Redundancia en Teleprotección sobre Ethernet

David Gil Donate(*) **Marco Senesi Ranaldi**
ZIV **ZIV**

RESUMO

Los sistemas de conmutación de circuitos dominaron durante muchos años pero, como consecuencia de la obsolescencia del hardware usado y el auge de las redes IP, las tecnologías utilizadas hasta entonces (SDH) han sido progresivamente sustituidas por otras nuevas basadas en la conmutación de paquetes. En las redes de datagramas no se puede garantizar a priori ni el orden ni el tiempo en el que se recibe la información, ambos parámetros fundamentales para el servicio de teleprotección pero se puede aumentar la fiabilidad de las comunicaciones mediante la redundancia de rutas. Los dos protocolos incluidos en el estándar Reliable Industrial Ethernet Networks (IEC 62439-3) son HSR y PRP.

Este artículo evaluará el uso de PRP en comunicaciones de teleprotección entre subestaciones.

PALAVRAS-CHAVE

Teleprotección, Ethernet, Redundancia, Comunicaciones, PRP

1.0 - INTRODUÇÃO

Mantener una alta calidad en el servicio eléctrico es una obligación hoy en día, por lo que la detección y corrección de faltas en el menor tiempo posible es una de las prioridades de las empresas eléctricas. Para ello son fundamentales los sistemas de teleprotección, que permiten la comunicación entre protecciones de distancia remotas para tomar mejores y más rápidas decisiones.

Los canales de comunicación utilizados para el servicio de teleprotección han evolucionado con el tiempo, desde sistemas analógicos por cable piloto o portadora de línea eléctrica, pasando por redes digitales PDH y SDH, hasta las actuales redes Ethernet, que permiten transmitir fácilmente multitud de servicios entre subestaciones aprovechando de una amplia gama de tecnologías de bajo coste como 5G o DSL, incluso a veces suministradas por terceros.

En todos los casos, los equipos de teleprotección deben estar diseñados para garantizar los parámetros de seguridad (probabilidad de recibir órdenes no deseadas), obediencia (probabilidad de no perder órdenes) y tiempo máximo de transmisión bajo los valores requeridos por el servicio y especificados en la norma IEC 60834-1. (ver Tabla 1).

Esquema de Protección	Tiempo Transmisión (Tac)	Obediencia (Puc)	Seguridad (Pmc)

(*) Carrer Ciències , n° 149– CEP 08908 Hospitalet de LLobregat, Barcelona, – España Tel: (+34 933490700 – E-mail: david.gil@zivautomation.com

Bloqueo	< 10 ms	$< 10^{-3}$	$< 10^{-4}$
Premisivo subalcance	< 10 ms	$< 10^{-2}$	$< 10^{-7}$
Permisivo sobrealcance	< 10 ms	$< 10^{-3}$	$< 10^{-7}$
Disparo directo	< 10 ms	$< 10^{-4}$	$< 10^{-8}$

(*) BER = 10^{-6} para Obediencia y "peor caso" para Seguridad

Tabla 1: Requerimientos definidos en el estándar IEC 60834-1 (*)

Sin embargo, mientras que las redes PDH y SDH utilizan multiplexación determinista, las redes Ethernet tienen un comportamiento estadístico, de modo que no se puede garantizar a priori ni el orden ni el retraso con el que se recibirá la información, ambos parámetros fundamentales para el servicio de teleprotección.
En este último caso, el uso de la tecnología MPLS (Multiprotocol Label Switching) es de gran ayuda para reducir la influencia del comportamiento estadístico en los servicios de teleprotección.

2.0 - TÉCNICAS DE REDUNDANCIA EN REDES ETHERNET

Por otro lado, la fiabilidad de las comunicaciones se puede mejorar mediante técnicas de redundancia en redes Ethernet, siendo los dos protocolos incluidos en el estándar Reliable Industrial Ethernet Networks (IEC 62439-3) el HSR (High-availability Seamless Redundancy) y el PRP (Parallel Redundancy Protocol).
Ambos ofrecen tiempo de recuperación cero y pérdida de tramas en caso de falla de una ruta o equipo de red, y un sólido mecanismo de control y monitoreo de red distribuido y administrado automáticamente por todos los nodos.

2.1 HSR

El protocolo HSR se basa en la conexión en anillo de todos los nodos de la red, los cuales deben tener dos puertos Ethernet y enviar información simultáneamente en ambos sentidos del anillo.
Cada nodo actúa como un switch, reenviando de un puerto a otro los paquetes que no van dirigidos a él o recogiendo y eliminando de la circulación aquellos que sí van dirigidos a él. En el caso de los paquetes multicast, es el propio remitente quien los elimina del anillo cuando los recibe de vuelta.
Los nodos que no tengan dos interfaces pueden conectarse al anillo a través de una RedBox (Redundancy Box), que se encarga de gestionar las comunicaciones en ambos sentidos del anillo.

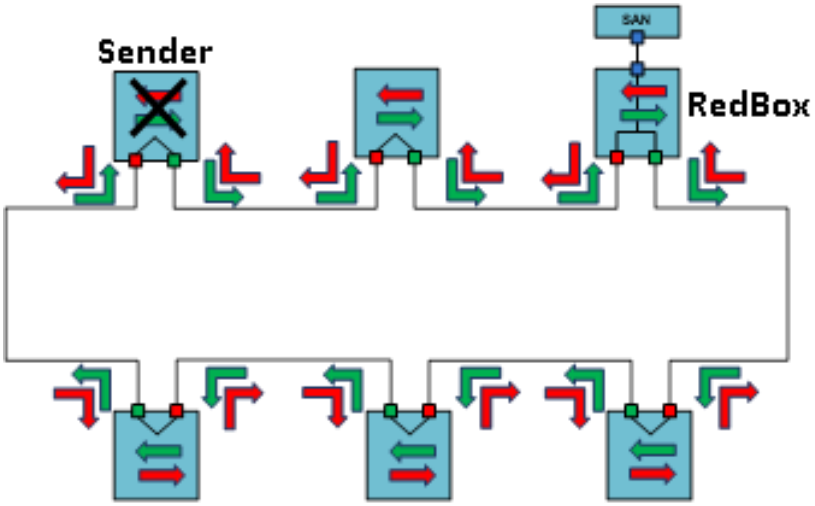


FIGURA 1 – Topología HSR

2.2 PRP

PRP se basa en transmitir la misma información a través de dos redes completamente independientes. En este caso, los nodos también deben tener dos puertos Ethernet o, alternativamente, utilizar una RedBox.

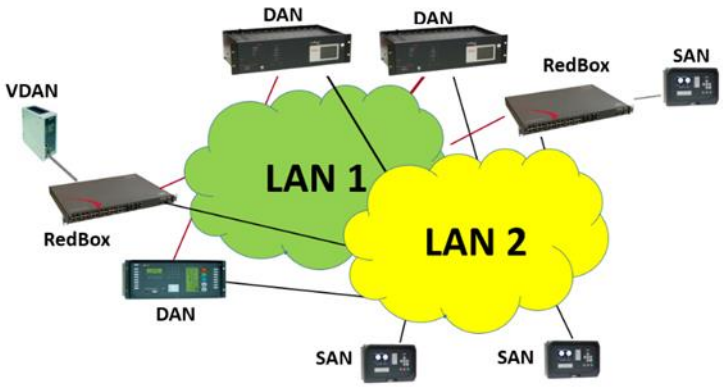


FIGURA 2 – Topología PRP

2.3 Consideraciones

En ambos casos, los nodos incluyen en los paquetes la información necesaria para que los receptores puedan gestionar los duplicados. De esta forma, los sistemas aseguran que, en caso de fallo de una ruta, la información seguirá llegando a la otra sin ningún retraso o interrupción.

Esto abre una nueva posibilidad de redundancia en las comunicaciones entre terminales de teleprotección. En el pasado, se debían utilizar dos interfaces de línea en el mismo equipo, como un E1 sobre SDH y un enlace

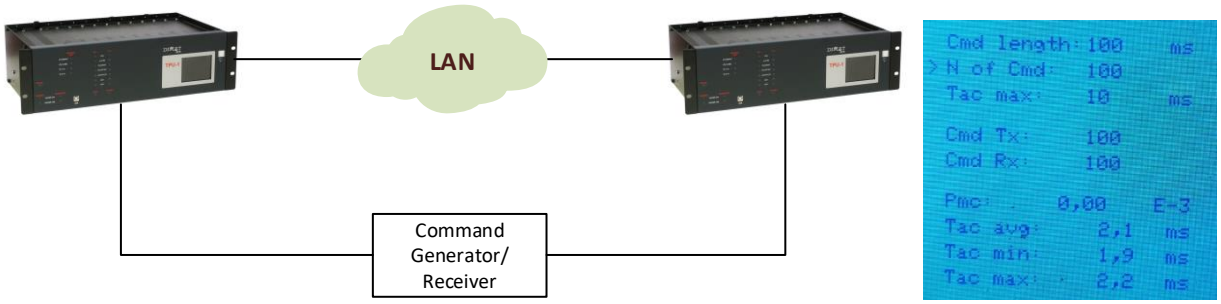
directo sobre línea eléctrica o fibra óptica. En las redes Ethernet, en cambio, es posible utilizar una única interfaz, siempre que tenga dos puertos y sea capaz de manejar uno de estos protocolos de redundancia.
En cualquier caso, el protocolo HSR, aunque ampliamente utilizado en IEC 61850 para comunicaciones entre IED dentro de una misma subestación, no es adecuado para comunicaciones entre terminales de teleprotección ubicados en diferentes subestaciones debido a la topología utilizada, a diferencia del PRP, que sí lo es. Se podrían utilizar como soportes de comunicación dos redes en la misma red MPLS, o incluso en diferentes medios, como una red MPLS y una red aérea 5G.

3.0 TESTS

Se han realizado pruebas de comunicación en laboratorio en diferentes escenarios para verificar la viabilidad del PRP para comunicaciones Ethernet redundantes entre terminales de teleprotección.

3.1 TEST-1 - Comunicación a través de una única LAN

Inicialmente se probó el comportamiento de una comunicación sin redundancia a través de una red Ethernet. Para ello se transmitió un tren de 100 comandos de 100ms de duración con un intervalo de 100ms entre ellos y se probaron los tiempos máximo y mínimo de transmisión y su dispersión.

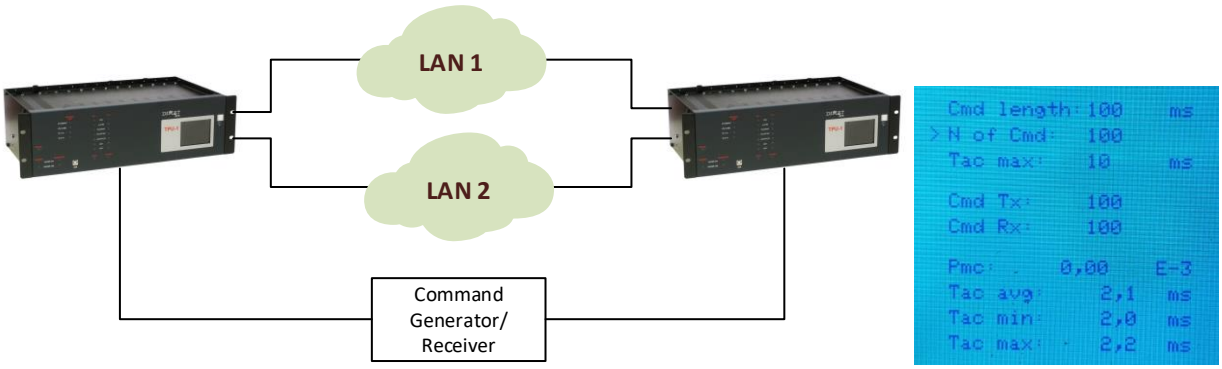


Transmitted commands: 100 Tmax: 2,2ms
Received commands: 100 Tmin: 1,9ms

FIGURA 3 – Test 1 – Comunicación a través de LAN única

3.2 TEST-2 - Comunicación PRP

Se repite la prueba anterior pero activando el PRP en los terminales de teleprotección.

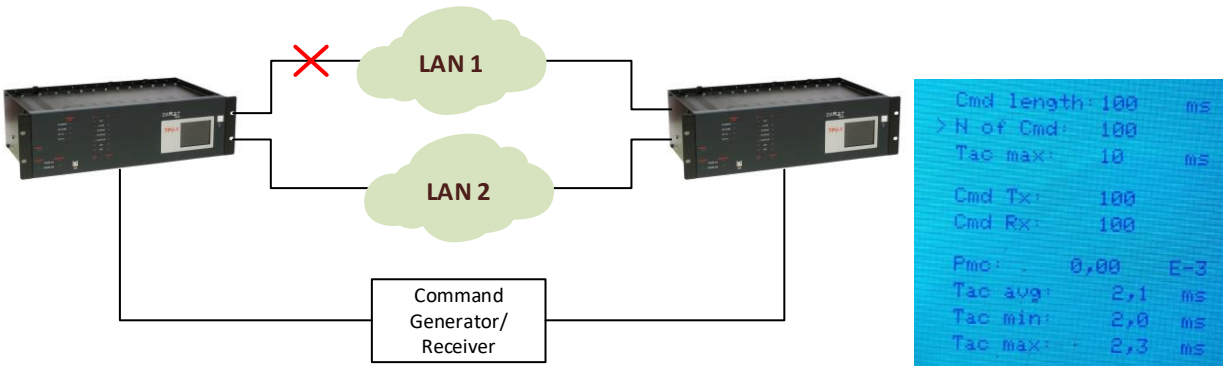


Transmitted commands: 100 Tmax: 2,2ms
Received commands: 100 Tmin: 2,0ms

FIGURA 4 – Test 2 – Comunicación PRP

3.3 TEST-3 - Comunicación PRP con simulación de fallos.

A partir de la configuración del PRP se vuelve a enviar el mismo tren de mando, pero esta vez interrumpiendo uno de los canales durante la prueba y comprobando qué ocurre con los tiempos máximos y mínimos de transmisión y su dispersión.



Transmitted commands: 100 Tmax: 2,3ms
Received commands: 100 Tmin: 2,0ms

FIGURA 5 – Test 3 – Comunicación PRP con simulación de fallos.

4.0 - CONCLUSÃO

Se puede observar que los resultados obtenidos en las diferentes pruebas no muestran variaciones significativas. Aún teniendo en cuenta que han sido obtenidos en laboratorio y que habría que validarlos en instalaciones reales, dan motivos para creer que el PRP sería una técnica de redundancia muy adecuada para las comunicaciones de teleprotección sobre redes Ethernet.
Estos resultados abrirán la posibilidad de utilizar dos redes Ethernet diferentes como MPLS y 5G manteniendo los parámetros de teleprotección.

5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) 9_XIX ERIAC_ZIV_Teleprotección_sobre_nuevos_canales_comunicación - David Gil, ZIV, Spain

(2) Comunicación entre Subestaciones con Redes de Paquetes Conmutados - David Gil, ZIV

6.0 - DADOS BIOGRÁFICOS

David Gil Donate. Ingeniero de Telecomunicaciones por la Universidad Politécnica de Catalunya UPC. España. Trabaja en DIMAT-ZIV desde 1996 como director de proyectos de teleprotecciones y portadoras de alta y media tensión. Actualmente trabaja como responsable de Ingeniería de Aplicación de productos de comunicaciones en zIV.
Autor de artículos y presentaciones en conferencias internacionales como SEAPAC, PACW, SIPSEP, ERIAC, STPC, CIGRE, etc.