon receiving a login from a user, the device, if the *Authentication Method* setting is set to **LDAP**, executes the following process:

1) If the device is able to connect to the primary server, continue to step 1.1.
   If it is not able to connect to the primary server, continue to step 1.2.
   If the IP of the primary is 0.0.0.0, continue to step 2.

   1.1) Send a *bindRequest* to the primary server indicating simple authentication, but without username and password (both zero length). This is known as *Anonymous authentication*.
   - If the response is *bindResponse* success, continue to step 1.1.1.
   - Otherwise, the user's authentication is rejected and the process is terminated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

1.1.1) Send a *searchRequest* to search for the user's role, consisting of:
- *baseObject* field equal to the *Base DN* setting.
- *Filter* field that is an AND of:
  - *Search Filter* setting (e.g., **objectClass=equiposSAS**).
  - *uid* equal to the name of the user to be authenticated (e.g., *uid=admin*).
- *attributes* field containing a single attribute whose *AttributeDescription* is the value of the *Role Attribute* setting (e.g., *perfil-usu*).

It must receive from the LDAP server as many *searchResEntry* as entries in the *Base DN* directory and match the indicated search criteria (theoretically one, if it hypothetically responds with more, the device will keep the first one), ending in a *searchResDone*. This means that if only *searchResDone* is returned, there are no entries in the directory.

- If the response is at least one *searchResEntry*, continue to step 1.1.1.1.
- Otherwise, the user's authentication is rejected and the process is terminated.

1.1.1.1) It sends a *bindRequest* to the primary server indicating simple authentication, with username and password (in clear). This is known as the *Name/Password Authentication Mechanism of Simple Bind*.
- If the response is *bindResponse* success, continue to step 1.1.1.1.1.
- Otherwise, the user authentication is rejected and the process is terminated.

1.1.1.1.1) The device takes the first *SearchResEntry* received in step 1.1.1.
The device checks the value of the role received from the server against the list of roles it has defined. The role attribute can contain a text string or an integer. Therefore, to be versatile, the device compares the value of that variable with (in this order):
- The role *name* field. It must match exactly (case sensitive).
- The role *identifier* field.

First the names are checked and then the role identifiers. The first role of the device that matches this search will be the chosen role. For better understanding, the following example of device roles is included:

# (role)	*Name*	*identifier*
1	VIEWER	-7
2	OPERATOR	-5
3	-7	3

If the role attribute received by LDAP is "-7", the chosen role will be #3, because the *name* field is checked first.
- If it does not match any role or it matches one, but it does not have *visualization* permission, the user authentication is rejected and the process is terminated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- If the check has been successful, the user authentication is accepted, takes note of the permissions associated with said role and allows the user to execute only the operations associated with the permissions available to said role and the process is finished.

1.2) If it does not answer or refuses the socket connection in the *Timeout* setting:
   - If it has tried less than *Number of Attempts* times, skip to step 1.
   - If it has tried *Number of Attempts* times, go to step 2 and generate the **LDAP repository not accessible** cybersecurity event.

2) Repeat step 1, but now with the secondary server.
If the secondary's IP is 0.0.0.0, continue to step 3.

3) If the *Fallback to Local Access* setting is a:
   - **On**, it attempts to validate the user and password against the local users of the device and terminates the process.
   - **Off**, the user authentication is rejected and the process is terminated.

At the end of the process, if it has been able to connect to the server, the device sends an *unbindRequest* before closing the connection to the LDAP server.

In the case of using a secure method (LDAPS or StartTLS), when connecting to the LDAP server, the device performs a TLS mutual authentication based on certificates. On the one hand, the device sends its device certificate so that it can be validated by the LDAP server. On the other hand, the device asks the LDAP server for its certificate and checks that the certificate sent by the LDAP server is valid based on the following checks:

- The remote certificate must be signed by one of the certificate authorities (CA) present in the list of CAs of the device. If it is not, the connection to the LDAP server is rejected and the **Certificate validation failed - certificate signature check failed** cybersecurity event is generated.
- The remote certificate must not be revoked, which is checked using certificate revocation lists (CRL) of the device. If the certificate is revoked, the connection to the LDAP server is rejected and the **Certificate validation failed - certificate revoked** cybersecurity event is generated.
- The remote certificate must not be expired (checking that the current date of the device is between the *Valid from* and *Valid to* dates of the server certificate). If the certificate is expired, the connection to the LDAP server is rejected and the **Certificate validation failed - certificate expired** cybersecurity event is generated.
- The remote certificate must contain the IP of the LDAP server in one of the following certificate fields: CN (Common Name) or SAN (Subject Alternative Name). If the IP does not appear in either of these two fields or appears but does not match the IP of the LDAP server, the connection to the LDAP server is rejected and the **Certificate validation failed - certificate does not comply with authorization policies** cybersecurity event is generated.

For details on how the certificate and lists of CAs and CRLs of the device are managed, see **Credential Management** section.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.4.3 Remote User Authentication Configuration

The configuration of remote user authentication must be performed by a user with *user management* permission. Remote user authentication is managed from several interfaces:

- Web interface (HTTP / HTTPS).
- CLI command line interface (Telnet / SSH).
- ***ZIV e-NET Tool***® configuration tool, using the *DevicePreferences* file.

F.4.3.a Remote User Authentication Configuration from the Web

To manage remote user authentication from the web interface, some of the LAN ports and the HTTP or HTTPS services must be enabled. It is recommended to use HTTPS connection instead of HTTP because the data is encrypted.

The website of the device is accessed through a browser by entering the IP address configured in the LAN adapter of the device. Initially, a login web page appears where the user's name and password must be entered (*admin* is the default user).

The ***Configuration→Access*** menu is accessed to manage the following information related to remote authentication:

- Configuration of the authentication method for each access:

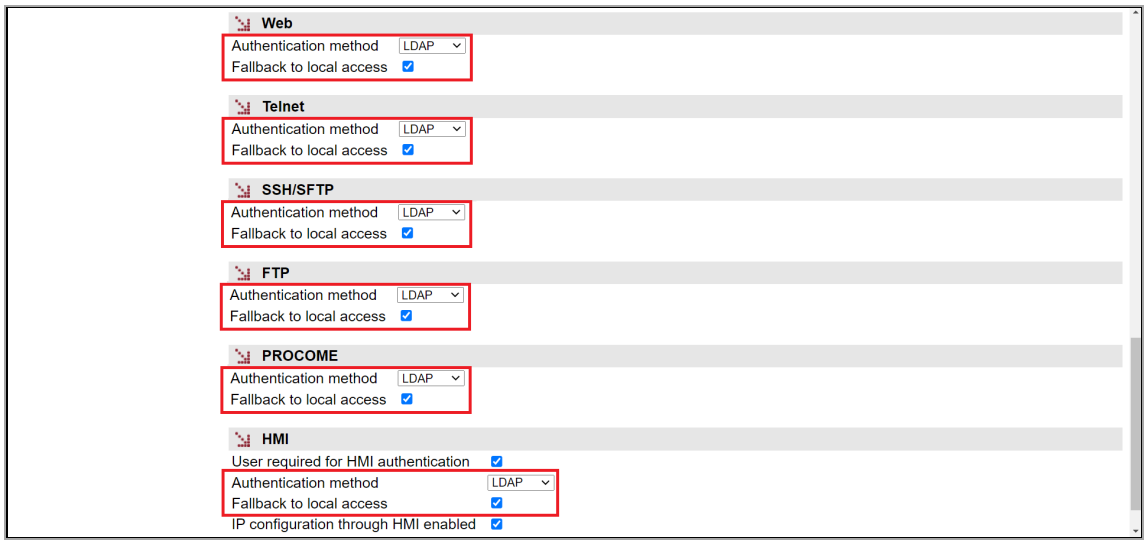


Figure F.21 Authentication Method Settings in Website.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- RADIUS Configuration:

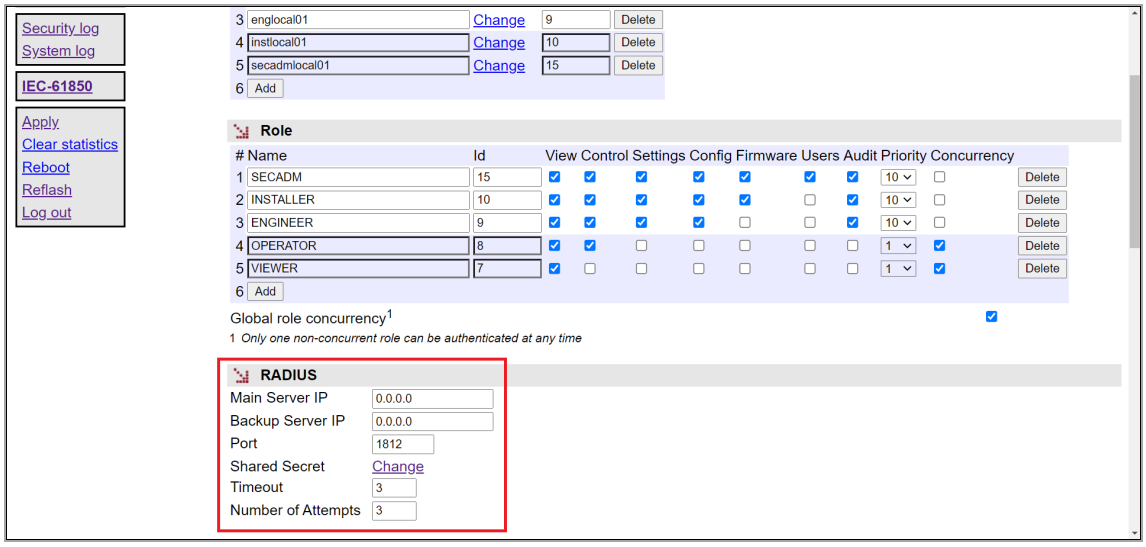


Figure F.22 RADIUS Settings in Website.

To change the secret key, proceed in the same way as for changing a user's password (Figure F.5).

- LDAP Configuration:

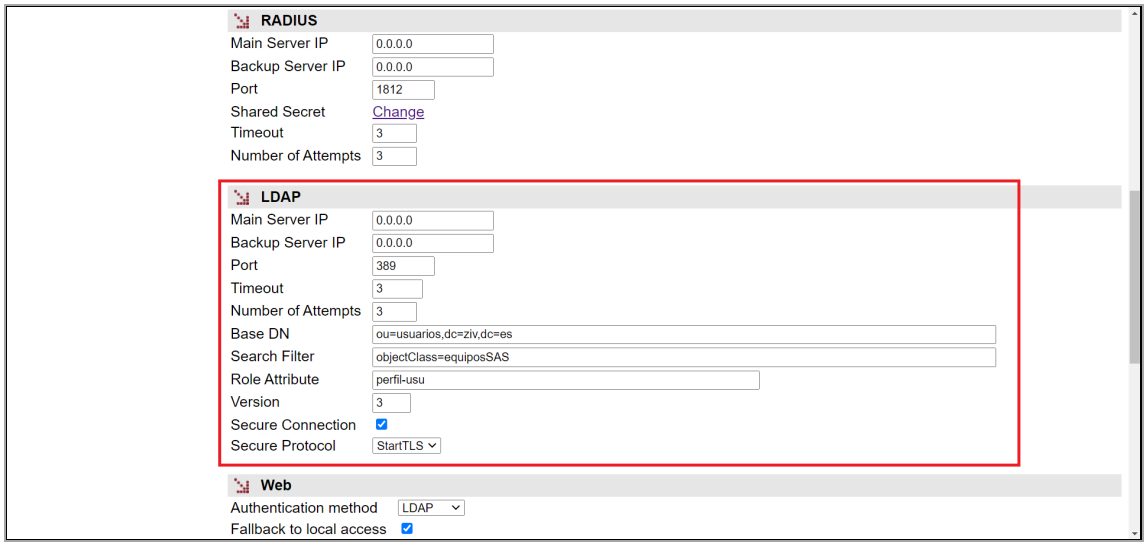


Figure F.23 LDAP Settings in Website.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.4.3.b Remote User Authentication Configuration from CLI

To manage remote user authentication from the CLI command line interface, one of the LAN ports and the Telnet or SSH services must be enabled. It is recommended to use the SSH connection instead of Telnet because the data is encrypted.

The CLI of the device is accessed by launching the Telnet or SSH application from a host and entering the login of the user who has user management permissions.

The CLI of the device is automatically accessed. The parameter tree can be viewed with the ***get*** command. The settings for remote user authentication are in the ***main/access*** node:

- Configuration of the authentication method for each of the accesses:

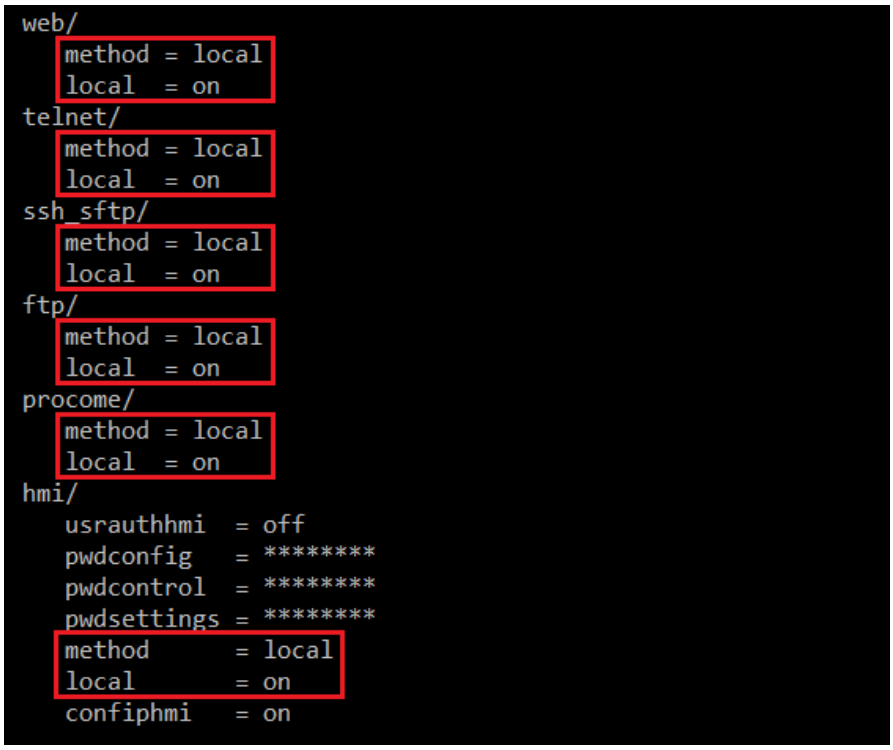


Figure F.24 Authentication Method Settings in CLI.

- RADIUS Configuration:

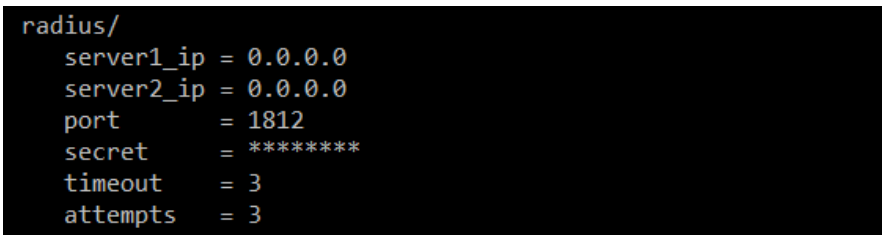


Figure F.25 RADIUS Settings in CLI.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- LDAP Configuration:

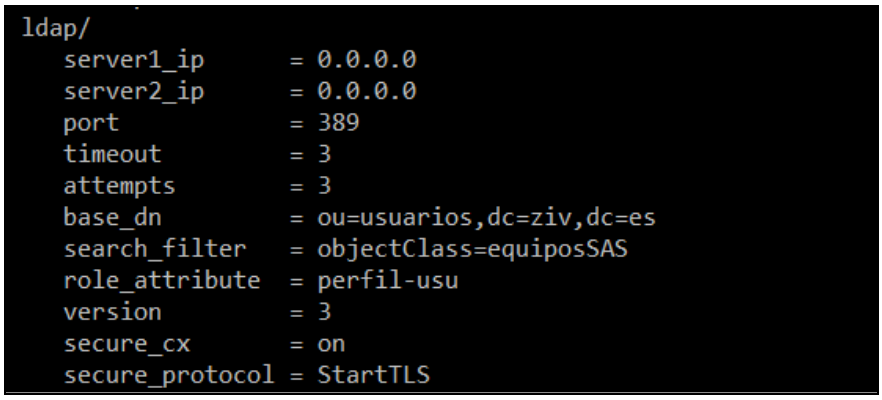


Figure F.26 LDAP Settings in CLI.

To change a setting, proceed by executing the ***set*** command with the name of the setting and the device will ask for the value, or by directly executing the ***set*** command of the field to be modified, for example:

- ***set main/access/web/method local***
- ***set main/access/radius/timeout 5***
- ***set main/access/radius/secret*** (entering the key value twice).
- ***set main/access/ldap/port 636***

Once the desired settings have been configured, the data are saved with the ***save*** command and the changes are made effective on the device with the ***apply*** command.

F.4.3.c Remote User Authentication Configuration from *ZIV e-NET Tool®*

To manage remote user authentication from the ***ZIV e-NET Tool®*** it is necessary that some of the LAN ports and the SSH and SFTP services are enabled.

Remote user authentication is configured with the *DevicePreferences* file.

- Configuration of the authentication method for each of the accesses:

  To configure the authentication methods for the different accesses, in the ***Navigation View*** go to the ***Preferences→Security→Access*** option.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

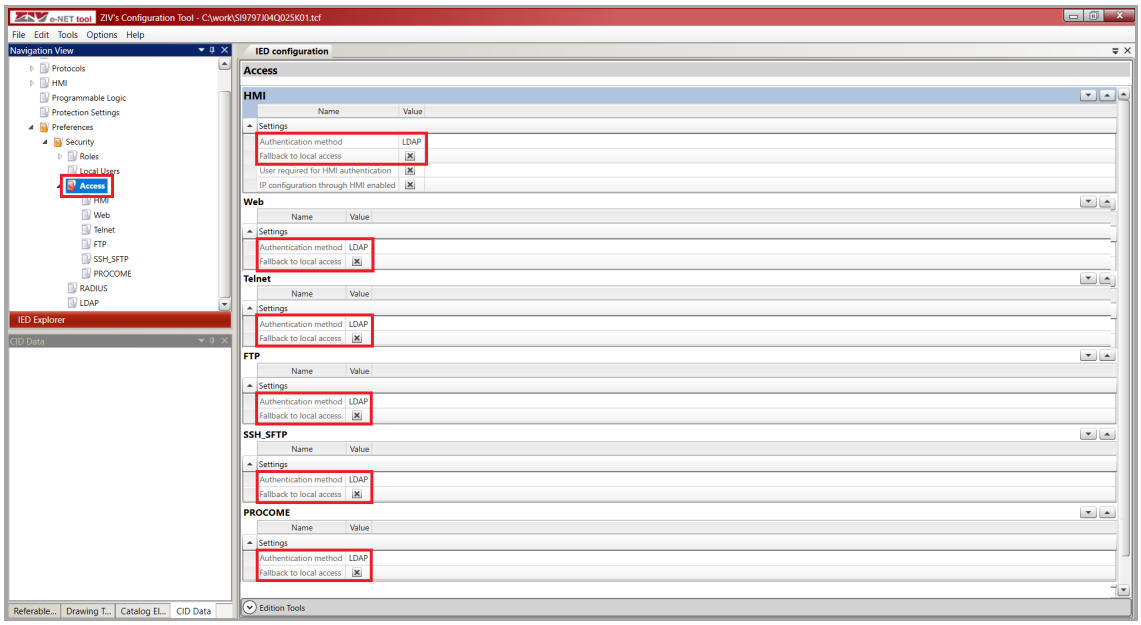


Figure F.27 Configuring the Authentication Method for each Access with the Configuration Tool.

By right-clicking on this option ***Preferences→Security→Access***, you can export the authentication methods to a *DevicePreferences* file or import them from a previously configured *DevicePreferences* file.

The authentication methods for each access are part of the *DevicePreferences* file. This is an XML file whose authentication methods section has the following format (settings are highlighted):

Node	Description	Child nodes	Attributes
device	Root node.	ROLES, RADIUS, LDAP, **ACCESS**	**tversion**: file version. **filetype**: type of file ("DevicePreferences").
ACCESS	Access parameters.	**HMI**, **WEB**, **TELNET**, **FTP**, **SSH_SFTP**, **PROCOME**	-
HMI	Definition of authentication method for HMI access: method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each HMI access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for HMI access (local, LDAP or RADIUS). - **local**: alternative use of local users for HMI access. - **userauthhmi**: role name. - **confiphmi**: it is allowed to change the IP by HMI. **value**: setting value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Node	Description	Child nodes	Attributes
WEB	Definition of authentication method for web access (HTTP/HTTPS): method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each web access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for web access (local, LDAP or RADIUS). - **local**: alternative use of local users for web access. **value**: setting value.
TELNET	Definition of authentication method for Telnet access: method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each Telnet access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for Telnet access (local, LDAP or RADIUS). - **local**: alternative use of local users for Telnet access. **value**: setting value.
FTP	Definition of authentication method for FTP access: method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each FTP access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for FTP access (local, LDAP or RADIUS). - **local**: alternative use of local users for FTP access. **value**: setting value.
SSH_SFTP	Definition of authentication method for SSH/SFTP access: method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each SSH/SFTP access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for SSH/SFTP access (local, LDAP or RADIUS). - **local**: alternative use of local users for SSH/SFTP access. **value**: setting value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Node	Description	Child nodes	Attributes
PROCOME	Definition of authentication method for PROCOME access: method and alternative use of local users.	**Setting**	-
Setting	One **Setting** node for each PROCOME access setting.	-	**name**: setting name. The following settings are available: - **method**: authentication method for PROCOME access (local, LDAP or RADIUS). - **local**: alternative use of local users for PROCOME access. **value**: setting value.

Example of *DevicePreferences* file (only with access section, authentication method settings are highlighted):

```
<?xml version="1.0" encoding="utf-8"?>
<device tversion="0.1" fileType="DevicePreferences">
 <ACCESS>
  <HMI>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
   <Setting name="usrauthhmi" value="Yes" />
   <Setting name="confiphmi" value="Yes" />
  </HMI>
  <WEB>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
  </WEB>
  <TELNET>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
  </TELNET>
  <FTP>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
  </FTP>
  <SSH_SFTP>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
  </SSH_SFTP>
  <PROCOME>
   <Setting name="method" value="LDAP" />
   <Setting name="local" value="Yes" />
  </PROCOME>
 </ACCESS>
</device>
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To transfer the authentication methods for the different accesses to the device, access the ***Tools→Device access*** menu. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Transfer Files*** tab, check the ***TCF→Preferences*** option (if you want to transfer the complete *DevicePreferences* file), the ***TCF→Preferences→Access*** option (if you want to transfer the complete access section) or the ***TCF→Preferences→Access→XXX*** option (where XXX=HMI, Web, Telnet, FTP, SSH_SFTP or PROCOME if you want to transfer a particular access section, this is the minimum section that can be sent) and click ***Transfer*** to upload the information to the device. The upload progress is indicated in the ***Information*** window. If it has been successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if there is any error in the validation by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

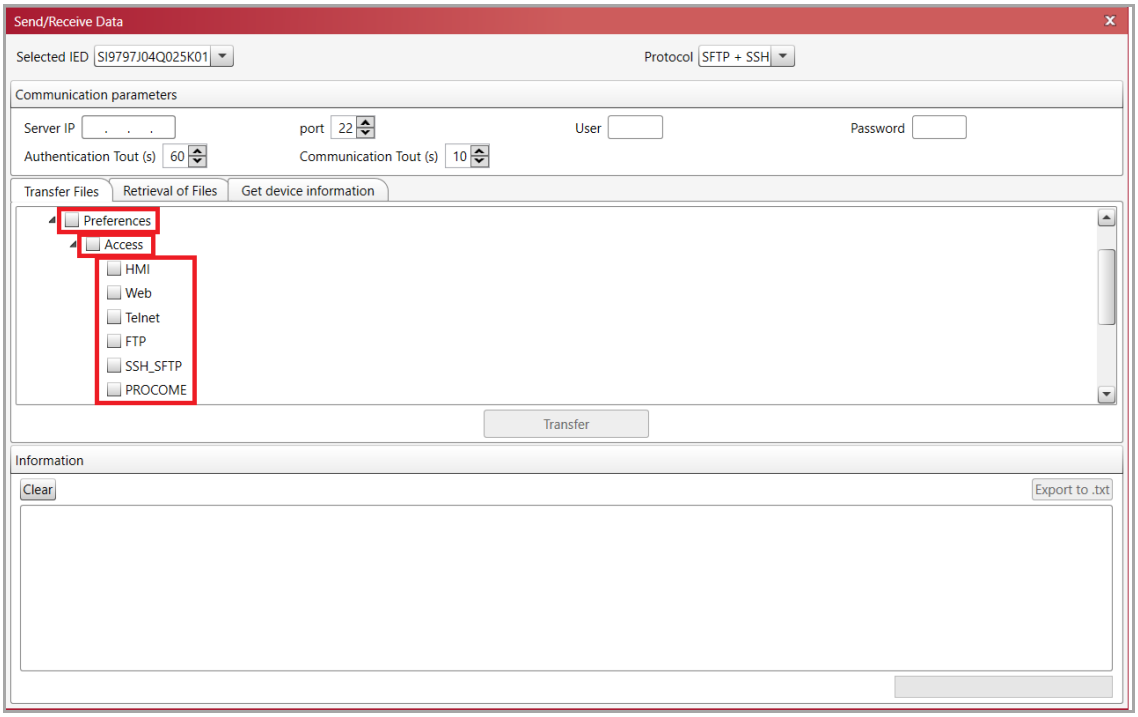


Figure F.28 Sending Authentication Methods with Configuration Tool.

To retrieve the authentication methods for the different accesses of the device, proceed as indicated in the **User and Role Management from ZIV e-NET Tool®** section for the roles, as it is only possible to retrieve the complete *DevicePreferences* file.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- RADIUS Configuration:

  To configure RADIUS, in the ***Navigation View*** go to the ***Preferences→Security→RADIUS*** option.

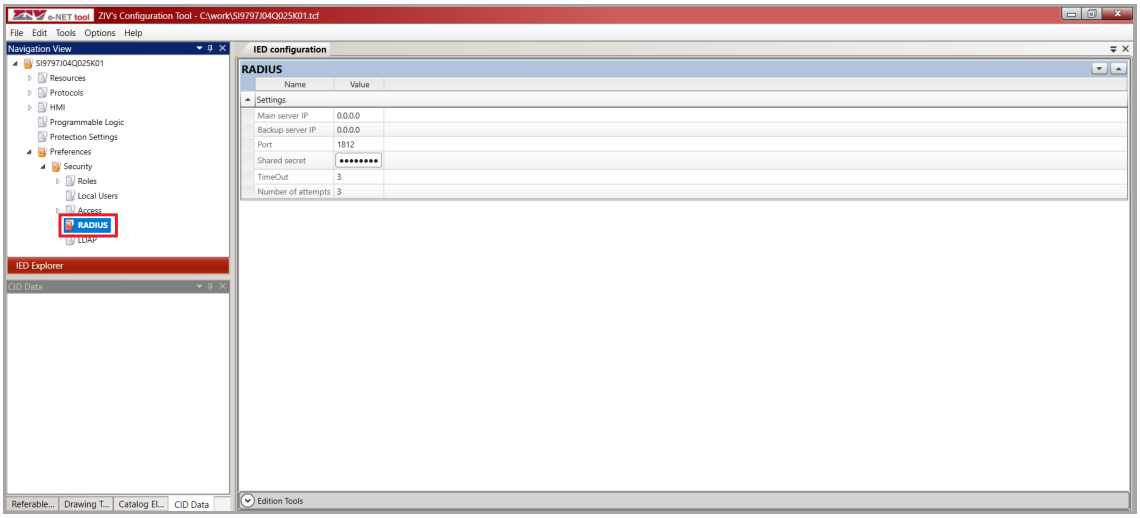


Figure F.29 RADIUS Configuration with Configuration Tool.

By right-clicking on this option ***Preferences→Security→RADIUS***, you can export the RADIUS settings to a *DevicePreferences* file or import them from a previously configured *DevicePreferences* file.

The RADIUS settings are part of the *DevicePreferences* file. This is an XML file whose RADIUS section has the following format:

Node	Description	Child nodes	Attributes
device	Root node.	ROLES, **RADIUS**, LDAP, ACCESS	**tversion**: file version. **filetype**: type of file ("DevicePreferences").
RADIUS	Parameters for RADIUS remote authentication	**Setting**	-
Setting	One **Setting** node for each RADIUS setting.	-	**name**: setting name. The following settings are available: - **server1_ip**: IP address of the primary RADIUS server. - **server2_ip**: IP address of the secondary RADIUS server. - **port**: RADIUS server port. - **secret**: password encryption key. - **timeout**: RADIUS server response waiting time. - **attempts**: authentication attempts against the RADIUS server. **value**: setting value.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Example of *DevicePreferences* file (only with RADIUS section):

```
<?xml version="1.0" encoding="utf-8"?>
<device tversion="0.1" fileType="DevicePreferences">
   <RADIUS>
   <Setting name="server1_ip" value="0.0.0.0" />
   <Setting name="server2_ip" value="0.0.0.0" />
   <Setting name="port" value="1812" />
   <Setting name="secret" value="ziv12345" />
   <Setting name="timeout" value="3" />
   <Setting name="attempts" value="3" />
  </RADIUS>
</device>
```

To transfer RADIUS settings to the device, access the ***Tools→Device access*** menu. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Transfer Files*** tab, check the ***TCF→Preferences*** option (if you want to transfer the entire *DevicePreferences* file) or the ***TCF→Preferences→RADIUS*** option (if you want to transfer only the RADIUS section) and click ***Transfer*** to upload the information to the device. The upload progress is indicated in the ***Information*** window. If it has been successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if there is any error in the validation by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

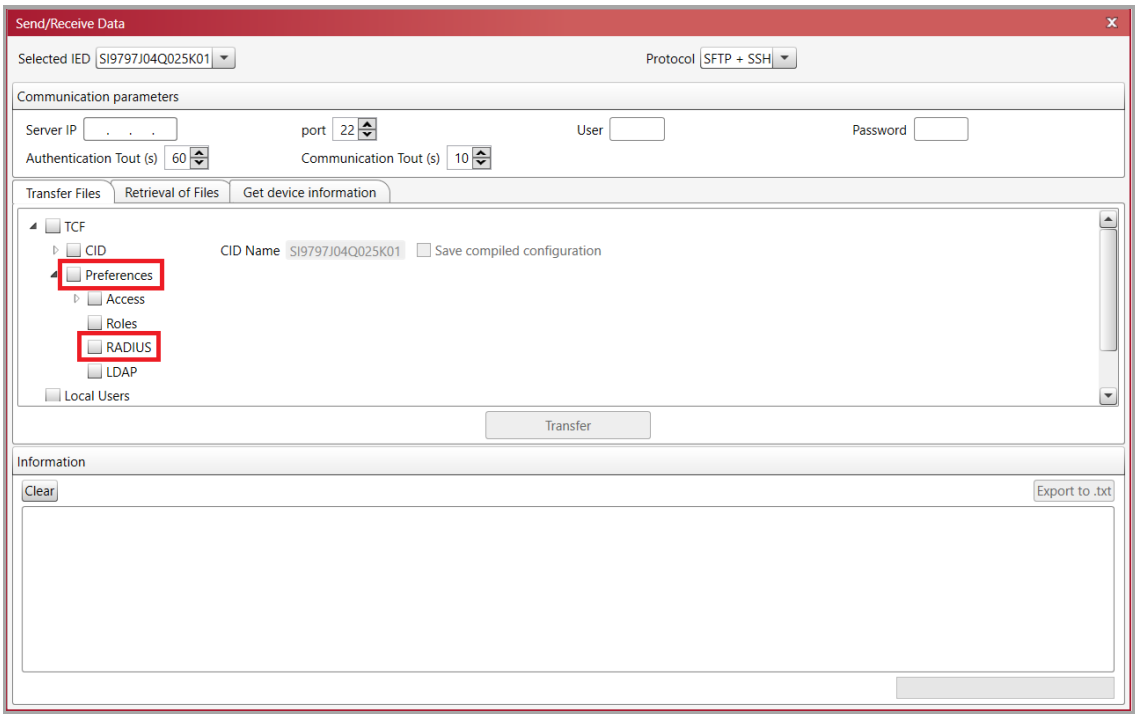


Figure F.30 Sending RADIUS Settings with Configuration Tool.

To retrieve the RADIUS settings of the device, proceed as indicated in the **User and Role Management from ZIV e-NET Tool®** section for the roles, as it is only possible to retrieve the complete *DevicePreferences* file.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- LDAP Configuration:

  To configure LDAP, in the ***Navigation View*** go to the ***Preferences→Security→LDAP*** option.

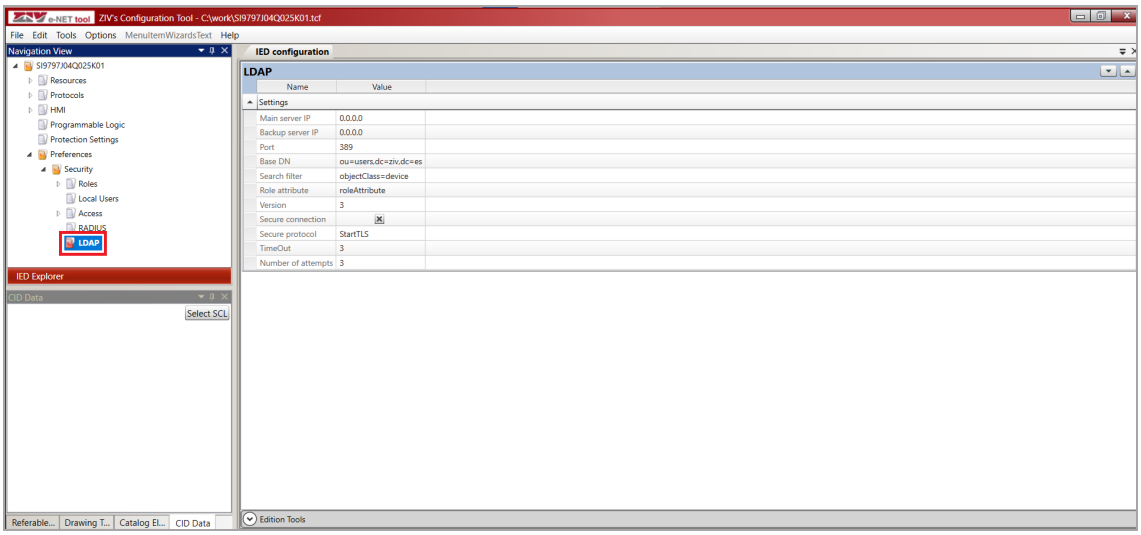


Figure F.31 LDAP Configuration with Configuration Tool.

By right-clicking on this option ***Preferences→Security→LDAP***, you can export the LDAP settings to a *DevicePreferences* file or import them from a previously configured *DevicePreferences* file.

The LDAP settings are part of the *DevicePreferences* file. This is an XML file whose LDAP section has the following format:

Node	Description	Child nodes	Attributes
device	Root node.	ROLES, RADIUS, **LDAP**, ACCESS	**tversion**: file version. **filetype**: type of file ("DevicePreferences").
LDAP	Parameters for LDAP remote authentication.	-	**lpAuth**: IP address of the primary LDAP serve. **lpAuth2**: IP address of the secondary LDAP serve. **port**: LDAP server port. **tRetryAuth**: LDAP server response time. **NRetryAuth**: authentication attempts against the LDAP server. **base_dn**: organizational unit (OU) in which users are stored on the LDAP server. **search_filter**: additional search filter for the user. **role_attribute**: name of the attribute containing the user role. **version**: LDAP version.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Node	Description	Child nodes	Attributes
LDAP	Parameters for LDAP remote authentication.	-	**secure_cx**: indicates whether the LDAP connection is secure or not. **secure_protocol**: indicates the secure protocol to be used.

Example of *DevicePreferences* file (only with LDAP section):

```
<?xml version="1.0" encoding="utf-8"?>
<device tversion="0.1" fileType="DevicePreferences">
  <LDAP tRetryAuth="3" NRetryAuth="3" port="389" IpAuth="192.168.1.69"
  IpAuth2="0.0.0.0" role_attribute="perfil-usu" version="3" secure_cx="Yes"
  secure_protocol="StartTLS" base_dn="ou=usuarios,dc=ziv,dc=es"
  search_filter="objectClass=equiposSAS" />
</device>
```

To transfer LDAP settings to the device, access the ***Tools→Device access*** menu. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Transfer Files*** tab, check the ***TCF→Preferences*** option (if you want to transfer the entire *DevicePreferences* file) or the ***TCF→Preferences→LDAP*** option (if you want to transfer only the LDAP section) and click ***Transfer*** to upload the information to the device. The upload progress is indicated in the ***Information*** window. If it has been successfully uploaded to the device, the **Configuration uploaded successfully** cybersecurity event is generated. However, if there is any error in the validation by the device, the **Configuration upload failed - invalid configuration** cybersecurity event is generated.

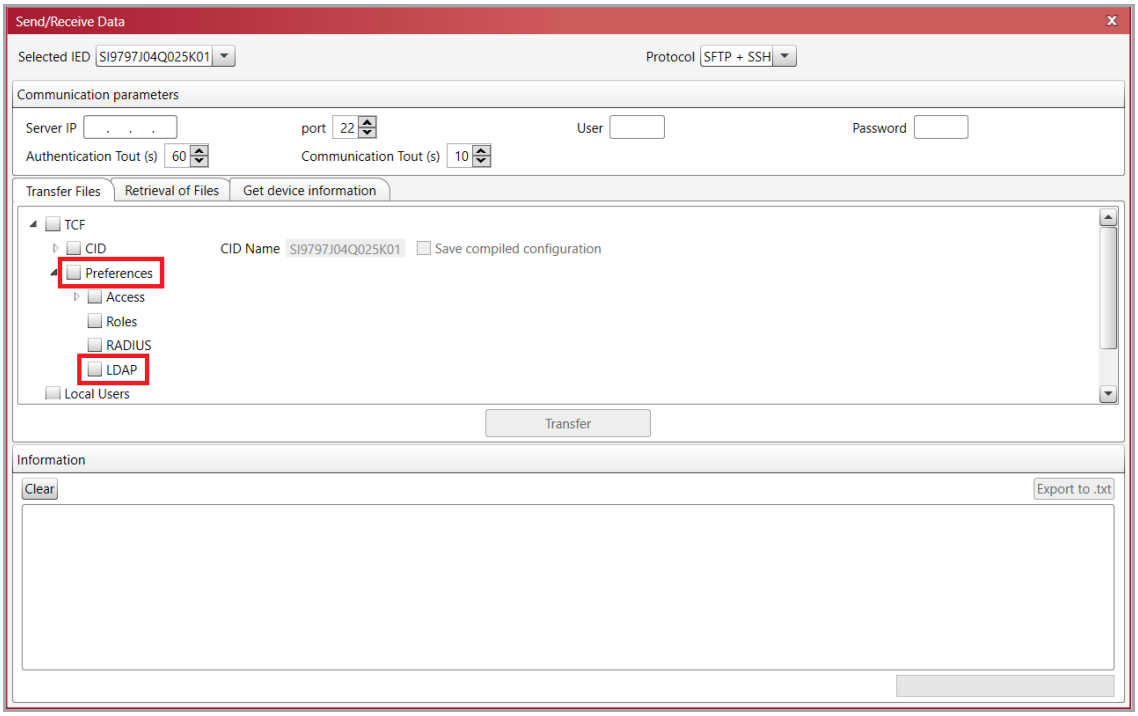


Figure F.32 Sending LDAP Settings with Configuration Tool.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

To retrieve the LDAP settings of the device, proceed as indicated in the **User and Role Management from ZIV e-NET Tool®** section for the roles, as it is only possible to retrieve the complete *DevicePreferences* file.

F.5 Communication with Configuration Tool using PROCOME

Zivercomplus® and ***ZIV e-NET Tool®***[1] communications with the device use PROCOME protocol. This PROCOME protocol has been strengthened so that communications are authenticated and encrypted (the latter only in the case of LAN port communication).

Authentication is based on a new private ASDU that includes user and password, replacing ASDU 116, which only uses a password.

On the other hand, for LAN port communications, there is the possibility for the protocol to use encryption, using TLS v1.2.

The different instances of communication with PROCOME protocol that can be present in the device are:

- Local Port.
- Remote Port 1 and 2.
- LAN ports: one fixed PROCOME instance and four more configurable instances (TCP/IP Protocol 1, 2, 3 and 4).

The settings for configuring whether each of the PROCOME instances is authenticated and/or encrypted (the latter only in case of LAN port communication) are detailed in Chapter 1, **Description and Start-up**, **Communication Settings** section.

By default, all instances are set with authentication except for the local port. Therefore, any session opened through an authenticated connection will require the user/password to be entered on the device at the start of the connection.

The authenticated local port setting can only be adjusted from HMI.

Only instances that communicate over LAN ports (PROCOME Protocol and TCP/IP Protocols), can be configured to work with encryption, and by default they are adjusted to encrypted mode. For more details on the type of encryption used, see **Secure Sockets** section. Each of these instances also has an adjustable logical port number.

In TCP/IP protocols, encryption and authentication only affect the PROCOME protocol. The other configurable protocols, DNP3 and MODBUS, are not affected by these settings.

*When communicating the configuration tools with the device via LAN, the user must configure the **secure** / **non-secure** communications option in the tool, according to the corresponding PROCOME instance that has been configured as **encrypted** / **not encrypted** on the device. If they do not match, communication will not be possible.*

[1] ***ZIV e-NET Tool®*** also uses other protocols such as SFTP and SSH to communicate with the device.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.6 Secure Sockets

In order to prevent communications from being spied on, a suitable countermeasure is to encrypt communications using secure sockets.

The device uses the secure (encrypted) versions of the following protocols:

Protocol	Secure Version
Telnet	SSH
FTP	SFTP
HTTP	HTTPS
PROCOME	PROCOME over TLSv1.2
LDAP	LDAPS/StartTLS

F.6.1 SSH (Secure Shell)

Secure Shell is a cryptographic network protocol for securing communications. It establishes a secure channel over an insecure network in a client/server architecture.

In the case of the device, it provides an SSH server that allows SSH clients to connect in an authenticated manner (login) for maintenance functions by using the command line interface (CLI).

This protocol is a direct and secure replacement for the Telnet interface.

The encryption used by SSH provides confidentiality and data integrity over an insecure network, such as the Internet.

SSH uses public key cryptography to authenticate the remote machine and allow the user to authenticate.

The protocol version used on the device is SSH Version 2 (SSHv2).

The device supports both Telnet and SSH (see **Ports and Communication Services** section to see how to enable / disable one, the other or both).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.6.2 SFTP (SSH File Transfer Protocol)

SSH File Transfer Protocol (also known as Secure File Transfer Protocol) is a network protocol that provides file access, file transfer and file management functionality over SSH. It works together with SSH to provide secure file transfer capabilities.

This protocol assumes that it is running on a secure channel, such as SSH, that the server has already authenticated the client, and that the client's user identity is available to the protocol.

The encryption and authentication aspects for this protocol are handled by the SSH server also running on the device. Therefore, the encryption and authentication methods are identical to those for SSH described above.

The device supports both FTP and SFTP (see **Ports and Communication Services** section for how to enable/disable one, the other or both).

F.6.3 TLS / SSL (Transport Layer Security / Secure Socket Layer)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over a TCP/IP network. They use the X.509 certificate and, therefore, asymmetric cryptography to authenticate the machine they are communicating with and to exchange a symmetric session key. This session key is used to encrypt the data flowing between the two parties. This allows data confidentiality and message authentication codes for message integrity and, in addition, message authentication.

In Internet Protocol Suite, TLS and SSL encrypt the network connection data at the application layer. In OSI model equivalencies, TLS/SSL is initialized at layer 5 (session layer) and functions as layer 6 (presentation layer). The session layer has a link protocol that uses asymmetric encryption to set up encryption configurations and a shared key for that session. The presentation layer then encrypts the rest of the communication using symmetric encryption and that session key. In both models, TLS and SSL work on behalf of the underlying transport layer, whose segments carry encrypted data.

In the device, TLS is only used for the Secure Web Server (HTTPS) application and for PROCOME, which is explained in the **Communication with Configuration Tool using PROCOME** section.

The TLS version supported is TLSv1.2. During TLS negotiation, the most secure option common to both client and server is always chosen.

The SSL1, SSL2, SSL3, TLSv1.0 and TLS v1.1 protocols are not available on the device as they are considered insecure.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.6.4 HTTPS (Secure Web Server)

The Secure Web Server application uses the Hypertext Transfer Protocol (HTTPS) which is a communications protocol for secure communication over a network.

Technically it is not a protocol per se but is the result of simply placing the Hypertext Transfer Protocol (HTTP) over the SSL/TLS protocol (explained in the previous section), thus adding the security capabilities of SSL/TLS for standard HTTP communications.

The security of HTTPS is that of the underlying SSL / TLS, which uses long-term public and secret keys to exchange a short-term session key to encrypt the data flow between a client and a server.

The X.509 certificate is used to ensure that you are communicating to the peer you want to communicate with.

In its popular implementation on the Internet, HTTPS provides authentication of the website and the associated web server. In addition, it provides bi-directional encryption of communications between a client and a server, which protects against eavesdropping and manipulation and / or falsification of the communication content.

A website must be fully supported over HTTPS, without having some of its content uploaded over HTTP, or the user will be vulnerable to some attacks and surveillance.

The device supports both HTTP and HTTPS (see **Ports and Communication Services** section for how to enable/disable one, the other or both).

F.6.5 Mutual Authentication

Mutual authentication or two-way authentication (not to be confused with two-factor authentication) refers to two ends of a communication authenticating each other at the same time in an authentication protocol. Mutual authentication is a desired feature in verification schemes that transmit sensitive data, in order to ensure the security of such data. Mutual authentication can be achieved with two types of credentials: user/password and public key certificates.

Two scenarios are distinguished in the device:

- Communications using TLS protocol:
  Mutual authentication is performed based on X.509 certificates. The device sends its certificate so that it can be validated by the other end and additionally requires the remote end to send its certificate to perform the pertinent checks and validate it. In HTTPS and PROCOME communications over TLS (in this second case if it is configured to be authenticated) a second authentication factor consisting of user and password is additionally required.
- Communications using SSH protocol:
  Mutual authentication is performed as follows:
  - Server authentication is performed based on the server's public key. That is, all clients communicating with the device using SSH will need to include the public key of the device among their known hosts if they want to check the validity of the server.
  - Client authentication is based on username/password authentication. In other words, clients connecting to the device must enter username and password in order to be validated by the device (they will be checked against remote servers or against local users, as explained in the **Remote User Authentication** section).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

The device manages a single common private key for TLS and SSH communications. There is, therefore, a single place where the private key and certificate of the device are configured. When new credentials (private key/certificate) are uploaded to the device, the public key used by SSH is derived internally from those credentials by software within the device.

Root certificates, used to validate remote certificates received by the device during TLS communications, are common to all services using TLS (HTTPS, secure LDAP or encrypted PROCOME LAN). They correspond to the list of Certificate Authorities (hereinafter CA) of the device. When a device has a list of CAs configured (by default the device is configured with the ZIV CA), the device will require TLS mutual authentication, although this mutual authentication can be disabled per service as explained in the **Credential Management** section.

Devices with basic cybersecurity do not perform TLS mutual authentication.

The process for validating a remote certificate is as follows:

- The remote certificate is validated against the list of CAs of the device. If the certificate is not trusted (not signed by any of the CAs present in the list), the communication is rejected and the **Certificate validation failed - certificate signature check failed** cybersecurity event is generated.

- The revocation of the remote certificate is checked against the CRL (Certificate Revocation List) of the device. If the certificate is revoked, the communication is rejected and the **Certificate validation failed - certificate revoked** cybersecurity event is generated.

- The remote certificate is checked for expiration (the certificate is expired or not yet valid). If the certificate is expired, the communication is rejected and the **Certificate validation failed - certificate expired** cybersecurity event is generated.

- Additional validations can be performed on the remote certificate expressed in an authorization policy file based on certificate details (fingerprint and CN and OU fields) which are detailed in the **Credential Management** section. If the certificate does not comply with these authorization policies, the communication is rejected and the **Certificate validation failed - certificate does not comply with authorization policies** cybersecurity event is generated.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.7 Credential Management

Credential management refers to the way in which the entire public key infrastructure (hereinafter PKI) is managed within the device. The following shows how the certificate and private key of the device are managed (the only thing available in devices with basic cybersecurity), as well as the list of certification authorities (CAs), the certificate revocation list (CRLs) and the authorization policy file for devices with enhanced cybersecurity.

F.7.1 Devices with Basic Cybersecurity

In devices with basic cybersecurity, the PKI consists only of a certificate and private key that allow the device to perform secure communications without TLS mutual authentication capability, i.e., without performing any type of remote certificate verification.

By default, the devices at the first boot up generate a self-signed X.509 certificate with a 2048-bit RSA public key and a 2048-bit private key, both in PEM format.

The self-signed certificate generated has the following identifiers and validity period:

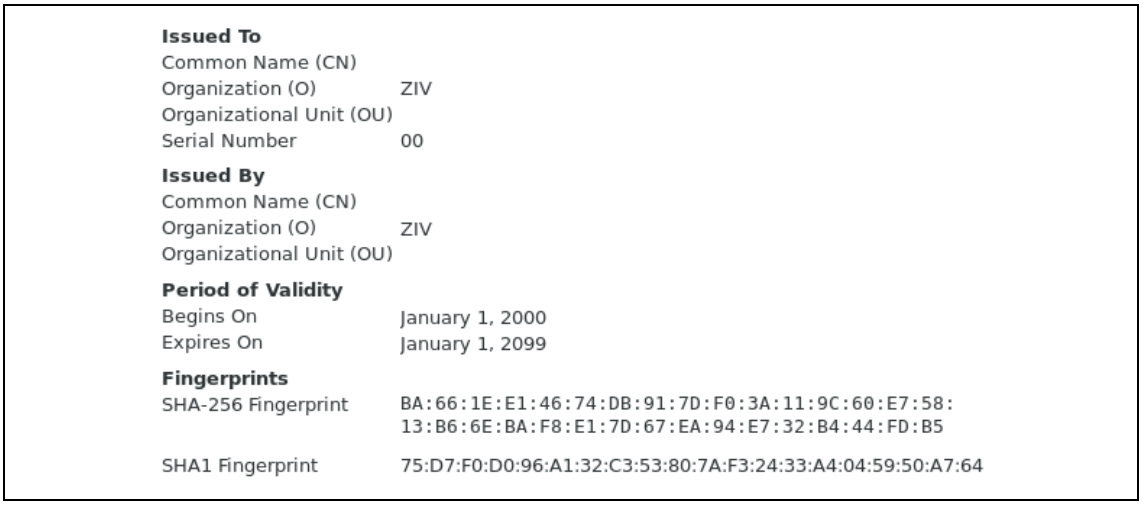


Figure F.33 Characteristics of the Self-Signed Certificate for Devices with Basic Cybersecurity.

This certificate and its private key are provisional and should be replaced by the client with a trusted certificate and its corresponding private key. For this purpose, the device has a menu on the website that allows the upload of a new certificate and private key, as well as the download of the current certificate.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

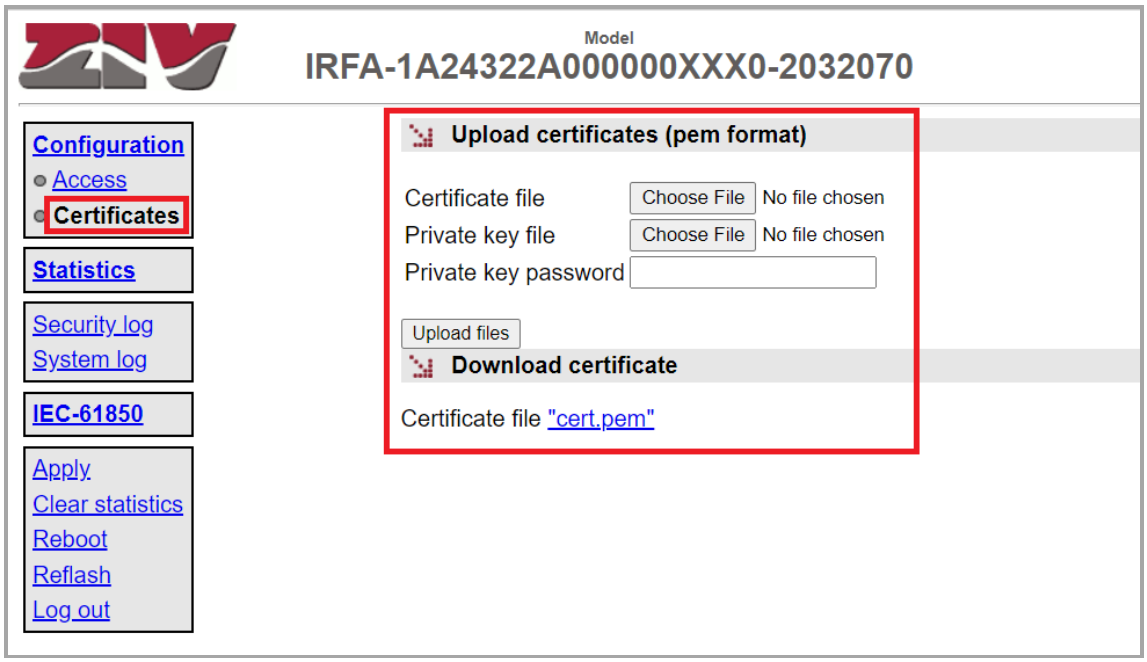


Figure F.34 Certificate and Private Key Configuration on Website for Devices with Basic Cybersecurity.

The certificate management operation is as follows:

- Access to the certificate menu of the device is only possible with a user with *user management* permission.
- The certificate and private key upload option are only available with HTTPS connections. In case of using an unsecured connection (HTTP), only the certificate download is allowed.
- Only certificates and private keys in PEM format can be uploaded to the device. The private key can be either clear or encrypted with AES encryption.
- From the website you can select the certificate (***Certificate File***), the private key (***Private Key File***) and the encryption key of the private key (***Private Key Password***).
- You can upload the certificate and the private key individually or simultaneously with the ***Upload files*** button, selecting the ***Choose File*** button to choose the file corresponding to the certificate and/or the private key.
- When only the certificate is uploaded, it must be paired with the private key already stored in the device, or else a verification error will occur. In this case, the uploaded file is discarded. The same thing happens with the private key.
- If no value is entered in the encryption key of the private key, then the private key is considered not to be encrypted. If the password is entered, the private key is decrypted with said password and re-encrypted with a password specific to the device using the AES 256 CBC algorithm. The password entered by the user is not stored in the device in any case.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- After pressing the ***Upload files*** button, a certificate and/or private key check is performed. If there is an error, it will be indicated to the user with a message and the uploaded files will be discarded.

- From the website it is possible to download the current certificate (***Download Certificate***), but in no case the private key.

- Once the files have been uploaded, it is necessary to apply the changes to the device (press the ***Apply*** button) so that the new certificate and/or private key files take effect.

F.7.2 Devices with Enhanced Cybersecurity

In devices with enhanced cybersecurity, the PKI consists not only of a certificate and a public key, but also of a series of additional files (list of CAs, list of CRLs, authorization policy file) that allow the device both to perform secure communications with mutual authentication capability and to check the correct securization of the firmware.

A device with enhanced cybersecurity capability can be manufactured without such enhanced cybersecurity in terms of PKI at the request of a customer who does not wish to include the features described below. In this case, in terms of credential management, it will behave as described in the previous **Devices with Basic Cybersecurity** section.

The files that make up the PKI are the following:

- Master password:
  Used to encrypt certain sensitive information (private key/certificate) when it is sent to the device for updating. The sensitive information is encrypted inside the device using an own password of the device with AES 256 CBC algorithm.
  When you want to update this password in the device, the file sent with the new master password must be encrypted AES 256 CBC with the current master password.

- Certificate / Private key:
  This is the private key and certificate similar to those explained in the previous section (**Devices with Basic Cybersecurity**). In this case they are not self-generated and the certificate is not self-signed, different ones are installed for each device during the manufacturing process and the certificate is signed by the ZIV CA and is valid for 20 years. The key is 4096-bit RSA.
  When you want to update the device, either only the certificate or both, certificate and private key, you must use a PKCS#12 file whose key is the current master password of the device.

- List of Certification Authorities (CAs):
  This is a file containing all the root certificates that will be used to verify both the remote certificates in the case of TLS mutual authentication (verifying that they are signed by one of the CAs on the list), and the signatures of the firmware as explained in the **Digital Firmware Securization** section. The file format is PEM and contains a concatenation of all the possible CAs managed by the device, both for communications and for firmware signature verification.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- Certificate Revocation List (CRLs):
  This is a file containing all the certificate revocation lists (CRLs) associated with all the CAs of the device, which are going to be used to verify the revocation of remote certificates in the case of TLS mutual authentication, as well as of the firmware signatures. The file format is PEM and contains a concatenation of all possible CRLs managed by the device.

- Authorization policy file:
  This is a file that includes a set of policies that allow checking additional parameters of the remote certificates in the case of TLS mutual authentication, as well as the signatures of the firmware.
  Of course, the validity of the certificates must first be checked: signing by CAs, revocation and expiration. Then these additional rules (policies) are checked. Each policy affects one service (firmware signature verification, PROCOME communications, HTTPS communications) and you can select whether any or all certificates must comply with these rules. The rules are specified per certificate and can include the certificate fingerprint (of the subject and/or issuer), the CN attribute (of the subject and/or issuer) and/or the OU attribute (of the subject and/or issuer).
  The file format is XML and is as follows:

Node	Description	Child nodes	Attributes
AuthPolicy	Root node.	**Policy** (only one)	-
Policy	Authorization policy.	**Certificate** (several)	**effect**: indicates the service to which the policy applies. Possible values are: - **allow-signature-verify**: firmware signature verification service. After verification that the firmware is signed by the certificate(s) and that the certificate(s) is (are) signed by a CA from the list of CAs of the device and is (are) neither expired nor revoked, the certificate(s) must comply with the rules of this policy for the firmware signing process to be valid for the device. - **allow-procome-connection**: PROCOME TLS communications service. After verifying that the remote certificate is signed by a CA from the list of CAs of the device and that it is neither expired nor revoked, the remote certificate must comply with the rules of this policy for the PROCOME TLS connection to be accepted by the device. - **allow-https-connection**: HTTPS communications service. Identical operation to **allow-procome-connection**, but for HTTPS communication.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Node	Description	Child nodes	Attributes
Policy	Authorization policy.	**Certificate** (several)	**condition**: indicates whether the policy affects all certificates or only some of them. The possible values are: - **allow-if-any-certificate-matches**: the policy will be successful if any of the certificates used complies with the certificate rules included in the policy. - **allow-if-all-certificates-match**: the policy will be successful if all certificates used comply with the certificate rules included in the policy. - **allow-always**: only for TLS communication, it is used when you do not want to use mutual authentication despite having configured the list of CAs and CRLs in the device. This option allows you to disable mutual authentication by service (PROCOME or HTTPS). This value is ignored for firmware signature verification.
Certificate	Rules to check for a certificate.	**Thumbprint**, **CN**, **OU** (up to 2 of each)	-
Thumbprint	Fingerprint of the certificate. The fingerprint (SHA256) of the certificate to be checked (**from**="subject") or of the certificate signing the certificate to be checked (**from**="issuer") must match this attribute for the rule to be successful.	-	**from**: indicates whether the rule (Thumbprint) is to be checked for the subject or issuer of the certificate.
CN	CN attribute of the certificate. The CN attribute of the subject (**from**="subject") or issuer (**from**="issuer") of the certificate to be checked must contain this attribute (case sensitive) for the rule to be successful.	-	**from**: indicates whether the rule (CN) is to be checked for the subject or the issuer of the certificate.
OU	OU attribute of the certificate. The OU attribute of the subject (**from**="subject") or issuer (**from**="issuer") of the certificate to be checked must contain this attribute (case sensitive) for the rule to be successful.	-	**from**: indicates whether the rule (OU) is to be checked for the subject or the issuer of the certificate.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

An example of the file is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
 <AuthPolicy>
  <Policy effect="allow-signature-verify" condition="allow-if-all-
  certificates-match">
   <Certificate>
   <Thumbprint
   from="issuer">3500c3951b03ef20e4954575705fe50b9b0b69ee32e46b72ab0f5a1b170
   42010</Thumbprint>
   <CN from="subject">ziv-firmware-signing</CN>
   <OU from="subject">ZIV</OU>
   </Certificate>
  </Policy>
  <Policy effect="allow-https-connection" condition="allow-if-any-
  certificate-matches">
   <Certificate>
   <CN from="issuer">ziv-ca</CN>
   </Certificate>
  </Policy>
  <Policy effect="allow-procome-connection" condition="allow-always">
  </Policy>
 </AuthPolicy>
```

Credentials management must be performed by a user with *user management* permission and is done using the ***ZIV e-NET Tool***® configuration tool.

To manage the credentials of the device from the ***ZIV e-NET Tool***® it is necessary that some of the LAN ports and the SSH and SFTP services are enabled.

This is accessed from the ***Tools→Device access*** menu.

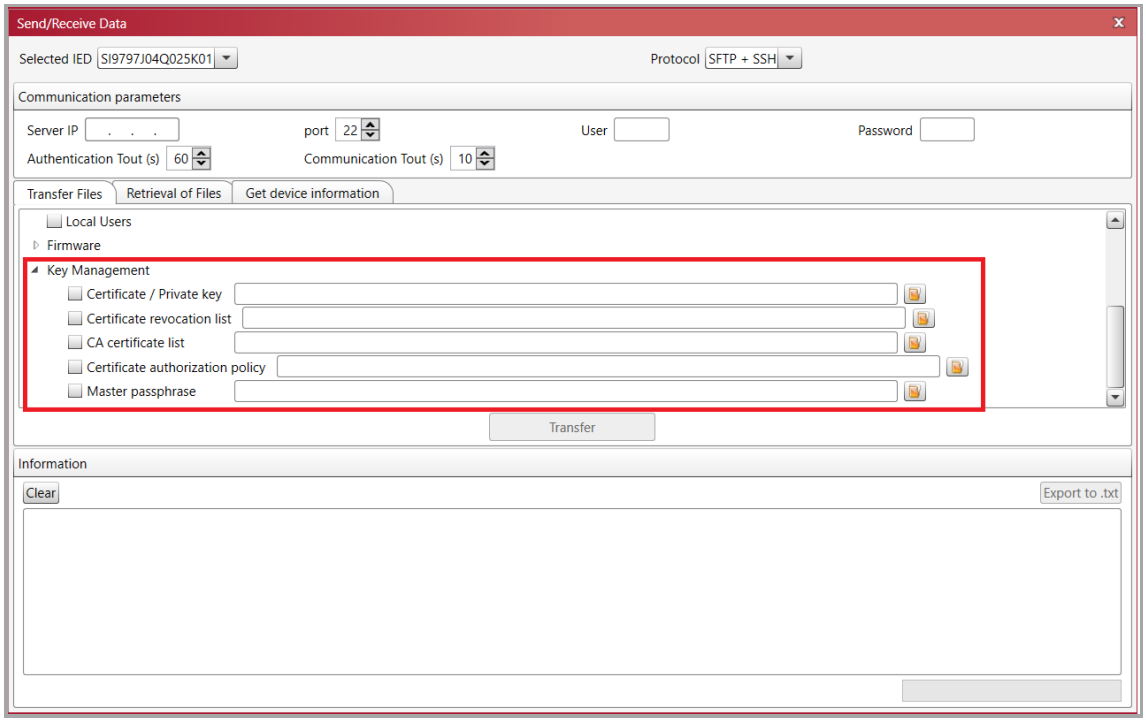


Figure F.35 Sending of PKI Files with Configuration Tool.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (username and password). In the ***Transfer Files*** tab, under the ***Key Management*** option, there are several options for sending the different PKI files available on the device:

- ***Certificate / Private key***: Option to upload a certificate or a certificate + private key to the device. A file in PKCS#12 format must be used whose key is the current master password of the device. If it contains only the certificate, it must be paired with the current private key of the device.
- ***Certificate revocation list***: Option to upload a certificate revocation list (CRLs). A file in PEM format must be used and must contain a concatenation of all possible CRLs managed by the device. It cannot be empty; it must contain at least one CRL.
- ***CA certificate list***: Option to upload a list of CA certificates to the device. A file in PEM format must be used and it must contain a concatenation of all the possible CAs managed by the device, both for communications and for firmware signature verification. It cannot be empty; it must contain at least one CA and the CAs cannot be revoked or expired.
- ***Certificate authorization policy***: Option to upload an authorization policy file to the device. The XML format file explained above must be used.
- ***Master passphrase***: Option to upload a new master password to the device. A file must be used in which the new master password is encrypted AES 256 CBC with the current master password of the device.

To select the PKI file to be sent, press the button  on the right. After selecting the desired option (only one option must be selected at a time), the ***Transfer*** button is used to upload the PKI file to the device. The upload progress is displayed in the ***Information*** window. If the PKI file is successfully uploaded to the device, the **Security credentials changed successfully** cybersecurity event is generated. However, if any error occurs in the validation of the PKI file by the device, the **Security credentials change failed** cybersecurity event is generated.

When a list of CAs is sent to the device, it checks that, for each CA present in the list, its associated CRL is present in the device. If not, the device rejects the list of CAs.

When a list of CRLs is sent to the device, the device checks that, for each CA present in the device, its associated CRL is present in the list. If not, the device rejects the list of CRLs.

That is, in the device, for each CA, there must be its associated CRL (only one CRL for each CA) and other additional CRLs may also be present.

Therefore, when you want to add one or more CA+CRLs to the device, you must first send the list of CRLs and then the list of CAs; and when you want to remove one or more CA+CRLs from the device, you must first send the list of CAs and then the list of CRLs.

To retrieve the PKI files from the device, access the menu ***Tools→Device access***. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (user and password). In the ***Retrieval of Files*** tab, under the ***Key Management*** option, there are several options to collect the different PKI files available from the device:

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- ***Certificate***: Option to download the certificate of the device in PEM format.
- ***Certificate revocation list***: Option to download the Certificate Revocation List (CRLs) of the device in PEM format.
- ***CA certificate list***: Option to download the CA certificate list of the device in PEM format.
- ***Certificate authorization policy***: Option to download the authorization policy file of the device in XML format.

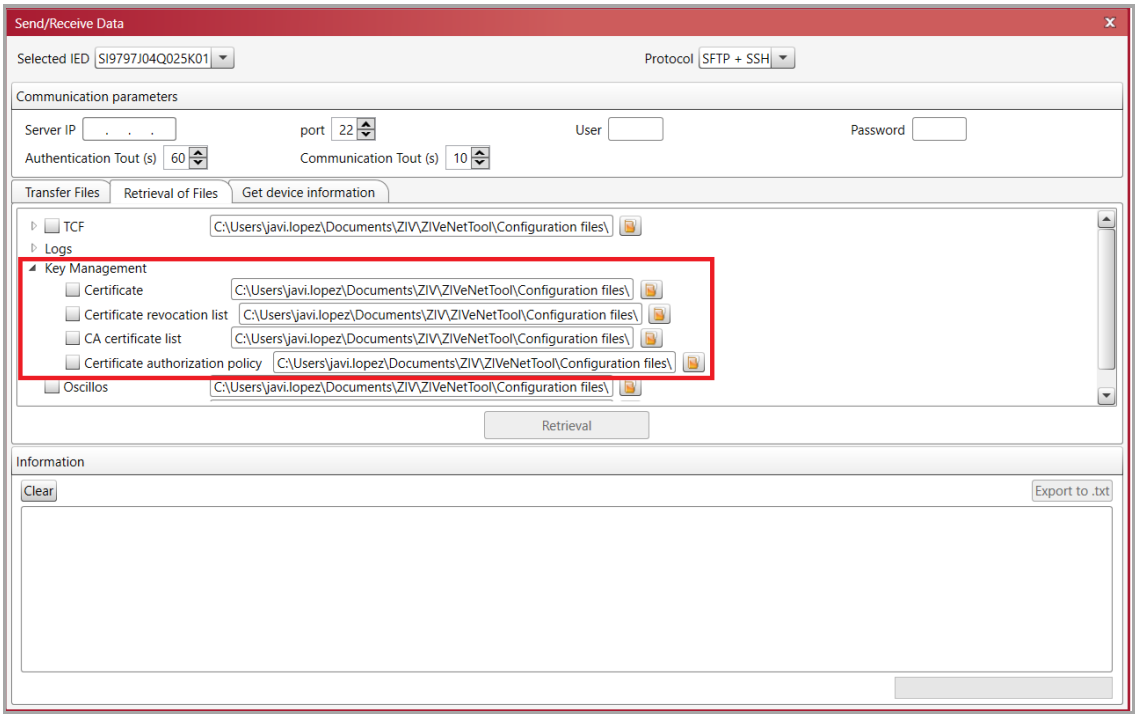


Figure F.36 Retrieval of PKI files with configuration tool.

To select the destination directory for each PKI file, click the button on the right. After selecting the desired options, click on the ***Retrieval*** button to download the PKI files from the selected device. The download progress is displayed in the ***Information*** window.

F.8 Digital Firmware Securization

In the world of cybersecurity and due to its continuous evolution, it is very common that certain security measures become insecure over time, security gaps are discovered in software components and it is necessary to update the firmware of the devices to eliminate such security gaps.

Firmware upload is one of the most critical processes for devices. It is vital to ensure that the firmware uploaded to the device is valid and has not been altered or modified by third parties.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.8.1 Devices with Basic Cybersecurity

For devices with basic cybersecurity, firmware securization consists of including a hash of the firmware and performing encryption using fixed criteria known by manufacturer and devices, which provides confidentiality and integrity.

When new firmware is uploaded to the device (via website), the device decrypts the firmware, checks the hash, performs additional internal checks to ensure that the firmware structure is valid, and only then restarts to take the new firmware, generating the **Firmware uploaded successfully** cybersecurity event. If something fails in the validation process of the new firmware, the device remains with the firmware it had uploaded before the failed update, generating the **Firmware upload failed - Invalid firmware** cybersecurity event.

F.8.2 Devices with Enhanced Cybersecurity

In devices with enhanced cybersecurity, firmware securization is more sophisticated. The firmware of the devices is digitally encrypted, which provides confidentiality. In addition, the encrypted firmware is signed based on X.509 certificates using CMS/PKCS#7 DER format, allowing multiple signatures (in addition to the original signature by ZIV), which provides integrity.

Signatures may be associated with a set of metadata (manifest), encoded as signed attributes of the CMS/PKCS#7 signature (*signedAttributes*). In general, this manifest will have a common structure that includes generic information about the manifest and a particular structure for each type of manifest. Specifically, for the ZIV signature, the following signed attributes have been defined to include firmware related information. For each one, the internal name, its ***OID*** (identifier) and its meaning are indicated:

- *manifestInformation* (***1.3.6.1.4.1.15732.8191.1***): general information about the manifest. It includes the following sequential information (SEQUENCE):
  - *class*: is an enumerated (ENUMERATED) indicating the type of manifest. At the moment it only takes the value 0 (firmware). In the future it may take other values for possible client signatures.
  - *version*: is an integer (INTEGER) indicating the version of the manifest. At the moment it only takes the value 1.
  - *owner*: a text string (VISIBLE STRING) from 0 to 256 characters indicating the owner of the manifest. The value is ZIV.
  - *copyright*: in a text string (VISIBLE STRING) from 0 to 256 characters indicating the manifest copyright. The value is ZIV.

- *basicFirmwareInformation* (***1.3.6.1.4.1.15732.8191.2.1***): basic firmware information. It includes the following sequential information (SEQUENCE):
  - *version*: in a text string (VISIBLE STRING) from 1 to 64 characters indicating the full firmware version, e.g., 0.10.0-0C03-02.
  - *description*: is a text string (VISIBLE STRING) from 0 to 512 characters indicating the following information:
    - A first text string **Firmware** indicating that it corresponds to the complete firmware of the device (at the moment the device firmware is atomic, it is uploaded in full). In the future it may contain other words to indicate that it is a security patch or a specific part of the firmware.
    - The character | to separate both text strings.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

  - A second text string indicating the complete firmware model, including hardware and software parts, e.g., **IRFA-mA14mA00000000x0xX-2032070**.

  Example: **Firmware|IRFA-mA14mA00000000x0xX-2032070**.
- *supportedModels*: this is a sequence (SEQUENCE) of text strings (VISIBLE STRING) from 1 to 256 characters indicating the list of hardware models for which the signed firmware is valid. Examples: **IRFA-1A140A00000000XXXX**, **IRFA-1A142A00000000XXXX**, **IRFA-1A143A00000000XXXX**, **IRFA-1A146A00000000XXXX**, **IRFA-1A147A00000000XXXX**, **IRFA-2A140A00000000XXXX**, **IRFA-2A142A00000000XXXX**, **IRFA-2A143A00000000XXXX**, **IRFA-2A146A00000000XXXX**, **IRFA-2A147A00000000XXXX**.

These signed attributes can be viewed by applying a CMS/PKCS#7 viewer or analyzer to the signed firmware.

When new firmware is uploaded to the device (either via website or using the ***ZIV e-NET Tool***®), it performs the following checks on the received firmware file:

- Verify that the firmware is correctly signed by certificates that comply with the PKI of the device explained in the **Credential Management** section. The certificates of the sigantures, therefore, must be signed by CAs contained in the list of CAs of the device, must not be revoked (checked using the list of CRLs of the device) or expired and must comply with the firmware signature verification authorization policy. If any of these checks are not met, an invalid firmware message is displayed due to a signing error and the firmware upload process is aborted.
- Verify that the signed attribute information (if available, only mandatory for ZIV signing) *manifestInformation* and the particular attribute (*basicFirmwareInformation* in the case of ZIV signing) is correctly structured and valid. If it is not, an invalid firmware message is displayed due to an error in the associated information and the firmware upload process is aborted.
- Extracts the firmware version from the signed *basicFirmwareInformation* attribute. From the website you can simply upload firmware and upgrade and downgrade is always allowed. But from the ***ZIV e-NET Tool***® it is possible to upgrade and downgrade separately. In this case, the device compares the current firmware version with that of the new firmware you are trying to upload.
  - If the new version is later than the current version and the operation is a downgrade, an invalid firmware message is displayed because it is not possible to downgrade to a later version and the firmware upload process is aborted.
  - If the new version is lower than the current version and the operation is an upgrade, an invalid firmware message is displayed because it is not possible to upgrade to a previous version and the firmware upload process is aborted.
  - If the new version is the same as the previous one, both upgrade and downgrade operations are allowed.
- Checks that the new firmware is valid for the hardware model of the device, comparing that the current hardware model of the device is included in the hardware models for which the firmware is valid present in the signed *basicFirmwareInformation* attribute. If it is not valid, an invalid firmware message is displayed because the model is not supported and the firmware upload process is aborted.
- It proceeds to decrypt the firmware with a key uploaded during the device manufacturing process. If it fails to decrypt it, an invalid firmware message is displayed because of a decryption error and the firmware upload process is aborted.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Finally, the device performs additional internal checks to ensure that the firmware structure is valid and, only then, reboots to take the new firmware, generating the **Firmware uploaded successfully** cybersecurity event. If something fails in the validation process of the new firmware (cases detailed above), the device remains with the firmware it had uploaded before the failed update, generating the **Firmware upload failed - Invalid firmware** cybersecurity event.

A device with enhanced cybersecurity capability may be manufactured without such enhanced PKI cybersecurity at the request of a customer who does not wish to include this enhanced firmware securization feature. In that case, in terms of firmware securization, it will behave as a device with basic cybersecurity and both upgrade and downgrade options of ***ZIV e-NET Tool***® will work the same, without version checking.

F.8.3 Firmware Upload Methods

In order to upload firmware, the user must have *firmware change* permission.

There are two methods to upload firmware to the device:

- Website. To upload firmware from the web interface, one of the LAN ports and the HTTP or HTTPS services must be enabled. It is recommended to use HTTPS connection instead of HTTP because the data is encrypted. Access the ***Reflash*** menu, authenticating first if necessary.

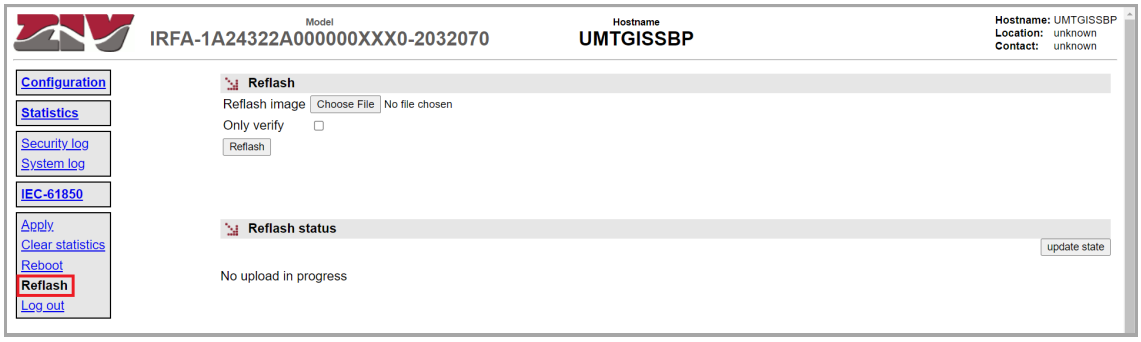


Figure F.37 Uploading Firmware via Website.

The firmware file to be uploaded to the device is selected by clicking on the ***Choose File*** button.

The ***Only verify*** option is used to validate if the firmware is valid, but without updating the device with the new firmware.

Pressing the ***Reflash*** button starts the firmware upload process to the device (or validation if ***Only verify*** is checked). The firmware upload/validation progress is displayed in the ***Reflash status*** window. This progress is refreshed periodically or can be refreshed on demand by pressing the ***update state*** button.

As indicated above, from the website it is always possible to upgrade and downgrade the firmware version, no version checking is performed.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- Configuration tool. To upload firmware from the ***ZIV e-NET Tool***® it is necessary that some of the LAN ports and the SSH and SFTP services are enabled. This is accessed from the ***Tools→Device access*** menu.

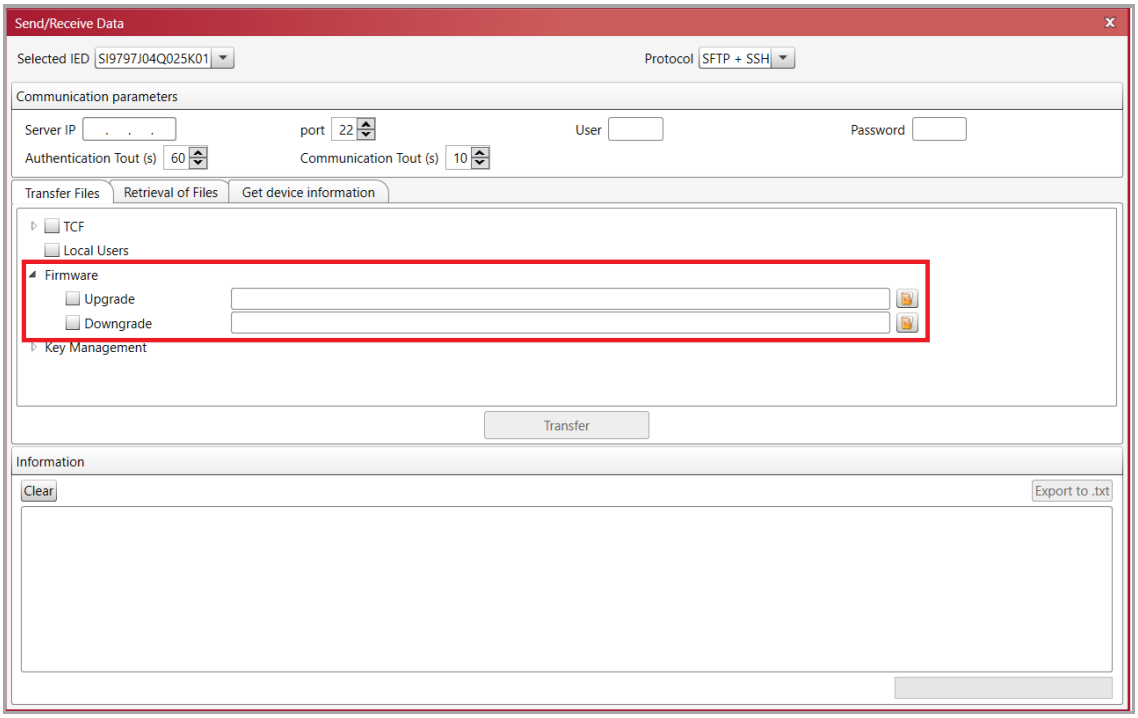


Figure F.38 Firmware Upload with Configuration Tool.

In this window it is verified that **SFTP + SSH** is selected in ***Protocol***, the device IP address and port data are configured (it must coincide with the SSH/SFTP port of the device) and the user credentials (user and password) are entered. In the ***Transfer Files*** tab, under the ***Firmware*** option, there are two options:

- ***Upgrade***. Option for uploading a firmware version equal to or higher than the current one.
- ***Downgrade***. Option to upload a firmware version equal to or lower than the current version.

In both options, the firmware file to be sent to the device must first be selected by pressing the button on the right. After selecting the desired option, the firmware is uploaded to the device by clicking on the ***Transfer*** button. The firmware upload progress is indicated in the ***Information*** window.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.9 Registration of Activities

One of the classic cybersecurity requirements is *non-repudiation*, which is to avoid the possibility of denying that the device performed an action or claiming that the device performed an action when it really did not. The main countermeasure to ensure *non-repudiation* is the recording of cybersecurity activities or events.

The device has a cybersecurity event log. These events, in addition to being displayed online on the website of the device and stored in a file for later collection, can be sent to a centralized cybersecurity system using the **Syslog** protocol, complying with RFC5424. This will allow the centralized system to analyze cybersecurity events instantly and detect and mitigate possible attacks, including coordinated attacks on several devices simultaneously.

F.9.1 Syslog Format

For the Syslog format of cybersecurity events and their transmission to possible Syslog servers, see Annex G, **Syslog Protocol**.

F.9.2 Events

The cybersecurity events that can be generated in the device are listed in the following table. For each event, its universal identifier (see ***EventID*** field in Annex G, **Syslog Protocol**), its severity (event or alarm), its associated text (see ***EventText*** field in Annex G, **Syslog Protocol**) and a brief description are indicated.

Id	Severity	Text	Description
***Access Control* Events**			
0000001	Event	Login successful	Successful login (authentication).
0000038	Event	Logout	Logout (manual or automatic).
0000039	Event	Login failed	Authentication failure.
0000069	Alarm	Login failed – too many user sessions	Authentication failed due to no sessions available.
0000070	Alarm	Login failed – user rejected due to role concurrency	Authentication failed because it cannot authenticate due to role concurrency.
0000071	Alarm	Logout – session closed by other user	Logout due to being expelled by a user.
0000072	Event	CLI access initiated	CLI access initiated (may be by SSH or Telnet).
0000073	Event	FTP access initiated	FTP access initiated (via SSH).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Id	Severity	Text	Description
***User and Credential Management* Events**			
0000030	Event	User account created successfully	User created.
0000031	Event	User account modified successfully	User modified.
0000032	Event	User account deleted successfully	User deleted.
0000043	Event	Role created successfully	Role created
0000044	Event	Role modified successfully	Role modified
0000045	Event	Role deleted successfully	Role deleted
0000065	Alarm	Security credentials changed successfully	Successful change of operation PKI credentials.
0000066	Alarm	Security credentials change failed	Failed change of operation PKI credentials.
0000067	Event	LDAP repository not accessible	The LDAP remote authentication server is not available.
0000068	Event	RADIUS server not accessible	The RADIUS remote authentication server is not available.
0000111	Alarm	Default security credentials changed successfully	Successful change of default PKI credentials.
0000112	Alarm	Default security credentials change failed	Failed change of default PKI credentials.
0000113	Alarm	Security credentials restored to default due to integrity problems	An integrity error has been detected in the PKI information and certain values have been restored to their default values.
***Settings and Configuration Change* Events**			
0000012	Event	Parameters changed successfully	Change of settings. The number of settings that have been changed is indicated in parentheses.
0000015	Event	Configuration downloaded	Successful configuration download.
0000016	Event	Configuration uploaded successfully	Successful configuration upload.
0000018	Alarm	Configuration upload failed – invalid configuration	Wrong configuration upload (invalid file).
***Firmware Change* Events**			
0000020	Event	Firmware uploaded successfully	Successful firmware upload.
0000022	Alarm	Firmware upload failed – invalid firmware	Wrong firmware upload (invalid firmware).
***Device Restart* events**			
0000023	Alarm	Device reset to factory default	Device reset to factory settings.
0000024	Alarm	Manual reset	Device manually restarted.
0000025	Alarm	IED startup	Device started.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Id	Severity	Text	Description
		***Hardware Change* Events**	
0000026	Alarm	Hardware change detected	Hardware change detected (valid model, HW compatible).
0000027	Alarm	Hardware change detected – invalid hardware	Hardware change detected (invalid model, HW incompatible).
		***Hardware/Software Error* Events**	
0000075	Alarm	Critical error - Read/write settings error	Existence of incorrect settings or loss of the value of a setting. Corresponds to alarm 0x00000001 of the device.
0000076	Alarm	Non-critical error - Local port HW error	Error when operating on the front USB communications port. Corresponds to alarm 0x00000002 of the device.
0000077	Alarm	Critical error - Protection error	Protection error, protection not operative. Corresponds to alarm 0x00000004 of the device.
0000078	Alarm	Critical error - ADC error	Error in the ADC or in the auxiliary microcontroller that receives and controls the samples. Corresponds to alarm 0x00000008 of the device.
0000079	Alarm	Critical error - Digital I/O error	Problems in the digital I/O module. Corresponds to alarm 0x00000010 of the device.
0000080	Alarm	Critical error - Flash error	Flash memory problems. Corresponds to alarm 0x00000020 of the device.
0000081	Alarm	Critical error - Internal power failure	Internal power failure. Corresponds to alarm 0x00000040 of the device.
0000082	Alarm	Non-critical error - IEC 61850 error	Problems with data files, CID attached to the SW, unknown device model, inability to choose a data model or error interpreting a previously validated CID. Corresponds to alarm 0x00000080 of the device.
0000083	Alarm	Non-critical error - Error in configuration	The error occurs if the system cannot be configured with the requested configuration. Corresponds to alarm 0x00000100 of the device.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Hardware/Software Error Events			
0000084	Alarm	Critical error - Program error	Unexpected problems in the SW that prevent its operation. Corresponds to alarm 0x00000200 of the device.
0000085	Alarm	Non-critical error - Remote port 1 error	Remote port 1 hardware error. Corresponds to alarm 0x00000400 of the device.
0000086	Alarm	Critical error - Hardware error	Incorrect hardware configuration. The HW detected by the device does not correspond to the internal models provided by the SW. Corresponds to alarm 0x00000800 of the device.
0000087	Alarm	Critical error - Microcontroller error	Error in the communication with the auxiliary microcontroller that controls the different boards. Corresponds to alarm 0x00001000 of the device.
0000088	Alarm	Non-critical error - RTC error	Problems with RTC. Corresponds to alarm 0x00002000 of the device.
0000089	Alarm	Critical error - Transducer input error	Error in the communication with the input transducer. Corresponds to alarm 0x00004000 of the device.
0000090	Alarm	Non-critical error - Remote port 2 error	Remote port 2 hardware error. Corresponds to alarm 0x00008000 of the device.
0000091	Alarm	Critical error - External flash error	Problem in flash memory external to the CPU board. Corresponds to alarm 0x00010000 of the device.
0000092	Alarm	Critical error – 87L microcontroller error	Internal communications error between microcontrollers of the 87L communications board. Corresponds to alarm 0x00020000 of the device.
0000093	Alarm	Non-critical error – 87L communication error	Error in the communication with the 87L communications board. Corresponds to alarm 0x00040000 of the device.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Id	Severity	Text	Description
		***Communication Certificate Validation* Events**	
0000114	Alarm	Certificate validation failed – certificate expired	The certificate received by communications is expired (or not yet valid).
0000115	Alarm	Certificate validation failed – certificate revoked	The certificate received by communications is revoked.
0000116	Alarm	Certificate validation failed – certificate signature check failed	The certificate received by communications is not trusted (it has not been successfully validated against the list of CAs of the device).
0000117	Alarm	Certificate validation failed – certificate does not comply with authorization policies	The certificate received by communications does not comply with the authorization policies (it has not been successfully validated against the authorization policy file of the device).
		***Ports Enabling / Disabling* Events**	
0000049	Event	Local port disabled	Local port disabled.
0000050	Event	Local port enabled	Local port enabled.
0000051	Event	Remote port 1 disabled	Remote port 1 disabled.
0000052	Event	Remote port 1 enabled	Remote port 1 enabled.
0000053	Event	Remote port 2 disabled	Remote port 2 disabled.
0000054	Event	Remote port 2 enabled	Remote port 2 enabled.
0000055	Event	LAN port 1 disabled	LAN port 1 disabled
0000056	Event	LAN port 1 enabled	LAN port 1 enabled
0000057	Event	LAN port 2 disabled	LAN port 2 disabled
0000058	Event	LAN port 2 enabled	LAN port 2 enabled
0000059	Event	LAN port 3 disabled	LAN port 3 disabled
0000060	Event	LAN port 3 enabled	LAN port 3 enabled
0000061	Event	LAN port 4 disabled	LAN port 4 disabled
0000062	Event	LAN port 4 enabled	LAN port 4 enabled
0000063	Event	USB port disabled	USB port disabled
0000064	Event	USB port enabled	USB port enabled

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Other events			
0000028	Event	Date and time set successfully	Change in device date/time > 100ms.
0000029	Event	Security events log downloaded	Cybersecurity events log downloaded.
0000041	Event	USB connected	It occurs when a USB pendrive is connected to the USB-A port.
0000042	Event	USB disconnected	It occurs when a USB pendrive is disconnected from the USB-A port.
0000074	Alarm	Unauthorized physical access detected	Detection of unauthorized physical access, for the moment, removal/insertion of hardware boards (except CPU and power supply) with the device powered up.
0000106	Event	CLI command performed “XXXX”	Indicates that the XXXX command has been successfully executed by CLI. XXXX corresponds to the complete command executed on the CLI.

F.9.3 Storage File

The device has the capacity to hold at least 2048 cybersecurity events in a circular buffer (FIFO).

The events are stored in a FLASH file, so that they are not lost in the event of a shutdown.

The size of the file is 256 kB, and the number of events it can hold will depend on the text occupied by each event with its additional information, but always greater than 2048 events.

The file is called */audit/security.log* and cannot be modified or deleted in any way.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

F.9.4 Viewing and Downloading the File

Only a user with *audit log* permission can view the cybersecurity events and/or download the file.

There are several ways to access the cybersecurity event file (*security.log*):

- By FTP or SFTP file transfer. In this case the file location is */audit/security.log*.
- From the website, ***Security log*** menu. The events are displayed directly on the web page in order of occurrence. In addition, the file can be downloaded by clicking the ***Download File*** button.

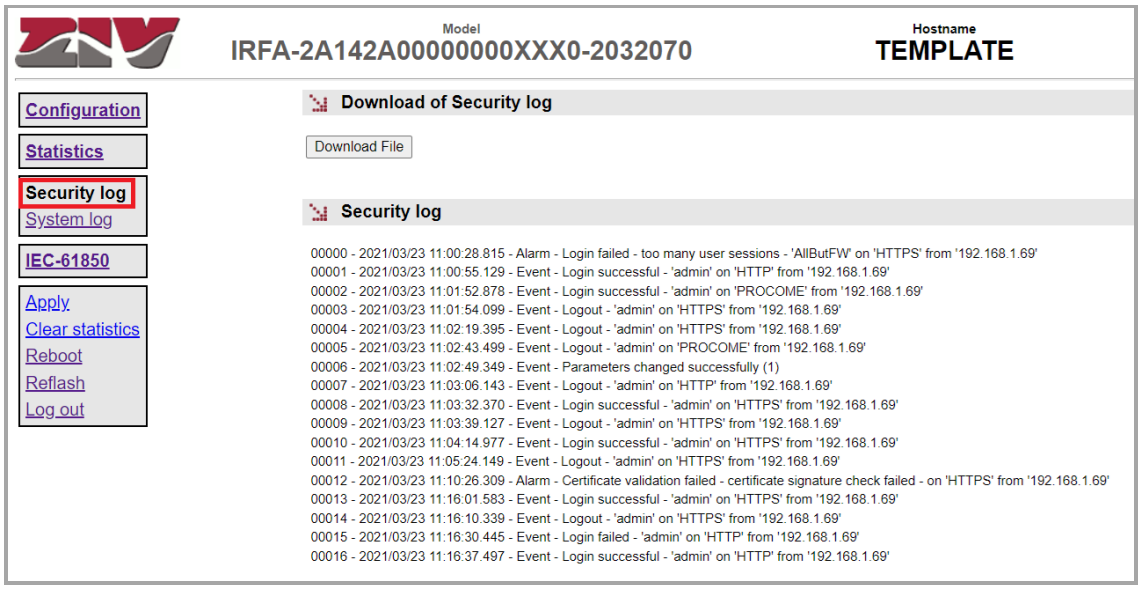


Figure F.39 Display of Cybersecurity Events on Website.

- Using the ***ZIV e-NET Tool***® configuration tool. To collect cybersecurity events using the ***ZIV e-NET Tool***®, access the ***Tools→Device access*** menu. In this window, check that **SFTP + SSH** is selected in ***Protocol***, configure the device IP address and port data (it must match the SSH/SFTP port of the device) and enter the user credentials (username and password). In the ***Retrieval of Files*** tab, check the ***Logs→Security Events*** option and click ***Retrieval*** to download the cybersecurity events file. The download progress is displayed in the ***Information*** window.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

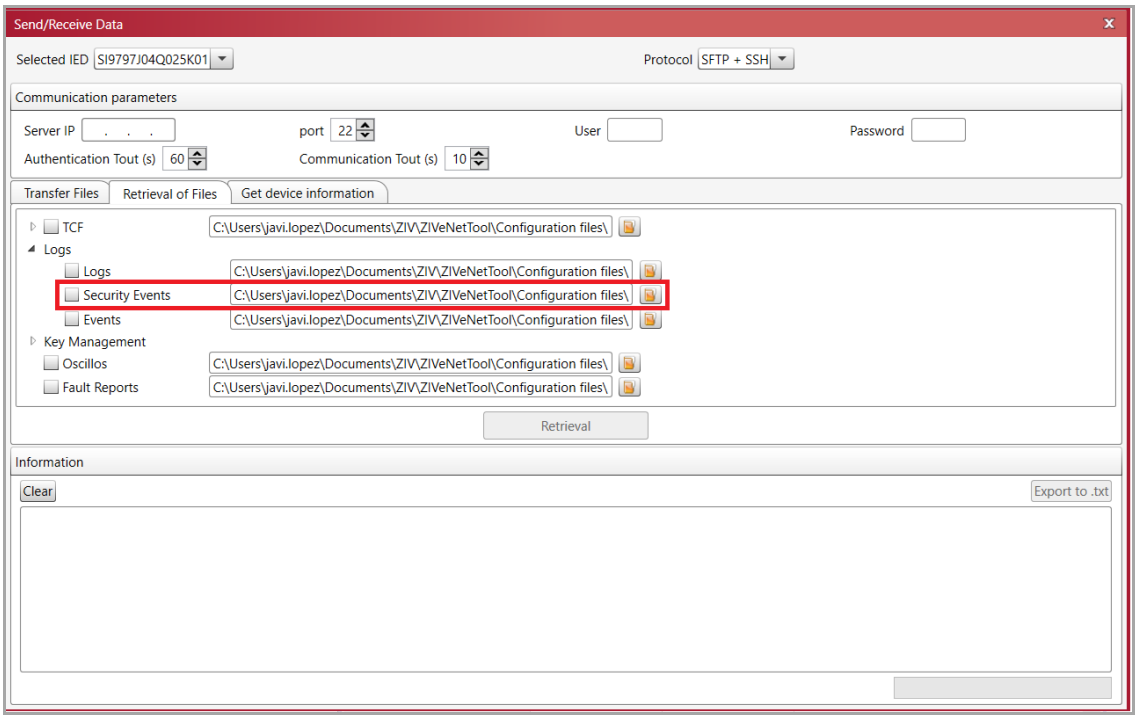


Figure F.40 Collection of Cybersecurity Events with Configuration Tool.

Each time the cybersecurity event file is downloaded from the device, the **Security events log downloaded** cybersecurity event is generated.

Cybersecurity events are displayed on the website and stored in the file *security.log* with the following format:

YYYY/MM/DD hh:mm:ss.mmm - eveala - evtext - 'user' on 'service' from 'ipaddr' (interface)

where:

- ***YYYY/MM/DD hh:mm:ss.mmm***: it is the date and time of the event (up to milliseconds). Corresponds to the TIMESTAMP field of the Syslog HEADER.
- ***eveala***: reflection of Syslog HEADER field PRI. It will be able to take the values:
  - Event (PRI=<108>)
  - Alarm (PRI=<105>)
- ***evtext***: text of the event. It is the faithful reflection of the *EventText* field of Syslog's STRUCTURED_DATA. If after ***evtext*** there is no more information to show or it is only shown (*interface*), then the hyphen (-) following ***evtext*** will not be shown. Otherwise, it will be shown.
- ***user***: username. It is the faithful reflection of the *User* field of the Syslog STRUCTURED_DATA. If the *User* field is not present or has a NILVALUE ("-") value, then the text "*user*" will not be presented in the event.
- ***service***: name of the service. It is the faithful reflection of the PROCID field of the Syslog HEADER. If the PROCID field is set to NILVALUE ("-"), then the text "*on service*" will not be presented at the event.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

- ***ipaddr***: IP address of the device causing the event. It is the faithful reflection of the *PeerIpAddress* field of the Syslog STRUCTURED_DATA. If the *PeerIpAddress* field is not present or is set to NILVALUE ("-"), then the text "*from ipaddr*" will not be presented in the event.
- ***interface***: physical interface through which the event occurred. It is the faithful reflection of the *Interface* field of the Syslog STRUCTURED_DATA. If the *Interface* field is not present or is set to NILVALUE ("-"), then the text "(*interface*)" will not be presented in the event.

The following are examples of event format in file:

- Successful authentication of user "admin" by SSH from IP=192.168.1.69 with device SI3197E1Q11F01:
  `2016-04-17 22:36:41.358 - Event - Login successful - 'admin' on 'SSH' from '192.168.1.69'`

- Starting up of device TEMPLATE:
  `2016-04-171:24:32.498 - Alarm - IED startup`

- Logout of user "Ramon.Perez" by HMI in the device SWT650:
  `2016-04-17 23:35:49.423 - Event - Logout - 'Ramon.Perez' (HMI)`

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G. Syslog Protocol

G.1 General G-2
G.2 Syslog Format for Cybersecurity Events G-3
G.2.1 HEADER Format G-3
G.2.2 STRUCTURED-DATA Format G-4
G.2.3 Examples G-5
G.3 Syslog Format for Cybersecurity Events (version 2) G-6
G.3.1 HEADER Format G-6
G.3.2 STRUCTURED-DATA Format G-7
G.3.3 Examples G-8
G.4 Syslog Format for Protection Events (SOE) G-9
G.4.1 HEADER Format G-9
G.4.2 STRUCTURED-DATA Format G-10
G.4.3 MSG Format G-11
G.4.4 Examples G-11
G.5 Syslog Format for Based on IEC 61850 Events (SOE) G-12
G.5.1 HEADER Format G-12
G.5.2 STRUCTURED-DATA Format G-13
G.5.3 MSG Format G-13
G.5.4 Examples G-14
G.6 Syslog Transmission G-14

G.1 General

Due to its simplicity and wide acceptance and use, the format chosen for sending events is Syslog. Throughout the evolution of Syslog, several RFCs have been published, all with the aim of achieving greater compatibility and security between the different implementations. Of these, RFC 5424 is used, as it is widely accepted and provides all the required features.

The equipment has a cybersecurity event log. These events, in addition to being viewed online on the unit's web page and stored in a file for later collection, can be sent to a centralized cybersecurity system using the **Syslog** protocol, in compliance with RFC5424. This will allow such a centralized system to analyze cybersecurity events instantaneously and detect and mitigate possible attacks, including coordinated attacks on several devices simultaneously.

The equipment also has a Protection event record. By configuring the appropriate settings, as explained in the chapter Event Record, the user can configure protection events to be stored in a second log called **SYSLOGSOE**. All events stored in this log are automatically sent through the Syslog protocol.

The following acronyms and structures will be used throughout this Annex:

UTF-8-STRING	= *OCTET (UTF-8 string as specified in RFC 3629).
OCTET	= Characters from %d00 to %d255.
SP	= Blank space (%d32), used as field separator.
PRINTUSASCII	= Characters from %d33 to %d126.
NONZERO-DIGIT	= Characters from %d49 to %d57.
DIGIT	= Character %d48 + NONZERO-DIGIT.
NILVALUE	= “-“

The structure of a Syslog event is as follows:

HEADER SP **STRUCTURED-DATA** [SP **MSG**]

The **HEADER** field has the following structure:

HEADER = PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID

The **STRUCTURED-DATA** field has the following structure

STRUCTURED-DATA	= 1 * SD-ELEMENT
SD-ELEMENT	= "[" SD-ID *(SP SD-PARAM) "]"
SD-ID	= SD-NAME
SD-PARAM	= PARAM-NAME "=" %d34 PARAM-VALUE %d34
PARAM-NAME	= SD-NAME
PARAM-VALUE	= UTF-8-STRING; the characters “” (double quotation mark: %d34)’, ’\’ (%d92) and ’]’ (close bracket: %d93) must be escaped using the character ’\’ (%d92).
SD-NAME	= 1*32 PRINTUSASCII, except for the characters ’=’ (equals: %d61), ’ ‘ (blank space: %d32), ’]’ (close bracket: %d93) and ‘”’ (double quotation mark: %d34).

The details of the different fields are explained below for cybersecurity and protection events (SOE).

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.2 Syslog Format for Cybersecurity Events

This format is used by models with Basic Cybersecurity (see Model Selection chapter, digit 26 of Firmware Model Selection with value 1). The rest of models will use the format detailed in the next section.

For cybersecurity events, the MSG field is not used and, therefore, will never be present in the generated Syslog events.

Therefore, the structure of a cybersecurity Syslog event is as follows:

HEADER SP **STRUCTURED-DATA**

G.2.1 HEADER Format

RFC 5424 Information Fields		

HEADER	***PRI***	= "<PRIVAL>"
		Priority of the event:
		The ***PRIVAL*** field (1~3 DIGIT) is calculated as follows
		PRIVAL = (8 x ***Facility***) + (***Severity***)
		- ***Facility***: The value log audit is set =13.
		- ***Severity***:
		  - Events have severity level of "Warning" = 4
		  Event → PRIVAL = 8 x 13 + 4 = *108*.
		  - Alarms have severity level of "Alert" = 1
		  Alarm → PRIVAL = 8 x 13 + 1 = *105*.

	VERSION	1
	TIMESTAMP	Date and time of the event. The format is: ***FULL-DATE "T" FULL-TIME*** ***FULL-DATE*** = ***DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY*** ***DATE-FULLYEAR*** = 4 DIGIT ***DATE-MONTH*** = 2 DIGIT (01-12) ***DATE-MDAY*** = 2 DIGIT (01-28, 01-29, 01-30, 01-31, depending on the month). ***FULL-TIME*** = ***PARTIAL-TIME TIME-OFFSET*** ***PARTIAL-TIME*** = ***TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND "." TIME-SECFRAC*** ***TIME-HOUR*** = 2 DIGIT (00-23) ***TIME-MINUTE*** = 2 DIGIT (00-59) ***TIME-SECOND*** = 2 DIGIT (00-59) ***TIME-SECFRAC*** = 3 DIGIT representing milliseconds 000~999 ***TIME-OFFSET***="Z" (represents the date/time in UTC). UTC format is always used. Example: 2016-04-17T22:36:41.358Z

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

RFC 5424 Information Fields		
	HOSTNAME	Own IP (global or in service origin). Since the IED can have several IP addresses, the value of the HOSTNAME takes the value NIL = "-".
	APP-NAME	Name of the device where the event occurred (equipment name). When the equipment has IEC 61850, the name of the equipment obtained from the CID configuration file will be assigned. Otherwise, it can be modified from the website and from CLI.
	PROCID	Identifier of the service through which the event occurred. Text string with the following possible values: "HTTP", "HTTPS", "FTP", "Telnet", "SSH", "MMS" y "PROCOME".
	MSGID	Takes the fixed value "ZIV".

G.2.2 STRUCTURED-DATA Format

RFC 5424 Information Fields		
STRUCTURED-DATA (SD)	***SD-ID***	OID corresponding to the SMII Network management Private Enterprise Code: EventData@1.3.6.1.4.1.15732
	SOE	Event Sequence Counter. It is a sequential number, which is incremented with each cybersecurity event that occurs. It is a 32-bit unsigned integer. Therefore, possible values range from 0 to 4294967295. It is encoded with a text string of up to 10 characters. It is used to order events according to their occurrence, as the date/time could be altered.
	EventId	Universal identifier that identifies the event in a unique way. It is a text string of 7 characters. See column ***Id*** of the table in the ***Registration of Activities→Events*** section of the Cybersecurity Annex.
	EventText	Descriptive text of the event. It is a text string of up to 127 characters. See column ***Text*** of the table in the ***Registration of Activities→Events*** section of the Cybersecurity Annex.
	User	Identifier of the user who caused the event. Text string of up to 256 characters with the username that generated the event.
	Interface	A text string of up to 32 characters that identifies the physical interface through which the event occurred. This field is available for *access control* type events generated on interfaces other than LAN. Possible values are: "HMI", "LocalPort", "RemotePort1" and "RemotePort2". It is also available with the value "USB" in USB host port enable and disable events.
	PeerIpAddress	A text string of up to 39 characters that identifies the IP address (IP4 or IP6) of the machine that accessed the equipment and caused the event.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.2.3 Examples

Several examples of cybersecurity events in Syslog format are included below:

- Successful authentication of user "admin" by SSH from IP=192.168.1.69 with device SI3197E1Q11F01:

```
<108>1 2016-04-17T22:36:41.358Z - SI3197E1Q11F01 SSH
[EventData@1.3.6.1.4.1.15732 SOE=”131” EventId=”0000001”
EventText=”Login successful” User=”admin”
PeerIpAddress=”192.168.1.69”]
```

- Starting the device TEMPLATE:

```
<105>1 2016-04-17T21:24:32.498Z - TEMPLATE –
[EventData@1.3.6.1.4.1.15732 SOE=”128” EventId=”0000025”
EventText=”IED startup”]
```

- Logout of user "Ramon.Perez" by HMI on the device SWT650:

```
<108>1 2016-04-17T23:35:49.423Z - SWT650 –
[EventData@1.3.6.1.4.1.15732 SOE=”132” EventId=”0000038”
EventText=”Logout” User=”Ramon.Perez” Interface=”HMI”]
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.3 Syslog Format for Cybersecurity Events (version 2)

For cybersecurity events, the MSG field is not used and, therefore, will never be present in the generated Syslog events.

Therefore, the structure of a cybersecurity Syslog event is as follows:

HEADER SP **STRUCTURED-DATA**

G.3.1 HEADER Format

RFC 5424 Information Fields		

HEADER	***PRI***	= "<PRIVAL>"
		Priority of the event:
		The ***PRIVAL*** field (1~3 DIGIT) is calculated as follows
		PRIVAL = (8 x ***Facility***) + (***Severity***)
		- ***Facility***: The value log audit is set =13.
		- ***Severity***:
		  - Events have severity level of "Warning" = 4
		  Event → PRIVAL = 8 x 13 + 4 = *108*.
		  - Alarms have severity level of "Alert" = 1
		  Alarm → PRIVAL = 8 x 13 + 1 = *105*.

	VERSION	1
	TIMESTAMP	Date and time of the event. The format is: ***FULL-DATE "T" FULL-TIME*** ***FULL-DATE*** = ***DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY*** ***DATE-FULLYEAR*** = 4 DIGIT ***DATE-MONTH*** = 2 DIGIT (01-12) ***DATE-MDAY*** = 2 DIGIT (01-28, 01-29, 01-30, 01-31, depending on the month). ***FULL-TIME*** = ***PARTIAL-TIME TIME-OFFSET*** ***PARTIAL-TIME*** = ***TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND "." TIME-SECFRAC*** ***TIME-HOUR*** = 2 DIGIT (00-23) ***TIME-MINUTE*** = 2 DIGIT (00-59) ***TIME-SECOND*** = 2 DIGIT (00-59) ***TIME-SECFRAC*** = 3 DIGIT representing milliseconds 000~999 ***TIME-OFFSET***="Z" (represents the date/time in UTC). UTC format is always used. Example: 2016-04-17T22:36:41.358Z

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

RFC 5424 Information Fields		
	HOSTNAME	Own IP (global or in service origin). Since the equipment can have several IP addresses, the value of the HOSTNAME takes the value of the IP address of the first enabled LAN port, following the order LAN 1, LAN 2, LAN 3 and LAN 4.
	APP-NAME	Name of the device where the event occurred (equipment name). When the equipment has IEC 61850, the name of the equipment obtained from the CID configuration file will be assigned. Otherwise, it can be modified from the website and from CLI.
	PROCID	It takes the value NIL = "-", as stated in IEC 62351-14 standard.
	MSGID	It takes the value "IEC62351-14:1", as stated in IEC 62351-14 standard.

G.3.2 STRUCTURED-DATA Format

RFC 5424 Information Fields		
STRUCTURED-DATA (SD)	***SD-ID***	It takes the value "62351-14@41912", as stated in IEC 62351-14 standard.
	SOE	Event Sequence Counter. It is a sequential number, which is incremented with each cybersecurity event that occurs. It is a 32-bit unsigned integer. Therefore, possible values range from 0 to 4294967295. It is encoded with a text string of up to 10 characters. It is used to order events according to their occurrence, as the date/time could be altered.
	ID	Universal identifier that identifies the event in a unique way. It is a text string of 7 characters. See column ***Id*** of the table in the ***Registration of Activities→Events*** section of the Cybersecurity Annex.
	Text	Descriptive text of the event. It is a text string of up to 127 characters. See column ***Text*** of the table in the ***Registration of Activities→Events*** section of the Cybersecurity Annex.
	UsrID	Identifier of the user who caused the event. Text string of up to 256 characters with the username that generated the event.
	PeerInfo	A text string of up to 39 characters that identifies the IP address (IP4 or IP6) of the machine that accessed the equipment and caused the event.
	Param(0)	Identifier of the service through which the event occurred. HMI and USB are considered as possible services. Text string with the following possible values: "LDAP", "HTTP", "HTTPS", "FTP", "Telnet", "SSH", "MMS", "PROCOME", "HMI" and "USB".
	Param(1)	A text string of up to 32 characters that identifies the physical interface through which the event occurred. This field is available for access control type events generated on interfaces other than LAN. Possible values are: "LocalPort", "RemotePort1" and "RemotePort2".

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.3.3 Examples

Several examples of cybersecurity events in Syslog format are included below:

- Successful authentication of user "admin" by SSH from IP=192.168.1.69 with device SI3197E1Q11F01 with IP=192.168.1.81:

```
<108>1 2016-04-17T22:36:41.358Z 192.168.1.81 SI3197E1Q11F01 - IEC62351-
14:1 [62351-14@41912 ID=”0000001” Text=”Login successful” SOE=”131”
UsrID=”admin” PeerInfo=”192.168.1.69” Param(0)=”SSH”]
```

- Starting the device TEMPLATE with IP=192.168.2.81:

```
<105>1 2016-04-17T21:24:32.498Z 192.168.2.81 TEMPLATE – IEC62351-14:1
[62351-14@41912 ID=”0000025” Text=”IED startup” SOE=”128”]
```

- Logout of user "Ramon.Perez" by HMI on the device SWT650 with IP=192.168.3.81:

```
<108>1 2016-04-17T23:35:49.423Z 192.168.3.81 SWT650 – IEC62351-14:1
[62351-14@41912 ID=”0000038” Text=”Logout” SOE=”132” UsrID=”Ramon.Perez”
Param(0)=”HMI”]
```

- Failed authentication of user "secadm" by PROCOME using Local Port on the device IED_TEST with IP=192.168.4.81:

```
<108>1 2016-04-17T14:29:36.187Z 192.168.4.81 IED_TEST – IEC62351-14:1
[62351-14@41912 ID=”0000039” Text=”Login failed” SOE=”189” UsrID=”secadm”
Param(0)=”PROCOME” Param(1)=”LocalPort”]
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.4 Syslog Format for Protection Events (SOE)

The structure of a Syslog protection event (SOE) is as follows:

HEADER SP **STRUCTURED-DATA** SP **MSG**

G.4.1 HEADER Format

RFC 5424 Information Fields		
HEADER	***PRI***	= "<PRIVAL>" Event priority: PRIVAL = (8 x ***Facility***) + (***Severity***) ***Facility***: 13 log audit 16 local use 0 (local0) 17 local use 1 (local1) 18 local use 2 (local2) ***Severity***: 2 Critical: critical conditions 4 Warning: warning conditions 6 Informational: informational messages 7 Debug: debug-level messages
	VERSION	1
	TIMESTAMP	Date and time of event. The format is: ***FULL-DATE "T" FULL-TIME*** ***FULL-DATE*** = ***DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY*** ***DATE-FULLYEAR*** = 4 DIGIT ***DATE-MONTH*** = 2 DIGIT (01-12) ***DATE-MDAY*** = 2 DIGIT (01-28, 01-29, 01-30, 01-31, depending on the month) ***FULL-TIME*** = ***PARTIAL-TIME TIME-OFFSET*** ***PARTIAL-TIME*** = ***TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND "." TIME-SECFRAC*** ***TIME-HOUR*** = 2 DIGIT (00-23) ***TIME-MINUTE*** = 2 DIGIT (00-59) ***TIME-SECOND*** = 2 DIGIT (00-59) ***TIME-SECFRAC*** = 3 DIGIT representing ms 000~999 (000 when not in use) ***TIME-OFFSET***="Z" (represents the date/time in UTC). UTC format is always used. Example: 2016-04-17T22:36:41.358Z
	HOSTNAME	Own IP (global or in service origin). Since the equipment can have several IP addresses, the value of the HOSTNAME takes the value of the IP address of the first enabled LAN port, following the order LAN 1, LAN 2, LAN 3 and LAN 4.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

RFC 5424 Information Fields		
	APP-NAME	Name of the device where the event occurred (equipment name). When the equipment has IEC 61850, the name of the equipment obtained from the CID configuration file will be assigned. Otherwise, it can be modified from the website and from CLI.
	PROCID	It takes the value NIL = "-", as stated in IEC 62351-14 standard.
	MSGID	It takes the value "IEC62351-14:1", as stated in IEC 62351-14 standard.

G.4.2 STRUCTURED-DATA Format

RFC 5424 Information Fields		
STRUCTURED-DATA (SD)	***SD-ID***	It takes the value "62351-14@41912", as stated in IEC 62351-14 standard.
	SOE	Circular event sequence counter from 0 to 4294967295 (INT32U although it is really a string of 10 characters). It is used to order the events according to their occurrence, since the date/time could be altered. There is one SOE counter per facility: - SOE counter for facility 13 (log audit). - SOE counter for facility 16 (local0). - SOE counter for facility 17 (local1). - SOE counter for facility 18 (local2).
	ID	Universal identifier that identifies the event in a unique way. It is a text string of 7 characters. The range of *ID* is 0 to 9999999 (0 to 3446435 for cybersecurity events and 3446436 to 9999999 for SOE protection events). ***ID*** = (100 * *REG* + *BIT*) + *Offset_SEC_ID* - *REG* is the PROCOME registration number defined for the event. - *BIT* is the bit number of the event in the PROCOME register. - *Offset_SEC_ID* is the number following the highest *ID* defined for cybersecurity events (3446436). Example: The user event "ON RFT HV OPENING" is configured in REG=40021 BIT=23 => *ID* = (100 * 40021 + 23) + 3446436 = 7448559. This is the way the user knows the *ID* of the event he/she configures.
	Text	Descriptive text of the event, along with the value and quality of the event, all separated by the character "|" (e.g. "*Phase A Instantaneous unit 1 Trip|On|Good*"). It is a text string of up to 127 characters. This is the same text as the event log.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.4.3 MSG Format

MSG is the part of the message where the values of the magnitudes related to the event are shown when the event occurred. All these magnitudes are the same as those corresponding to the events in the protection event record.

[DESC1 : MAG1 UNIT1 DESC2 : MAG2 UNIT2 …. DESC12 : MAG12 UNIT12]:

RFC 5424 Information Fields		
MSG	***DESCX***	Label of the magnitude configured in *Settings\Records\Events\ Events Magnitudes\Magnitude* ***X***. The size is up to 21 characters.
	MAGX	Value of the magnitude configured in *Settings\Records\Events\ Events Magnitudes\Magnitude* ***X***. The size is 5 characters.
	UNITX	Unit of magnitude configured in *Settings\Records\Events\ Events Magnitudes\Magnitude* ***X***. The size is up to 10 characters (the longest unit description is currently 4 characters).

where ***X*** = 1..12.

G.4.4 Examples

The following is an example of a Protection event (SOE) in Syslog format:

```
<110>1 2020-04-29T12:25:35.231Z 192.168.1.81 IRF1Q11F01 - IEC62351-14:1-nocyb
[62351-14@41912 ID=”7446544” Text=”On Phase A Instantaneous unit 1
Trip|On|Good” SOE=”1234567890”]
[VA63.1VVB34VVC63.41VVG26.87VIA13.81AIB24AIC13.41AIG23.87AIGS4.75A]
```


© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.5 Syslog Format for Based on IEC 61850 Events (SOE)

The structure of a Syslog protection event (SOE) is as follows:

HEADER SP **STRUCTURED-DATA** SP **MSG**

G.5.1 HEADER Format

RFC 5424 Information Fields		
HEADER	***PRI***	= "<PRIVAL>" Event priority: PRIVAL = (8 x ***Facility***) + (***Severity***) ***Facility***: Configuration parameter *facility*. ***Severity***: Configuration parameter *severity*. E.g.: *110*.
	VERSION	It takes the value of the parameter *version.* E.g.: *1*
	TIMESTAMP	Date and time of event. The format is: ***FULL-DATE "T" FULL-TIME*** ***FULL-DATE*** = ***DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY*** ***DATE-FULLYEAR*** = 4 DIGIT ***DATE-MONTH*** = 2 DIGIT (01-12) ***DATE-MDAY*** = 2 DIGIT (01-28, 01-29, 01-30, 01-31, depending on the month) ***FULL-TIME*** = ***PARTIAL-TIME TIME-OFFSET*** ***PARTIAL-TIME*** = ***TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND "." TIME-SECFRAC*** ***TIME-HOUR*** = 2 DIGIT (00-23) ***TIME-MINUTE*** = 2 DIGIT (00-59) ***TIME-SECOND*** = 2 DIGIT (00-59) ***TIME-SECFRAC*** = 3 DIGIT representing ms 000~999 (000 when not in use) ***TIME-OFFSET***="Z" (represents the date/time in UTC). UTC format is always used. Example: 2016-04-17T22:36:41.358Z
	HOSTNAME	It takes the value interpreted from the configuration parameter hostname. E.g.: *192.168.1.81*
	APP-NAME	It takes the value interpreted from the configuration parameter *appName*. E.g.: *L45GISDB*
	PROCID	It takes the value NIL = "-", as stated in IEC 62351-14 standard.
	MSGID	It takes the value of the configuration parameter *msgId*. E.g.: *IEC62351-14:1-nocyb*.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.5.2 STRUCTURED-DATA Format

RFC 5424 Information Fields		
STRUCTURED-DATA (SD)	***SD-ID***	It takes the value of the configuration parameter *sdId*. E.g.: *62351-14@41912*.
	SOE	Circular event sequence counter from 0 to 4294967295 (INT32U although it is really a string of 10 characters). It is used to order the events according to their occurrence, since the date/time could be altered.
	ID	Universal identifier that identifies the event in a unique way. It takes the interpreted value of the configuration parameter *idSyslog*. E.g.: e8ca5212bec076cc
	Text	Descriptive text of the event. It takes the interpreted value of the configuration parameter *textSyslog* E.g.: *INT502|ED-2|BREAKER 52 CLOSED|ON|good*

G.5.3 MSG Format

MSG is the part of the message where the values of the magnitudes related to the event are shown when the event occurred. It is important to remark that the magnitudes shown in each event can be different from each other and the values of these magnitudes will be always primary values.

The field MSG will have a limit of 1000 characters. If the field is bigger than this limit, then the field will be truncated to 1000 characters.

There are different fields depending on which magnitude has been configured:

- *desc*: Description of the magnitude according to the configuration parameter *descSyslog*.
- *Val*: Value of the magnitude in primary values.
- *Unit1*: Unit of the magnitude. It will be empty if the magnitude does not have unit.
- *Ang*: Angle of the magnitude.
- *Unit2*: Unit of angles (º).

The rules to form the MSG field are the following ones:

- If the value and the angle of a magnitude have been configured, then the *desc* field will take the value of the configuration parameter *descSyslog* of the configured value (*desc=ValUnit1,AngUnit2*).
- If only the value or the angle of a magnitude has been configured, then the *desc* field will take the value of the configuration parameter *descSyslog* of the configured value or angle: (*desc=ValUnit1*) or (*desc=AngUnit2*).
- The character comma (,) is used to separate a value from its angle.
- The character blank space ( ) is used to separate magnitudes.

E.g.: The magnitudes MMXU1.A.phsA.instCVal.mag.f, MMXU1.A.phsA.instCVal.ang.f, MMXU1.PhV.phsA.instCVal.mag.f y MMXU1.PhV.phsA.instCVal.ang.f are configured, then MSG field will be as follows: IA=123.567A,90.000º VA=38.956kV,2.087º

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

G.5.4 Examples

The following is an example of a Protection event (SOE) in Syslog format:

```
<110>1 2020-04-29T12:25:35.231Z 192.168.1.81 IRF1Q11F01 - IEC62351-14:1-nocyb
[62351-14@41912 ID="e8ca5212bec076cc" Text="INT502|ED-2|BREAKER 52
CLOSED|ON|good" SOE="1234567890"] VA=0.000V,0.000° VB=0.000V,0.000°
VC=0.000V,0.000° VG=0.000V,0.000° IA=0.000A,0.000° IB=0.000A,0.000°
IC=0.000A,0.000° IG=0.000A,0.000° IGS=0.000A,0.000°
```

G.6 Syslog Transmission

The device can send events via Syslog protocol to up to 3 Syslog servers.

To communicate these events in Syslog format to said servers, the UDP protocol (standard port UDP/514), as specified in RFC 5426, or the TCP protocol, as specified in RFC 6587, can be used. Regarding the TCP protocol, the octet counting framing method is used.

To connect to each of the 3 possible Syslog servers, the following settings can be modified from the configuration tool and from HMI, corresponding to the IP addresses of each server and the logical port to communicate with it:

Syslog Transmission Settings - Server 1				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
IP Address	IP Address	ddd.ddd.ddd.ddd		0.0.0.0
Port	Port	1 - 65535	1	514
Protocol	Protocol	UDP TCP		UDP

Syslog Transmission Settings - Server 2				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
IP Address	IP Address	ddd.ddd.ddd.ddd		0.0.0.0
Port	Port	1 - 65535	1	514
Protocol	Protocol	UDP TCP		UDP

Syslog Transmission Settings - Server 3				
Configuration Tool	**HMI**	**Range**	**Step**	**Default**
IP Address	IP Address	ddd.ddd.ddd.ddd		0.0.0.0
Port	Port	1 - 65535	1	514
Protocol	Protocol	UDP TCP		UDP

Sending events to a server can be disabled by setting the IP address of the Syslog server to 0.0.0.0. The Syslog client can also be deactivated by disabling the Syslog service, as described in the section **Ports and Communication Services** in the Cybersecurity Annex.

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

H. List of Illustrations and Tables

H.1 List of Figures

1.1 Introduction 1.1-1
Figure 1.1.1: General HW Design. 1.1-4
Figure 1.1.2: Measurement Processing. 1.1-5
Figure 1.1.3: Functional Diagram. 1.1-6

1.4 Current Transformers Dimensioning 1.4-1
Figure 1.4.1 Knee Point Voltage Definition. 1.4-5

1.5 Physical Description 1.5-1
Figure 1.5.1 Front of a 6U x 19" 1/3 Rack Model. 1.5-2
Figure 1.5.2 Front of a 6U x 19" 1/3 Rack Model with Extended Buttons Display. 1.5-3
Figure 1.5.3 Rear of a 6U x 19" 1/3 Rack Model. 1.5-4
Figure 1.5.4 Three 6U x 19" 1/3 RTF Rack Mounted. 1.5-5
Figure 1.5.5 Mounting two RTF to Steel Plate (built-in into the cell). 1.5-5
Figure 1.5.6 Alphanumeric Display. 1.5-8
Figure 1.5.7 Graphic Display. 1.5-8
Figure 1.5.8 Keypad. 1.5-9
Figure 1.5.9 Command Panel Default Screen. 1.5-9
Figure 1.5.10 Example of configured command panel screen. 1.5-10
Figure 1.5.11 Command Buttons. 1.5-12
Figure 1.5.13 Example of programmable buttons screen. 1.5-15
Figure 1.5.14 Range Settings. 1.5-16
Figure 1.5.15 Numbered Settings. 1.5-16
Figure 1.5.16 Selection Settings. 1.5-17
Figure 1.5.17 Mask Settings. 1.5-17
Figure 1.5.18 Element Enable Logic. 1.5-22
Figure 1.5.19 Digital Inputs Test. 1.5-27
Figure 1.5.20 Configuration of Communications Ports for Relays without Ethernet Redundancy. 1.5-31
Figure 1.5.21 Configuration of Communications Ports for Relays with Bonding Type Redundancy (Hot Stand By). 1.5-32
Figure 1.5.22 Configuration of Communications Ports for Relays with RSTP Type Redundancy. 1.5-32
Figure 1.5.23 Example of Connecting Relays with RSTP Redundancy with Simple Ring. 1.5-33
Figure 1.5.24 Configuration of Communications Ports for the Relay with PRP Type Redundancy. 1.5-33
Figure 1.5.25 Configuration of Communications Ports for the Relay with HSR Type Redundancy. 1.5-34
Figure 1.5.26 Examples of Common Redundancies. 1.5-35

1.6 Installation and Commissioning 1.6-1
Figure 1.6.1: Name Plate (RTF). 1.6-4

2.1 Voltage Regulator 2.1-1
Figure 2.1.1 Alphanumeric Display. 2.1-3
Figure 2.1.2 Insensitivity Degree. 2.1-5
Figure 2.1.3 Schematic Representation of Raise / Lower the Tap. 2.1-6
Figure 2.1.4 Time Curve for the First Control Operation: T1. ..... 2.1-8
Figure 2.1.5 Delay Time for Following Control Operations: T2 ..... 2.1-9

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Figure 2.1.6 Line Drop Compensation (LDC). 2.1-10
Figure 2.1.7 Line Drop Compensation: LDC-R&X. 2.1-12
Figure 2.1.8 Diagram of two Transformers with Different Impedances Working in Parallel. 2.1-14
Figure 2.1.9 Diagram Representing the Reactive Circulating Current. 2.1-15
Figure 2.1.10 Combined Compensation and Maximum Compensation. 2.1-18
Figure 2.1.11 Maximum Compensation Setting. 2.1-18
Figure 2.1.12 Main Regulator Control Loop (Automatic Mode). 2.1-19
Figure 2.1.13 Tap Monitoring Setting Diagram. 2.1-22
Figure 2.1.14 Blocking by Voltage out of Range. 2.1-24
Figure 2.1.15 Blockings within the Main Regulator Control Loop (Automatic Mode). 2.1-26
Figure 2.1.16 Specific Raise / Lower the Tap Blockings (Automatic and Manual Modes). 2.1-27
Figure 2.1.17 Power Flow Reversal Diagram. 2.1-28
Figure 2.1.18 Band Diagram. 2.1-29
Figure 2.1.19 Information in Default Screen. Alphanumeric Display. 2.1-30
Figure 2.1.20 Information in Control Screen (once the information element has been added in the control configuration of the device). Graphical Display. 2.1-30
Figure 2.1.21 Information in Default Screen. Graphical Display. 2.1-30
Figure 2.1.22 Example 1 Information. 2.1-33
Figure 2.1.23 Example 2 Information (Modifying the VT/CT Connection). 2.1-35

3.1 Voltage Elements 3.1-1
Figure 3.1.1 Block Diagram of the Phase Overvoltage Element. 3.1-3
Figure 3.1.2 Inverse Curve with Values Truncated at 1.23 Times. 3.1-4

3.2 Frequency Elements 3.2-1
Figure 3.2.1 Block Diagram of a Frequency Element. 3.2-3
Figure 3.2.2 Load Shedding System in an Industrial Plant. 3.2-9

4.1 Voltage Measurement Circuit Supervision 4.1-1
Figure 4.1.1 Voltage Circuit Failure Detection Element Scheme. 4.1-2

4.2 Trip and Close Coil Circuit Supervision 4.2-1
Figure 4.2.1 Trip/Close Coil Circuit Supervision Block Diagram. 4.2-4
Figure 4.2.2 Hard Wiring for the Control Circuit Supervision Test of the SLOT X (A and/or B). 4.2-8

4.8 Open Pole Detector 4.8-1
Figure 4.8.1 Logic Diagram of the Open Pole Detector with 3 Inputs. 4.8-2
Figure 4.8.2 Logic Diagram of the Open Pole Detector with 2 Inputs. 4.8-3

4.9 Pole Discordance Detector 4.9-1
Figure 4.9.1 Diagram of the Pole Discordance Detector. 4.9-2

5.3 Metering History Log 5.3-1
Figure 5.3.1 Explanatory Diagram of the Metering Log. 5.3-2
Figure 5.3.2 Metering History Log Logic. 5.3-3

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

H.2 List of Tables

1.4 Current Transformers Dimensioning 1.4-1
Table 1.4-1: General Parameters 1.4-6
Table 1.4-2: Saturation Free Time and Fault Current Values 1.4-7

1.5 Physical Description 1.5-1
Table 1.5-1: Digital Inputs of the Inputs Module 1.5-23
Table 1.5-2: Digital Outputs of the Inputs Module 1.5-24
Table 1.5-3: Auxiliary Outputs of the Outputs Module 1.5-26
Table 1.5-4: Output Signals of the Communications Module 1.5-48
Table 1.5-5: Output Signals of the Synchronization Module 1.5-53

1.10 Alarm Codes 1.10-1
Table 1.10-1: Alarm Status Magnitude and Severity Level 1.10-3

1.11 Troubleshooting 1.11-1
Table 1.11-1: Power Up 1.11-2
Table 1.11-2: In Service / Alarm Contact 1.11-3
Table 1.11-3: Error Messages during Power Up - IEC61850 Devices 1.11-3
Table 1.11-4: Error Messages during Power Up - IEC61850 Devices 1.11-4
Table 1.11-5: Error Messages when the Relay is in Normal Operation 1.11-4
Table 1.11-6: Errors while Communicating 1.11-5
Table 1.11-7: Error in Digital Inputs 1.11-7
Table 1.11-8: Error in Digital Outputs 1.11-7
Table 1.11-9: Error in Transducer Inputs 1.11-8

2.1 Voltage Regulator 2.1-1
Table 2.1-1: Delay Time Summary Table 2.1-9
Table 2.1-2: Example 1 for Settings Calculation 2.1-33
Table 2.1-3: Example 2 for Settings Calculation 2.1-35
Table 2.1-4: Analog Inputs to the Voltage Regulator Module 2.1-39
Table 2.1-5: Digital Inputs of the Voltage Regulator 2.1-39
Table 2.1-6: Auxiliary Outputs and Events of the Voltage Regulator 2.1-41
Table 2.1-7: Voltage Measurement Test 2.1-46
Table 2.1-8: Local and Parallel Current Measurement Test 2.1-47
Table 2.1-9: Circulating Current Measurement Test 2.1-47
Table 2.1-10: Line Drop Compensation LDC-Z Test 2.1-49
Table 2.1-11: Line Drop Compensation LDC R-X Test 2.1-50
Table 2.1-12: Reactive Compensation through Wiring Test 2.1-51
Table 2.1-1: Reactive Compensation Test through Communications 2.1-52

3.1 Voltage Elements 3.1-1
Table 3.1-1: Analog Inputs of the Phase Overvoltage Modules 3.1-5
Table 3.1-2: Digital Inputs to the Phase Overvoltage Modules 3.1-6
Table 3.1-3: Auxiliary Outputs and Events of the Phase Overvoltage Modules 3.1-7
Table 3.1-4: Pickup and Reset of the Overvoltage Elements 3.1-8

3.2 Frequency Elements 3.2-1
Table 3.2-1: Auxiliary Outputs and Events of the Undervoltage Element for Blocking 3.2-5
Table 3.2-2: Voltage Reset 3.2-7
Table 3.2-3: Analog Inputs to the Underfrequency Modules 3.2-11

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

Table 3.2-4: Digital Inputs to the Underfrequency Modules 3.2-11
Table 3.2-5: Auxiliary Outputs and Events of the Underfrequency Modules 3.2-12
Table 3.2-6: Pickup and Reset of the Underfrequency Elements 3.2-13

4.1 Voltage Measurement Circuit Supervision 4.1-1
Table 4.1-1: Analogue Inputs to the Voltage Measurement Circuit Supervision Module 4.1-3
Table 4.1-2: Digital Inputs to the Voltage Measurement Circuit Supervision Module 4.1-4
Table 4.1-3: Auxiliary Outputs and Events of the Voltage Measurement Circuit Supervision Module 4.1-4

4.2 Trip and Close Coil Circuit Supervision 4.2-1
Table 4.2-1: Configuration of Digital Inputs for Supervision by SLOTS 4.2-3
Table 4.2-2: Auxiliary Outputs and Events of the Coil Circuit Supervision Module 4.2-7

4.5 Change Settings Groups 4.5-1
Table 4.5-1: Digital Inputs to Change Settings Groups 4.5-3
Table 4.5-2: Auxiliary Outputs and Events to Change Settings Groups 4.5-4

4.6 Time Zone Calendar 4.6-1
Table 4.6-1: Auxiliary Outputs of the Time Zone Calendar 4.6-3

4.8 Open Pole Detector 4.8-1
Table 4.8-1: Analog Inputs to the Open Pole Module 4.8-4
Table 4.8-2: Digital Inputs to the Open Pole Module 4.8-4
Table 4.8-3: Auxiliary Outputs and Events of the Open Pole Module 4.8-5

4.9 Pole Discordance Detector 4.9-1
Table 4.9-1: Digital Inputs to the Pole Discordance Detector Module 4.9-3
Table 4.9-2: Auxiliary Outputs and Events of the Pole Discordance Detector Module 4.9-4

5.1 Oscillographic Recording 5.1-1
Table 5.1-1: Digital Inputs of the Oscillographic Recording 5.1-5
Table 5.1-2: Auxiliary Outputs and Events of the Oscillographic Recording 5.1-6

5.2 Event Record 5.2-1
Table 5.2-1: Event Record 5.2-2

© ZIV APLICACIONES Y TECNOLOGÍA, S.L. Zamudio, 2019

License agreement for Software Embedded in Equipment

ZIV APLICACIONES Y TECNOLOGÍA, S.L.
End-User Software License Agreement

THE EQUIPMENT YOU HAVE PURCHASED INCLUDES EMBEDDED SOFTWARE PROGRAM(S). THE PROGRAM IS COPYRIGHTED AND IS BEING LICENSED TO YOU (NOT SOLD) FOR USE WITH THE EQUIPMENT.

THIS IS A LEGAL AGREEMENT BETWEEN US (AS "LICENSEE) AND ZIV APLICACIONES Y TECNOLOGÍA, S.L. (AS "LICENSOR") FOR THE SOFTWARE PROGRAM INCLUDED WITH THE EQUIPMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE EQUIPMENT.

IF YOU INSTALL OR USE THE EQUIPMENT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE EQUIPMENT UNUSED TO YOUR SELLER, AND YOU WILL RECEIVE A REFUND OF YOUR MONEY.

Terms and Conditions of License

1. **License Grant**. Licensor hereby grants to you, and your accept, a nonexclusive and non-transferable license to use the embedded programs and the accompanying documentation, if any (collectively referred to as the "Software"), only as authorized in this License Agreement.
2. **Restrictions.** You may not (a) use, copy, modify or transfer the Software except as expressly provided in this or another Agreement with Licensor, (b) reverse engineer, decompile or disassemble or separate the components of the Software, or (c) rent, sell or lease the Software or make the Software available to others to do any of the foregoing.
3. **No Assignment.** This License is intended for your exclusive use with the purchased equipment. You agree that you will not assign, sublicense, transfer, pledge, lease, rent or share your rights under this License Agreement.
4. **Licensor's Rights.** You acknowledge and agree that the Software is the proprietary product of Licensor protected under U.S. copyright law and international treaties.. You further acknowledge and agree that all right, title and interest in and to the Software, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an ownership interest in or to the Software, but only a limited right of use revocable in accordance with the terms of this License Agreement.
5. **Confidentiality**. The Software is confidential and no details or information relating to the same shall be disclosed to any third party without the prior written consent of Licensor. For the purposes of this clause, sub-contract staff, employed or retained by the Licensee to perform computer systems development work, shall not be deemed to be third parties provided such staff are subject to the disclosure restrictions set forth above. In no event, except with a prior written authorization duly signed by an officer of Licensor, may you disclose any such confidential information, even for subcontracted jobs, to persons or entities that may be considered to be direct competitors of Licensor.

6. **Term**. The License Agreement is effective upon delivery of the equipment to you and shall continue until terminated. You may terminate this License Agreement at any time by returning the equipment to Licensor, or by destroying the equipment. Licensor may terminate this License Agreement upon your breach of any term hereof. Upon such termination by Licensor, you agree to return the equipment to Licensor.
7. **Warranty and Disclaimer.** Licensor warrants, for your benefit only, that the Software, when and as delivered to you, will conform to the specifications described in the instruction manuals for the equipment purchased, or any specifications agreed to in writing by Licensor with a particular customer. This warranty does not cover any minor errors or deviations from the specifications that do not affect the proper functioning of the equipment. **EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE SOFTWARE IS LICENSED "AS IS", AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**
8. **Licensee's Remedy.** You sole and exclusive remedy for any breach of Licensor's warranty shall be the repair or replacement, at Licensor's sole option, of any Software that does not conform to stated specifications. Licensor shall not be responsible for any failure arising from inadequate or improper use of the Software.
9. **Limitation of Liability.** Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the purchase price paid to Licensor for the equipment. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if licensor has been advised of the possibility of such damages.
10. **Trademark.** All ZIV trademarks (including ZIVERCOM, ZIVERLOG and ZIVERSYS) are common law trademarks of Licensor. No right, license or interest to such trademarks is granted hereunder, and you agree that no such right, license or interest shall be asserted by you with respect to such trademark.
11. **Licensee's Indemnity.** You shall defend, indemnify and hold Licensor harmless against any loss or damage of any kind arising from a breach by you of this License Agreement, or any use or misuse of the Software by you or your employees, agents or representatives, and from any other of your conduct or from any claim or action by any of your customers in connection with the Software or this License Agreement.
12. **Governing Law.** This License Agreement shall be construed and governed in accordance with the internal laws of the State of Illinois, U.S.A.
13. **No Waiv**er. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.
14. **Entire Agreement**. This License Agreement is the entire agreement between you and Licensor with respect to the use of the software and supersedes all prior understandings or agreements between the parties. This License Agreement may be amended only by a writing signed by an officer of Licensor.

ZIV Aplicaciones y Tecnología S.L.
Parque Tecnológico, 210
48170 Zamudio (Bizkaia)
Apartado 757
48080 Bilbao - Spain
Tel.- (34) 94 452.20.03