

SISTEMA DE GESTIÓN DE INFORMACIÓN DE PROTECCIONES

Autores

E. Rivero
UNELCO ENDESA (Grupo Endesa). España
L. Astarloa
R. Quintanilla
ZIV Aplicaciones y Tecnología, S. A. España

Introducción

Las redes eléctricas son, como todos dispositivos tecnológicos, susceptibles de sufrir anomalías de diferentes orígenes (faltas, inestabilidades, desequilibrios...) que, si no son atajadas a tiempo, conducen a daños que pueden ser de gran consideración con la consiguiente repercusión en los costes de operación y en el propio mercado, cuando no en sanciones por parte de las autoridades reguladoras o administrativas.

Un disturbio no resuelto adecuadamente desencadena una serie de acontecimientos que pueden conducir a un cero de tensión de graves proporciones. Una vez iniciada resulta difícil detenerla; dificultad que crece rápidamente con el tiempo de forma que llega un momento en que resulta imposible y el desastre está asegurado. Se produce la pérdida de mercado durante un tiempo que puede llegar a ser de varias horas y, en el peor de los casos, de más de un día. Pérdida de mercado inmediato y grave deterioro de la imagen, con consecuencias negativas seguras a medio y largo plazo.

Cadena accidental de acontecimientos

Una vez que el desastre se ha producido, aparecen voces ofreciendo alternativas a la topología, operación y gestión de las redes eléctricas. Hoy la tecnología ofrece posibilidades de mejora en cualquiera de estos aspectos, desde la introducción de generación distribuida e inteligente hasta la modernización de los dispositivos y sistemas de protección y control, pasando por la construcción de nuevas líneas, mejorando el mallado y la redundancia topológica de las redes.

Por supuesto, todas ellas son soluciones posibles y aplicables; cada una de ellas con diferentes resultados potenciales y muy distintos niveles de inversión, en un mercado en el que, por sus condiciones actuales, precisamente la inversión no resulta, por muchos motivos, suficientemente atractiva. Resulta cierto además que cualquiera de las alternativas, sobre todo las que recomiendan cambios drásticos en la concepción de la red, debe ser analizada a fondo para conocer los efectos que a

medio y largo plazo tendrá sobre la eficiencia y fiabilidad globales del sistema eléctrico.

En muchos de los casos, el acontecimiento desencadenante es único, aunque a veces resulta arduo llegar a determinar cuál fue, incluso tras complejos análisis de los resultados. Lo que habitualmente ocurre es que este acontecimiento se produce en un sistema en equilibrio muy precario, que tiene un gran número de debilidades que son, podemos decir, activadas por el suceso desencadenante. Así, tras los análisis, suele ocurrir que todo parece ser el resultado de una cadena de coincidencias accidentales, cuando lo que ha ocurrido es que el sistema estaba operando en un estado de **n-1** defectos de fiabilidad. En esta situación, un fallo más conduce, sin remedio, al desastre. Resulta difícil determinar cual de ellos es el realmente responsable; desde el punto de vista del análisis de causas todos ellos lo son, aunque decidamos que lo es el último en la secuencia temporal de fallos en la fiabilidad. Es el caso, tantas veces usado como ejemplo, de la última gota que desborda un vaso que ya estaba lleno por muchas otras gotas.

Valor de la información

El escenario descrito en el apartado anterior es el típico de un sistema complejo sobre el que se dispone de poca información o, en todo caso, insuficiente o poco organizada.

A pesar de lo que pueda parecer, sobre todo a tenor de lo que se lee y escucha en los medios de información cuando el desastre ocurre, el sistema eléctrico tiene un grado muy alto de fiabilidad y solidez. No olvidemos que se trata de un sistema que, en España, transporta cada día la energía equivalente a 40 bombas atómicas (más de 600 en USA) y, aun así, permanece en equilibrio dinámico. Es un sistema expuesto, en gran parte de su extensión a agresiones de todo tipo: climáticas (rayos, manguitos de hielo, viento, inundaciones...), ambientales (humo de incendios, árboles próximos a las líneas, aves...), accidentes derivados de la actividad humana (excavadoras, grúas, vuelos a baja altura...)...

Los pilares sobre los que se soporta la solidez del sistema eléctrico son varios y de diferente tipo:

- **Diseño**, en el que se han tenido en cuenta las posibilidades de fallo, con un alto grado de redundancia.
- **Mantenimiento** adecuado con especial dedicación a los aspectos preventivos que minimizan las posibilidades de fallo.
- **Sistemas de supervisión en tiempo real** que, a caballo de las más avanzadas tecnologías de comunicaciones y proceso de información, permiten el conocimiento del estado del sistema y la actuación inmediata de los operadores y/o automatismos para corregir o compensar las anomalías que se produzcan.
- **Sistema de protección** encargado de detectar las faltas instantáneamente y tomar las acciones necesarias para su aislamiento, minimizando el daño producido y el sector de red afectado.

El sistema de protección vigila el estado de la red en condiciones normales de operación, pero es al producirse un defecto cuando pone en marcha, no solo sus funciones automáticas para decidir en milisegundos que interruptores debe operar para garantizar el equilibrio del sistema, sino un sofisticado sistema de captura y almacenamiento de información sobre la evolución de la red inmediatamente antes, durante e inmediatamente después de la aparición del disturbio.

Esta información es de vital importancia ya que describe la reacción del sistema real en condiciones de falta real. Y no solo eso sino que almacena información de la reacción del propio sistema de protección y control.

Esta información es de primerísima utilidad para conocer la red en detalle y para detectar defectos en su diseño, en su fiabilidad, en los sistemas de operación, en el sistema de protección... Información que posibilita acciones de mantenimiento preventivo, diseño de automatismos de alta velocidad que ayuden al operador humano en las tomas de decisión, inicio de acciones correctoras... En fin, decisiones y acciones que ayudan a mejorar la solidez del sistema y a que no se produzcan desastres en su operación.

Naturalmente, lo dicho es cierto sólo si la información es recogida, ordenada, analizada y utilizada. En este paper se presenta, precisamente, un sistema para la recogida automática, la normalización y la ordenación de dicha información de manera que resulte útil a todos los departamentos de la compañía que pueden tomar decisiones para mejorar su fiabilidad y su eficacia. Es decir, para mejorar el conocimiento que la compañía posee sobre el proceso técnico de su negocio.

Tecnología digital y comunicaciones

Todo lo expuesto hasta ahora es cierto, con independencia de las tecnologías utilizadas para el control y protección de las redes eléctricas. La tecnología digital introduce un doble diferencia:

- Capacidad de capturar y almacenar información.
- Comunicaciones digitales: capacidad de enviar rápidamente la información recogida hasta lugares muy alejados de donde se produce. Esta es la aportación más importante de la tecnología digital en el campo de las protecciones, tanto es así que podríamos decir que una protección digital no comunicable puede, en todos los sentidos, considerarse una protección convencional.

Tecnología digital y comunicaciones marcan la diferencia: ponen a disposición del analista una enorme cantidad de datos que pueden ser utilizados tanto para el análisis de la actuación del sistema de protección como para conocer en mayor profundidad el sistema protegido, es decir, la red eléctrica.

Para que la información sea útil para tomar decisiones a corto plazo y, además, se convierta en conocimiento de la propia red, deben cumplirse algunos requisitos que enmarcan los problemas con los que las compañías se enfrentan en el manejo de los datos capturados.

- Recuperación rápida, lo que significa rápida disponibilidad para el análisis.
- Necesidad de conectarse y operar con datos procedentes de muy diversos equipos y de diferentes fabricantes y como consecuencia:
 - Normalización y unificación de formatos de la información capturada ya que diferentes dispositivos y fabricantes utilizan distintas soluciones a los problemas de captura, almacenamiento y protocolos de comunicaciones.

El Sistema de Gestión de Información de Protecciones (SGP) que se presenta en este paper cumple con ambos requisitos y ofrece una solución simple y escalable en coste.

Objetivos del proyecto

UNELCO ENDESA es una compañía eléctrica integrada dentro del grupo ENDESA y localizada en el archipiélago de las Islas Canarias que, durante el año 2003 suministro 7,046 GWh de energía a un total de 976,138 clientes distribuidos en siete islas.

La gestión y el control de un sistema de protecciones extendido por siete islas presenta serios problemas de logística. La recogida de sucesos y oscilos, así como la realización de cambios de ajustes implican sobrecostos debidos a los gastos de desplazamiento y, sobre todo, tiempos de respuesta muy lentos ante cualquier intervención.

UNELCO ENDESA y ZIV iniciaron en el año 1999 el diseño de un sistema de gestión que resolviera las dificultades mencionadas. UNELCO ENDESA se responsabilizó de la especificación de requisitos del proyecto, desde el punto de vista del usuario, adaptado a su red y a sus equipos de protección y registro y ZIV asumió el desarrollo de una solución que no sólo pudiera aplicarse a la red de UNELCO ENDESA sino que sirviera para dar solución a problemas similares sobre cualesquiera otras redes y equipos.

El sistema inició su operación, con un número limitado de equipos, en Julio de 1999. A partir de entonces se han ido incorporando diferentes modelos, fabricantes y equipos, con funcionamiento satisfactorio para el usuario.

Los objetivos planteados al inicio del proyecto, fueron la resolución de los dos problemas mencionados y la obtención adicional de otras ventajas que, también tiene sus consecuencias sobre los costes de explotación:

- La misma base de tiempos en todas las instalaciones.
- Datos unificados en formato independiente del fabricante del equipo de protección.
- Base de datos única.

Con estas ideas básicas en mente, se comenzó la especificación y desarrollo de un sistema que permitiera la captura y gestión de la información de los equipos de protección, con independencia del fabricante origen de cada uno de ellos.

Sistema de Gestión de Información de protección (SGP)

Sistema Básico

En la Figura 1 puede verse la arquitectura del sistema presentado, en su forma más simple.

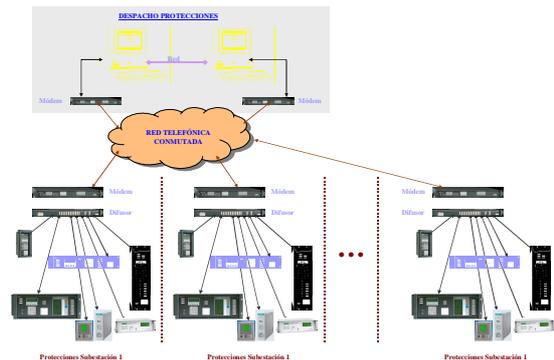


Figura 1

Está constituido por un Puesto Central, un Sistema de Comunicaciones y los Equipos de Protección.

Puesto Central

En el caso de la compañía UNELCO ENDESA, actualmente, el puesto central consta de dos ordenadores, conectados en red, que se reparten la tarea de lanzamiento de llamadas y que se utilizan como puestos de operación simultáneos. En el futuro, se añadirá dos puestos más, ubicados en otra isla del archipiélago.

La aplicación SGP está instalada en uno solo de los ordenadores que soporta, además, la base de datos del sistema. Sin embargo desde cualquiera de los otros ordenadores se tiene total acceso a la información y a las funciones del sistema:

- Configuración del sistema
 - Instalaciones
 - Equipos de protección y registro
 - Posiciones
 - Fabricantes
 - Automatismo y calendario de llamadas periódicas
 - Informes, filtros...

- Soporte de la base de datos, única para ambos ordenadores del puesto central:
 - Instalaciones y equipos
 - Información en formato unificado de la información recogida.
 - Información elaborada (informes de incidencias, informes diarios, estadísticas...) a partir de la información recogida.
 - Gestión de ajustes presentes en la base de datos protección y comparación con los ajustes reales, generación de alarmas, en caso de que no sean coincidentes; posibilidad de emitir una orden de actualización de la base de datos.
- Comunicación con los equipos de las subestaciones y control de los diferentes modos de operación:
 - Emulación de protocolos de cada uno de los equipos de protección que se encuentran en la base del sistema.
 - Establecimiento manual o automático del canal de comunicaciones e interrogación a los equipos de protección instalados en las subestaciones.
 - Establecimiento manual de comunicación, en modo transparente utilizando el programa del fabricante.
- Recogida de la información (sucesos, informes de falta, registros oscilográficos, ajustes...) y almacenamiento en formato unificado, independiente del fabricante del equipo o equipos interrogados.
- Visualización de la información recogida y elaborada:
 - Filtros, exportación, impresión...
 - Instalaciones y equipos
 - Estado de equipos, alarmas, errores de comunicación...
 - Sucesos, informes de falta, registros oscilográficos...
 - Incidencias e informes elaborados

Sistema de Comunicaciones

El sistema de comunicaciones en esta configuración, la más simple, está constituido por la Red Telefónica Conmutada, los modems de acceso en el Puesto Central y en las subestaciones y los difusores que realizan la función de concentradores pasivos y constituyen los nudos de la estrella ramificada que la red forma en la propia subestación.

Adelantamos que ésta no es la configuración utilizada por UNELCO ENDESA, que contiene otros equipos que, como veremos más adelante, facilitan la recogida de información.

Equipos de Protección

Los equipos de protección son los que capturan y generan información y la almacenan, a la espera de que el puesto central les interroge y se la envíen, en respuesta a la interrogación.

Limitaciones del Sistema

El sistema descrito es perfectamente operativo y constituye el mínimo necesario para disponer de las ventajas de un gestor de información de protecciones.

Aun siendo plenamente operativo, el SGP descrito tiene alguna limitación derivada de su simplicidad:

- Los equipos de protección utilizados deben todos disponer de protocolos serie asíncronos, con capacidad para funcionar en sistemas multipunto.
- La velocidad de recogida de información dista mucho de resultar óptima ya que debe establecerse conexión con cada uno de los equipos de cada una de las subestaciones.

Operación

El sistema se configura dando de alta en la base de datos el conjunto de equipos que se van a conectar a él y las instalaciones en las que se encuentran. La configuración incluye: modelos, protocolos y perfiles de comunicación, números de teléfono, velocidad, paridad, instalaciones asignadas a cada unidad del puesto central... Asimismo se establecerán los parámetros de la comunicación automática: orden de llamadas, número de intentos, frecuencia...

Cada uno de los ordenadores del puesto central realiza las llamadas a las instalaciones que le han sido asignadas durante el proceso de configuración, lanza los protocolos indicados en cada subestación e interroga a los equipos.

La información obtenida de los equipos: ajustes, registros (sucesos, oscilos, informes de falta...) es unificada en un formato común e introducida en la base de datos. En el caso de los ajustes se comparan con los existentes en la base de datos para cada uno de los equipos; si son diferentes se produce un aviso; en este caso el usuario tiene la opción de actualizar la base de datos con los valores recogidos de campo. En las implementaciones actuales, la posibilidad de cambio remoto de ajuste ha sido limitada a petición de los usuarios.

Las comunicaciones son supervisadas en todo momento, generando históricos de fallos, errores, alarmas...

Una vez en la base de datos, la información está disponible para su consulta y manipulación. El sistema dispone de un flexible conjunto de filtros (fechas, área, subestación, equipos, incidencia...) que facilitan la recuperación de la información y su tratamiento. Asimismo dispone de herramientas para la generación de informes (diarios, estadísticas...), impresión y exportación de la información y su inserción en documentos Excel.

Aunque el sistema ofrece sus máximas ventajas cuando se utiliza en modo automático, puede también utilizarse en modo manual. Dentro de la operación manual, puede utilizarse el propio SGP, con los automatismos de comunicaciones fuera de servicio o los programas de fabricante para la comunicación con los diferentes equipos. En este último caso, la información capturada no puede quedar integrada en la base de datos ya que no es sometida al proceso unificador establecido por el sistema cuando es él que controla las comunicaciones. La información obtenida en este modo manual-programa de fabricante puede, no obstante, almacenarse sobre los soportes de memoria que el puesto central disponga para ello.

Un Paso Más

En la Figura 2, puede verse el esquema del sistema que permite obviar las limitaciones descritas para la arquitectura básica.

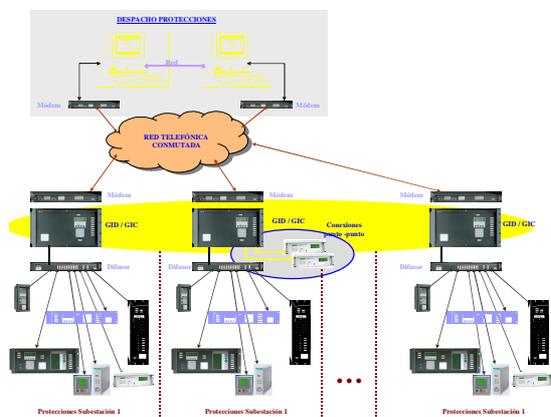


Figura 2

Si comparamos ésta con la Figura 1, veremos que la variación se encuentra en la inclusión de un nuevo equipo (GID/GIC) en cada una de las instalaciones, como parte del sistema de comunicaciones. Se trata de un equipo concentrador de información y procesador de comunicaciones, cuya función es doble:

- Automatización local de la interrogación a los equipos de protección, recogiendo la información en el momento en que se genera y almacenándola

en formato normalizado. La información queda disponible para ser enviada al SGP, en el momento en que éste realice las llamadas manuales o programadas.

Los dispositivos GID/GIC se comunican con los equipos a ellos conectados emulando los protocolos necesarios y disponiendo de tantos puertos de comunicación como se precisen, hasta un máximo de 18, en función del número de equipos y protocolos diferentes.

El SGP ya no necesita comunicarse con los equipos de protección individuales sino que en un solo proceso de comunicación con el GID/GIC, recoge toda la información almacenada hasta ese momento disminuyendo el tiempo de acceso a la información y el coste total de las llamadas a realizar

- Proporcionar un sistema multiplexor para la conexión de aquellos equipos que requieran una conexión punto-punto y no soporten comunicaciones en ambientes punto-multipunto. El equipo GID/GIC dispone de puertos que permiten la gestión de comunicaciones de este tipo de equipos de forma totalmente transparente para el sistema SGP.

La presencia de los equipos GID/GIC sigue permitiendo la comunicación, en modo transparente, por medio de los programas de fabricante, desde el puesto central del SGP.

Experiencias durante la implantación

Tanto desde el punto de vista de la compañía eléctrica destinataria del sistema como del equipo de desarrollo, la mayor dificultad encontrada ha sido la dificultad para conseguir la información necesaria para la emulación de algunos de los protocolos de comunicación con los equipos que componen el sistema de protección de UNELCO ENDESA. Este hecho no ha tenido una influencia determinante en la consecución de los objetivos del proyecto, aunque, ha supuesto un esfuerzo mayor en el desarrollo del inicialmente planificado, tanto desde el lado de ZIV como de la propia compañía eléctrica ya que ha necesitado un mayor trabajo de pruebas en campo, con los consiguientes repercusiones en el coste global de implantación.

Protocolos emulados

Como hemos visto, la emulación de protocolos se ha hecho tanto en el nivel superior SGP, como en el nivel de subestación (GID/GIC), disponiendo de un amplio espectro de protocolos disponibles entre los utilizados por los fabricantes actuales de equipos de protección y registro:

Fabricante	Tipo de Equipo	Protocolo
ABB	Protección Diferencial de Línea	SPABus
ABB	Protección Diferencial de Transformador	SPABus
ABB	Protección Sobreintensidad	SPABus
ARTUS	Registrador Oscilográfico	SOREL
GE	Protección Distancia	D-Link
GE	Protección Diferencial de Transformador	M-Link+
GE	Protección Sobreintensidad	M-Link
Siemens	Protección Distancia	Protocolo ASCII
Siemens	Protección Distancia	ZDEW/ZVEI
ZIV	Protección Diferencial de Transformador	PROCOME
ZIV	Protección Sobreintensidad	PROCOME
ZIV	Regulador de Tensión de Transformador	PROCOME
ZIV	Protección Frecuencia	PROCOME

Resultados obtenidos

Los resultados obtenidos han respondido plenamente a las expectativas planteadas al inicio del proyecto. Como resultado del trabajo UNELCO ENDESA ha obtenido:

- Una base de datos de ajustes actualizada y con la garantía de un sistema de supervisión que alarma sobre cualquier discrepancia entre el contenido de dicha base de datos y de los valores reales almacenado en la memoria de los equipos. El sistema de protección resulta con ello mucho más fiable, disminuyendo las malas actuaciones (o no actuaciones) con la consiguiente minimización de cortes y el aumento de la calidad de servicio.
- Recogida de sucesos y oscilos inmediata, sin desplazamientos, lo que permite un análisis rápido de los incidentes y la optimización de los recursos humanos, generalmente escasos, disponibles.

Ambas ventajas, aunque nos son las únicas obtenidas, tienen una repercusión económica directa en los costes de explotación. Normalización de la información, almacenamiento automático... son otras tantas ventajas que, aunque de modo indirecto, repercuten positivamente

en la eficacia de todo el sistema de protección de la compañía.

Como datos significativos, podemos indicar que el SGP, actualmente en servicio, gestiona la información de :

- 29 Subestaciones
- Más de 300 Equipos
- 5 Fabricantes

El máximo número de equipos conectados, en la misma instalación es de 24, siendo 5 el máximo número de protocolos diferentes gestionados dentro de una misma subestación.

Vías de desarrollo futuro

Son dos las vías de desarrollo futuro que las tecnologías disponibles ofrecen:

- Mejora en las infraestructuras de comunicación con las subestaciones, haciendo llegar la red corporativa hasta ellas para aprovechar los desarrollos en la normalización de protocolos y, en concreto, la inmediata realidad del nuevo estándar IEC 61850.
- Aplicación de tecnologías de acceso a la información (web e internet) que permitan la utilización de la información, dentro de la compañía, por cualquiera que la necesite, en cualquier momento del día o de la noche, no importa donde se encuentren tanto el potencial usuario como la propia información. Esto último, por supuesto, con todas las garantías de seguridad necesarias para mantener el control de accesos, sobre todo remotos, y la integridad de la información almacenada.

Conclusiones

Las conclusiones, tras el trabajo de desarrollo e implantación, han sido plenamente positivas. Se han alcanzado todos los objetivos planteados al inicio del proyecto, tanto desde la compañía eléctrica como desde el fabricante.

UNELCO ENDESA dispone de una herramienta que ha aumentado notablemente la eficiencia de su equipo de análisis de incidentes, y ha mejorado la calidad de la información disponible sobre su red y su sistema de protecciones. Podemos decir, sin miedo a exagerar, que la contribución del SGP a la gestión del conocimiento de la compañía ha sido fundamental en el proceso de optimización de sus procesos.

ZIV ha creado una herramienta de gestión de información y conocimiento, fácil de aplicar y ha obtenido una amplia biblioteca de protocolos continuamente creciente; así como una profunda experiencia en el campo de la gestión de información y las comunicaciones con equipos de otros fabricantes.