

Arquitecturas de red LAN para la automatización de subestaciones, basadas en la norma IEC 61850 (RSTP, PRP y HSR)

A. F. Zurita†

G. G. Rodríguez‡

† CELEC EP - TRANSELECTRIC

‡ CENACE

Resumen— La norma IEC 61850 es la base en la implementación de subestaciones eléctrica automatizadas, permite que los equipos de protección, control y medición de diferentes fabricantes puedan trabajar en una misma red Ethernet. Dependiendo de la disponibilidad requerida para cada subestación, se adoptan esquemas y protocolos de protección en las redes Ethernet, los cuales incrementan la disponibilidad del sistema.

Actualmente para esta protección se utiliza el protocolo RSTP (Rapid Spanning Tree Protocol), sin embargo para subestaciones principales, es necesario el empleo de nuevos esquemas de protección, que disminuyan e incluso eliminen el tiempo de indisponibilidad, en el caso de una falla en algún segmento de la red, esto se consigue a través de los protocolos PRP (Parallel Redundancy Protocol) y HSR (High-availability Seamless Redundancy).

El presente documento incluye una introducción a la norma IEC 61850, el análisis de los protocolos de protección de las redes LAN empleados para la conexión de los IEDs y switches: RSTP, PRP y HSR, y su comparación, concluyendo finalmente con criterios de selección de uno u otro dependiendo del diseño de la subestación a ser construida.

Palabras clave— IEC 61850, RSTP, PRP HSR, Ethernet.

Abstract— The IEC 61850 standard has become the foundation for implementing automated electric substations, and it permit protection, control and measuring equipment from different manufacturers to work in the same Ethernet network. Depending on the availability required for each substation, different protection schemes and protocols are adopted for the Ethernet networks, which increase system availability.

Currently is used the RTSP protocol (Rapid Square Spanning Tree Protocol), however for substations with more bay connection, it is necessary to use new protection schemes that diminish and even eliminate periods of unavailability. In the event of a failure in one segment of the network, the PRP Protocols (Parallel Redundancy Protocol) and the HSR (High-availability Seamless Redundancy) will come into play.

This paper gives an introduction to the IEC 61850 Standard, and an analysis of the protection protocols for LAN networks used for the IED connections and switches: RSTP, PRP and HSR, and their respective comparisons, concluding selection criteria for one or the other depending on the substation design.

Index Terms— IEC 61860, RSTP, PRP HSR, Ethernet.

1. INTRODUCCIÓN

En la actualidad la mayoría de las subestaciones eléctricas son diseñadas mediante sistemas de automatización, que incluyen equipamiento electrónico inteligente (IEDs por sus siglas en inglés) y computadores, interconectados a través de switches y fibra óptica, de tal forma que la administración sea más fácil, y que la intervención del hombre en éstas subestaciones vaya disminuyendo.

La norma IEC 61850 fue introducida en el año 2004 con el fin de ser el marco de referencia para lograr la interoperabilidad de los equipos que forman parte de los sistemas de automatización de las subestaciones eléctricas, y para lo cual adoptó estándares y tecnologías ampliamente utilizados a nivel mundial como TCP/IP y Ethernet, XML, aplicaciones cliente – servidor, nodos lógicos, etc.

En el caso de las redes LAN utilizadas para la conexión de dispositivos de un sistema de automatización la primera versión de la norma no estableció la arquitectura, ni los protocolos que permitan la protección de estas redes. Sin embargo, el desarrollo tecnológico incluyó al protocolo RSTP para este fin.

La versión 2 de la norma publicada en el año 2010 introduce dos protocolos para la protección de redes LAN dentro de los sistemas de automatización, estos son el PRPy HSR. Cada uno de estos protocolos cuenta con sus particularidades que los hacen adecuados a un determinado tipo de subestación, dependiendo de la disponibilidad requerida.

2. LA NORMA IEC 61850

La norma IEC 61850 está conformada por diez partes, las tres primeras definen ideas generales relacionadas con la norma. La parte 4 los requerimientos para la instalación de una subestación utilizando la norma IEC 61850. La parte 5 especifica los parámetros requeridos para la implementación física de la subestación. La parte 6 define el lenguaje XML para la configuración de los IEDs. La 7 detalla los conceptos lógicos y está dividida en cuatro subpartes. En la parte 8 se conceptualiza el mapeo interno de los objeto para la presentación en capas y para los enlaces de capa Ethernet. La parte 9 define el mapeo de los valores muestreados de medición para conexiones punto a punto Ethernet. La última parte detalla las instrucciones para las pruebas de conformidad [1].

2.1. Componentes físicos de la red Ethernet

En términos generales la norma incluye como partes físicas de la red Ethernet: equipo primario, IEDs, switches, computadores y la fibra óptica como medio de transmisión de la información.

2.1.1 DEI, Dispositivo Electrónico Inteligente

Un IED (por sus siglas en inglés) es un equipo instalado en una subestación que recibe y envía datos de control o protecciones desde y hacia una fuente externa, es básicamente un computador, con lógicas digitales específicas, para la ejecución de procesos específicos [2]. Dispone de puertos de entradas y salidas, digitales y analógicas, puertos de comunicación Ethernet, USB, etc. Es además el dispositivo en el cual se almacenan los objetos lógicos.

2.1.2 Switches

Un switch es un equipo que permite la comunicación entre los IEDs y demás dispositivos que forman parte de la red Ethernet, dentro de una subestación.

2.1.3 Fibra óptica

Considerando las excelentes características técnicas como son: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración, en las redes Ethernet de una subestación automatizada se utiliza fibra óptica como el medio de transmisión de la información entre los equipos que la conforman.

2.1.4 Equipo Primario

La información que en una subestación convencional anteriormente era enviada a través de cable de cobre, uno por cada señal, hacia la sala de control de la subestación, ahora puede ser enviada por un par de hilos de fibra óptica. Para esto el equipamiento de patio debe contar con los conversores (internos o externos) que le permitan esta funcionalidad.

2.1.5 Computadores

Para las funciones de monitoreo y configuración de la subestación, así como para el almacenamiento de eventos, se requieren computadores que también forman parte de la red Ethernet. Estos equipos pueden conectarse a la red Ethernet a través de cable de cobre en lugar de fibra óptica.

2.2. Arquitectura de red de la Subestación

La arquitectura de red una subestación está conformada por dos buses (switches de conexión); los equipos de patio forman parte del bus de proceso, los equipos de subestación (IEDs) y computadores forman parte del bus de subestación. En la Fig. 1 se puede observar la arquitectura básica de una subestación:

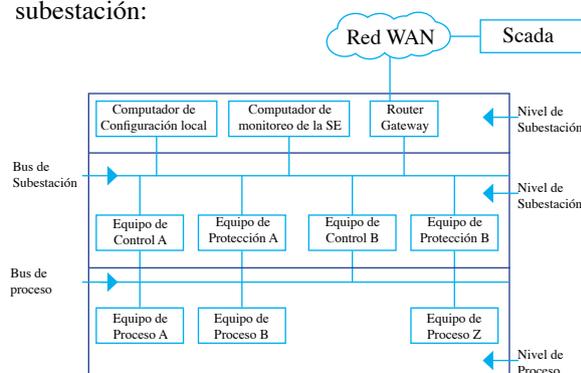


Figura 1: Arquitectura Básica de una subestación

En el esquema presentado se puede observar que la conexión de todos los equipos que conforman el sistema de automatización de la subestación se realiza a través de switches. De tal forma que la información requerida entre cada uno de los equipos puede ser transmitida sin la necesidad de conexión independiente por cada señal.

También se distinguen tres niveles principales, así el nivel de proceso que corresponde al equipo primario instalado en el patio de la subestación, el nivel de bahía está relacionado con los IEDs ubicados generalmente en las casetas de patio, y el nivel de subestación correspondiente a los computadores ubicados en las salas de control.

Las interacciones entre los equipos que forman parte del sistema de automatización principalmente se dividen en tres categorías:

1. Configuración y obtención de datos
2. Monitoreo y reporte de datos
3. Registro de eventos

Para poder realizar estas interacciones la norma define una estructura de comunicación compleja que incluye cinco perfiles de comunicación, los cuales se detallan a continuación:

4. ACSI (Abstract Communication Service Interface): comunicación cliente – servidor.
5. GOOSE (Generic Object Oriented Substation Event): comunicación rápida dentro del bus de la subestación.
6. GSSE (Generic Substation Status Event): provee una vía para el intercambio del estatus del nivel de subestación.
7. SMV (Sampled Measured Value Multicast): provee una vía para el intercambio de información en el bus de proceso.
8. Señales de sincronismo

2.3. Estructura de Intercambio de Información

Físicamente cada IED tiene una conexión hacia la red LAN de la subestación, lógicamente existe intercambio de información desde cada uno de los nodos lógicos que se encuentran en los IEDs. Un nodo lógico es la parte más pequeña de una función que intercambia información entre IEDs, definiéndose en él sus datos y atributos.

Cada función depende de uno o varios equipos físicos, los cuales contienen los nodos lógicos. Los nodos lógicos se encuentran enlazados por conexiones lógicas. La Fig. 2 presenta la relación entre estos conceptos.

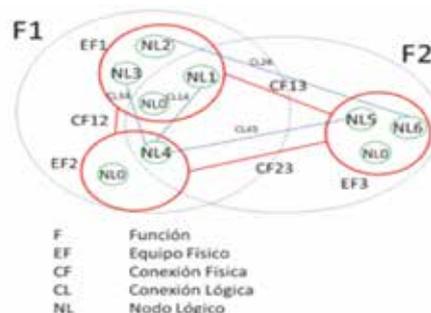


Figura 2. Estructura de intercambio de información

Un dispositivo físico puede contener varios nodos lógicos, y cada nodo lógico puede contener a su vez varios Objetos de Datos. Cada Objeto de Datos está conformado por atributos de datos, y por los componentes de los atributos de datos. La Figura 3 muestra lo descrito anteriormente.

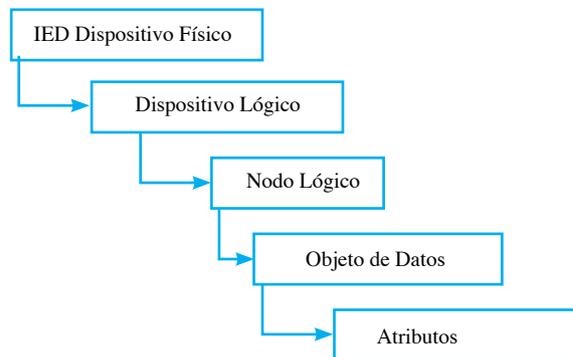


Figura 3: Estructura de conformación de datos

3. REQUERIMIENTOS DE COMUNICACIONES

Los sistemas de automatización de las subestaciones tienen dos características indispensables propias de sistemas de tiempo real: a) la sincronización de tiempo y b) la redundancia del sistema.

Los requerimientos para la sincronización de tiempo quedan cubiertos con el uso del protocolo SNTP (simple network time protocol) con estrictas exigencias establecidas en el estándar IEEE 1588 [2]; y en relación a la redundancia del sistema la segunda edición de la norma IEC 61850 incluye dos protocolos que cumplen en su totalidad con los requerimientos y que son aplicables

a subestaciones de cualquier tamaño y topología: PRP (Parallel Redundancy Protocol) y HSR (High-availability Seamless Redundancy), estos protocolos proveen un tiempo de cero = no interrupción en la conmutación por falla de enlaces o dispositivos de la red.

3.1. Redundancia

En una subestación, la comunicación de la red Ethernet industrial de datos y sus componentes es de vital importancia para la operación de todos los elementos, demandando requerimientos exigentes y distintos de tiempo para el nivel de supervisión del bus de la subestación y el bus de proceso, los mismos que definen los requerimientos de redundancia en la topología de red a implementar. El funcionamiento de la redundancia en toda la red debe ser chequeado periódicamente desde un nodo de operación de la red con frecuencias menores a 1 minuto al igual que los errores de configuración.

3.1.1 Métodos de Redundancia

Redundancia Dinámica (standby o serial): Esta redundancia no participa de forma activa en el control, sino una conmutación lógica es quien decide insertar la redundancia y ponerla en funcionamiento. La Tabla 1 muestra las principales características de éste método.

Redundancia Estática (activa o paralela): Esta redundancia participa de forma activa en el control, la red escoge el elemento operativo en que confiar. La Tabla 1 muestra las principales características de este método [3].

Tabla 1: Métodos de Redundancia

<i>Métodos de Redundancia</i>	
<i>Redundancia Dinámica</i>	<i>Redundancia Estática</i>
<i>Balancea redundancia y carga</i>	<i>Todos los elementos forman parte de la redundancia. Provee conmutación sin interrupciones</i>
<i>Implementa una redundancia parcial</i>	<i>Prueba continuamente la redundancia incrementando la detección de fallas</i>
<i>Reduce la tasa de fallas de redundancia</i>	<i>Provee protección a fallas</i>
<i>Reduce el modo común de errores</i>	
<i>La conmutación (switchover) toma tiempo</i>	<i>La duplicación de elementos incrementa los costos</i>

3.2. Topología de red de Alta Disponibilidad

Parámetros como la confiabilidad y disponibilidad son determinantes en la definición de una red de alta redundancia y desempeño. La disponibilidad es la fracción de tiempo de operación o estado "activo" de un sistema, se expresa en porcentaje que representa el "ciclo de trabajo" o capacidad de operación del sistema, por ejemplo, 99,99%.

La disponibilidad de un sistema se incrementa con la implementación de esquemas de redundancia, se consideran la inserción automática de redundancia ante fallas (sistemas tolerantes a fallas) y la reinserción automática después del restablecimiento, siendo el retardo de conmutación para el restablecimiento el factor más limitante en los sistemas tolerantes a fallas.

3.3. Requerimientos de Tiempo en una SE

En una red redundante el parámetro más importante es el tiempo de restablecimiento requerido para normalizar la operación después de un evento de falla, en este sentido los protocolos PRP y HSR garantizan un tiempo "cero = no interrupción" para este restablecimiento

El tiempo en el cual la subestación tolera una salida del sistema de automatización se denomina "tiempo de gracia", para instalaciones eléctricas el tiempo de gracia es de 5 mseg, los tiempos de restablecimiento de la red deben ser menores a este tiempo de gracia. La Tabla 2 resume los tiempos de restablecimiento dados por el Comité Técnico IEC 57 (TC57) – grupo de trabajo 10 (WG10).

Tabla 2: Requerimientos de Tiempos de Restablecimiento

<i>Comunicación entre Elementos</i>	<i>Nivel de comunicación</i>	<i>Tiempo de restablecimiento</i>
<i>SCADA a IED cliente - servidor</i>	<i>Bus de subestación</i>	<i>100 ms</i>
<i>IED a IED interlocking</i>	<i>Bus de subestación</i>	<i>4 ms</i>
<i>IED a IED bloqueo reverso</i>	<i>Bus de subestación</i>	<i>4 ms</i>
<i>bus bar protection</i>	<i>Bus de subestación</i>	<i>0 ms</i>
<i>valores muestreados</i>	<i>Bus de proceso</i>	<i>0 ms</i>

4. PROTOCOLOS DE COMUNICACIONES

4.1. RSTP (Rapid Spanning Tree Protocol)

4.1.1 Arquitectura

El protocolo Rapid Spanning Tree se usa en topologías donde se cuenta con enlaces redundantes, y su funcionamiento principal es evitar los lazos dentro de la red. Un lazo dentro de una red Ethernet se presenta cuando se tiene una doble conexión entre dos switches, la presencia de un lazo dentro de la red hace que el tráfico no tenga salida y se vaya incrementando rápidamente hasta saturar y bloquear los switches y demás equipos que conforman la red, para evitar este fenómeno el protocolo RTP activa solo una de las dos conexiones. La topología en la que puede ser empleado RSTP es estrella o anillo.

4.1.2 Modo de Operación

El Protocol Spanning Tree maneja varios conceptos que le permiten determinar el camino para enviar la información y el camino de respaldo. Cuando se cuenta con un par de conexiones la decisión es simple, sin embargo, cuando el número de switches y enlaces aumenta la decisión del camino principal y redundante requiere realizar cálculos y tomar decisiones las cuales se manejan a través del protocolo. El análisis que realizan los switches para la definición de los caminos de transmisión requiere de algunos segundos en el caso del protocolo STP, el protocolo RSTP presenta mejoras al STP de tal forma que el tiempo de definición o estabilización se reduzca.

Cuando uno de los switches de la red falla, se requiere detectar la falla y reconfigurar los caminos de configuración. Esta función se realiza enviando mensajes a los equipos que conforman la red para detectar cual es el enlace con problemas y realiza la reconfiguración. El tiempo de establecimiento para RSTP puede estar en el orden de 5 ms por cada switch Ethernet que conforma la red, dependiendo del número de equipos con que cuente la red esta recuperación puede tomar varios segundos. El detalle de la operación del protocolo se encuentra en [4].

4.2. PRP (Parallel Redundancy Protocol)

4.2.1 Arquitectura

Este protocolo establece un nivel de redundancia basado en una topología compuesta por dos redes de área local (LANs) independientes y paralelas;

estas dos redes están separadas a fin de asegurar independencia ante fallas pudiendo tener topologías diferentes y no solo de anillo, ambas redes operan en paralelo como se ejemplifica en la Fig. 4.

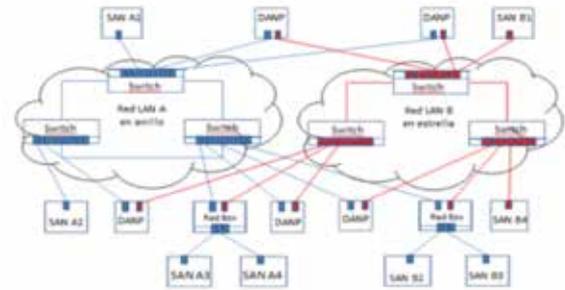


Figura 4: Arquitectura de Red Redundante PRP

La red PRP se compone de nodos DANP (doubly attached node with PRP) y SAN (simple attached node); los nodos DANP se conectan a las dos redes LAN independientes operando de forma paralela por éstas, es decir que los equipos requieren de dos puertos Ethernet para el uso del protocolo PRP; en tanto que los nodos SAN (no-PRP) o nodos simples de conexión (ejemplo: ordenadores, impresoras, etc.) se conectan a una de las redes teniendo comunicación únicamente con los dispositivos DANP o SAN de esa misma red. En caso de requerirse redundancia para los nodos SAN se debe utilizar un equipo de adaptación denominado RedBox que gestiona los protocolos redundantes. La Fig. 5 muestra el esquema de operación de este protocolo.

4.2.2 Modo de Operación

Una red PRP establece dos caminos activos independientes para la conexión entre dispositivos [5]. En una red PRP los nodos DANP usan los dos puertos para el envío simultáneo de las tramas Ethernet por ambas redes usando retardos de transmisión diferentes para cada una de las redes, e incluyendo la información necesaria para asegurar el adecuado tratamiento de las mismas (número de secuencia, identificadores de redundancia, etc.). En condiciones libres de errores, los nodos destino toman la primera trama recibida y descartan los duplicados, en caso de recibir una sola trama se determina la ocurrencia de una falla en una de las redes, manteniéndose la comunicación por la segunda red.

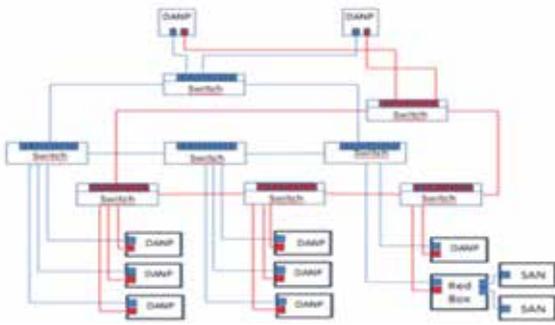


Figura 5: Modo de Operación PRP

El PRP garantiza tiempos de “cero=no interrupción” en el restablecimiento de comunicaciones de la red ante fallas y un chequeo continuo de la redundancia de la red que disminuye la ocurrencia de fallas, basándose en el uso de los nodos dobles PRP (DANP) conectados a ambas redes para garantizar el nivel de disponibilidad requerido. Los nodos chequean y detectan duplicaciones con secuencias numéricas que se introducen en las tramas después del paquete de información “payload”, esto permite una transparencia total de nodos PRP y NO PRP. El protocolo PRP puede ser ejecutado de forma completa vía software. La falla de nodos no está cubierta por el PRP, pero los nodos duplicados pueden ser conectados vía red PRP.

EL PRP es implementado en los dispositivos terminales, por lo cual es posible utilizar switches de red convencionales que no requieren conocer de este protocolo.

4.3. HSR (High-availability Seamless Redundancy)

4.3.1 Arquitectura

El protocolo HSR es producto del desarrollo de PRP, sin embargo las funciones de HSR principalmente son las de un protocolo que crea medios redundantes, mientras que PRP crea redundancia de la red. HSR a diferencia del PRP está básicamente diseñado para el uso de topologías de anillo, en ambos protocolos se utilizan dos puertos de red, pero HSR incorpora el nodo DANH (Doubly Attached Node for HSR) que conecta sus dos interfaces a una misma red conformando una topología de anillo como se muestra en la Fig. 6

El protocolo HSR aplica los principios de operación paralela del PRP sobre un anillo simple, tratando las dos direcciones de cada dispositivo como dos redes LAN virtuales, esto permite una reducción significativa en costos de hardware ya que

no requiere de dos switches, sin embargo todos los nodos del anillo deben ser nodos de conmutación que dispongan de dos puertos integrando un elemento de conmutación preferentemente de hardware.

Es posible establecer enlaces entre dos anillos HSR con el uso de elementos de conexión denominados QuadBoxes, estos permiten la conexión entre dos HSR sin un solo punto de falla, como muestra la Fig.6

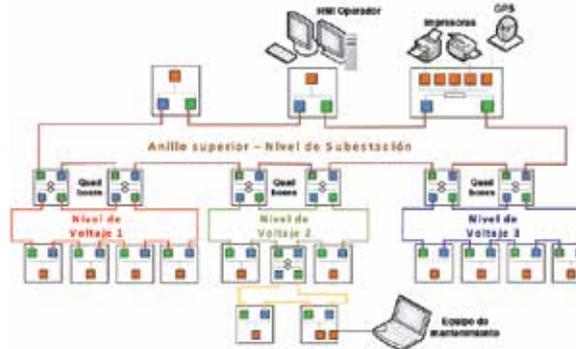


Figura 6: Arquitectura red redundante HSR

4.3.1. Modo de Operación

Para cada trama enviada, un nodo DANH envía dos tramas una sobre cada puerto, ambas tramas circulan en direcciones opuestas sobre el anillo y cada nodo reenvía las tramas que recibe desde uno de los puertos hacia el otro. Cuando el nodo originario recibe una trama enviada por él mismo la descarta para evitar lazos, es así que no es necesario un protocolo especial de anillo, como se muestra en la Fig. 7.



Leyenda Figura 7

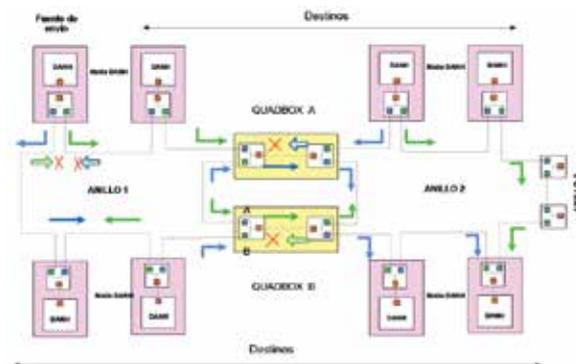


Figura 7: Modo de Operación HSR

Para detectar duplicaciones las tramas Ethernet incluyen una secuencia numérica incrementada por la fuente de cada trama enviada, contrariamente al PRP, la secuencia numérica se inserta en la cabecera y no después del paquete de información “payload”, así el elemento de conmutación puede reconocer la duplicación antes de recibir completamente una trama, de esta manera son posibles operaciones de “cut-through” o reenvío sin necesidad de recepción de una trama completa en tiempos menores a 5 useg por nodo.

Al usar un anillo simple el tráfico de bus casi se duplica, pero el promedio de tiempo de propagación se reduce permitiendo al anillo soportar un número similar de dispositivos que un anillo redundante. Adicionalmente nodos simples (SAN) como laptops e impresoras solo pueden conectarse al anillo usando una caja de redundancia que les permite actuar como un elemento del anillo.

En cuanto a tiempos de conmutación, HSR se comporta como PRP: enviando tramas desde ambos puertos de una conexión HSR, en el caso de ocurrir una falla una trama continuará siendo transmitida a través de cualquier camino disponible de la red, esto significa que la redundancia funciona con tiempo de conmutación cero y, a diferencia de PRP, no requiere dos redes paralelas. Se debe considerar que la transmisión duplicada de tramas por ambas direcciones implica que sólo el 50% del ancho de banda de la red está efectivamente disponible para el tráfico de datos.

5. COMPARACIÓN DE PROTOCOLOS RSTP, PRP Y HSR

La elección del protocolo de protección utilizado en de la red Ethernet depende de varios factores entre los principales: la disponibilidad establecida para la subestación, el presupuesto, la escalabilidad a futuro, entre otras. En la Tabla 3 se presenta una comparación de varias características que deben ser analizadas para la elección de uno y otro protocolo de protección.

De esta comparación se puede destacar que los protocolos HSR y PRP permiten contar con un mayor nivel de disponibilidad, y no presentan tiempo de recuperación ante la presencia de alguna falla en un enlace. La habilitación del protocolo PRP es la de mayor costo. Y el RSTP es el de más difusión en el mercado. El crecimiento de la red es más fácil de implementar cuando se utilizan protocolos PRP y HSR, así también el protocolo RSTP no requiere de una fuente de sincronismo, a diferencia de los otros dos protocolos. Por último se debe notar que

el protocolo PRP cuenta con el 100% del ancho de banda disponible en cada enlace a diferencia de los otros dos protocolos.

5.1. Ventajas RSTP:

- RSTP utiliza una red simple para la conexión de nodos.
- Tolera la falla de cualquier componente simple de red (con un tiempo relativamente corto de indisponibilidad de la red)
- No depende de protocolos de capa superior
- Esta altamente difundido en el mercado, existen varios fabricantes que utilizan este protocolo en sus equipos de red
- Es un protocolo probado en subestaciones a nivel mundial
- Implementación económica.

5.2. Desventajas RSTP:

- Ante fallas en la red la reconfiguración puede tomar varios segundos; en casos extremos.
- No cumple con los niveles de disponibilidad requeridos en las subestaciones, durante la reconfiguración por falla o inicio de equipos.
- Tiene un número máximo de equipos que pueden formar parte de la red

5.3. Ventajas de PRP

- PRP permite la conmutación sin interrupciones (tiempos cero) y sin pérdida de tramas; lo cual lo hace adecuado para la mayoría de sistemas de tiempo crítico.
- Puede usarse en variedad de topologías de red: anillo, estrella, etc.
- Cumple con todos los requisitos de automatización de subestaciones de acuerdo a la norma IEC 61850.
- Tolera fallas de cualquier componente simple de red.
- No depende de protocolos de capa superior.
- Es compatible con RSTP
- Permite el uso de nodos (SAN) que no están equipados para redundancia, que pueden operar en la misma red.
- Puede usarse fuera de la plataforma de componentes de red: herramientas, controladores, switches y enlaces.
- Soporta precisión para la sincronización de tiempo de acuerdo con la IEEE 1588.
- Es un protocolo probado para subestaciones de alta tensión.
- Es transparente para la aplicación.

- PRP reduce la tasa de pérdidas durante su operación normal.
- Usa métodos de chequeo periódico de nodos, que le permite identificar los nodos que participan y no en el protocolo

5.4. Desventajas de PRP

- Duplicación de costos en la red
- Los nodos simples (SAN) de una red LAN no pueden comunicarse directamente con nodos SAN de otra LAN.
- El tamaño de trama debe ser limitado para prevenir que se conviertan en tramas más largas que las máximas establecidas en IEEE 802.3

5.5. Ventajas de HSR

- HSR usa una red simple para la conexión de nodos.
- HSR es un protocolo transparente adecuado para aplicaciones críticas, costos eficientes.
- HSR permite la conmutación sin interrupciones con tiempos de conmutación cero y sin pérdida de tramas; lo cual lo hace adecuado para la mayoría de sistemas de tiempo crítico.
- Cumple con todos los requisitos de automatización de subestaciones de acuerdo a la norma IEC 61850.
- Tolera la falla de cualquier componente simple de red.
- No depende de protocolos de capa superior.
- Es compatible con RSTP y PRP
- Permite el uso de nodos (SAN) que no están equipados para redundancia, que pueden operar en la misma red.
- Soporta precisión para la sincronización de tiempo de acuerdo con la IEEE 1588.
- Es un protocolo probado para subestaciones de alta tensión.
- HSR chequea la presencia de nodos usando supervisión periódica de tramas que también identifican los nodos que participan y no en el protocolo

5.6. Desventajas de HSR

- Solo soporta topología de red en anillo, y anillos de anillos.
- Dispositivos doblemente conectados requieren un desarrollo inicial con costo (hardware)
- Para la conexión de nodos simples, SAN, se debe usar un dispositivo de conexión adicional: “RedBoxes”

Tabla 3: Comparación de protocolos

<i>Protocolos de protección red Ethernet</i>			
<i>Característica</i>	<i>RSTP</i>	<i>PRP</i>	<i>HSR</i>
<i>Tiempo de restablecimiento ante fallas</i>	<i>5 ms por switch</i>	<i>0 ms</i>	<i>0 ms</i>
<i>Nivel de disponibilidad de la red</i>	<i>Medio</i>	<i>Alto</i>	<i>Alto</i>
<i>Ancho de banda efectivo en todos los enlaces</i>	<i>>= 50%</i>	<i>100%</i>	<i>50%</i>
<i>Posicionamiento en la industria</i>	<i>Alto</i>	<i>Medio</i>	<i>Bajo</i>
<i>Costo</i>	<i>Bajo</i>	<i>Alto</i>	<i>Medio</i>
<i>Escalabilidad</i>	<i>Medio</i>	<i>Alto</i>	<i>Alto</i>
<i>Sincronización</i>	<i>N/A</i>	<i>Requiere</i>	<i>Requiere</i>

6. CONCLUSIONES Y RECOMENDACIONES

La norma IEC 61850 demanda ampliar los conceptos eléctricos utilizados hasta ahora para la puesta en marcha de una subestación, integrando conceptos que en la actualidad se utilizan en gran medida y que están relacionados con las ramas de telecomunicaciones, redes e informática.

Los protocolos PRP y HSR permiten la conmutación sin interrupción ante la falla de un elemento simple de la red, esto permite que la disponibilidad global de la subestación se incremente.

La implementación del protocolo PRP requiere la habilitación de una red totalmente redundante, convirtiendo esta solución en una opción costosa, y resultando HSR más conveniente.

La elección de uno u otro protocolo de protección depende de varios factores, entre estos la disponibilidad requerida para la subestación, el presupuesto, existencia de equipos que cumplan los protocolos, etc., no es necesario que todas las subestaciones manejen el mismo protocolo de protección.

Los esquemas PRP y HSR representan un reto para la sincronización de tiempo debido a que los retardos sobre las dos redes redundantes son diferentes y demandan la mejora de la robustez y precisión del reloj del sistema.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Liang Y. & Campbell R. (2009), “Understanding and Simulating the IEC 61850 Standard”, Department of Computer Science University of Illinois at Urbana-Champaign, pp 1-5.
- [2] McDonald, J. “Substation automation. IED integration and availability of information”.

(2003), Power and Energy Magazine, pp 22–31.

- [3] Kirmann H. (2012), “Highly Available Automation Networks Standard Redundancy Methods” ABB Switzerland Ltd, Corporate Research.
 - [4] Oñate E. “Rapid Spanning Tree Protocol Shortest Path, extension a RSTP” Universidad Técnica Federico Santa María, pp. 1-6.
 - [5] Kirmann H. (2012), “Seamless Redundancy”, ABB Switzerland Ltd, Corporate Research, pp. 55-61.
-



Ana Francisca Zurita Zaldumbide.- Nació en Quito, Ecuador en 1980. Recibió su título de Ingeniera en Electrónica y Telecomunicaciones de la Escuela Politécnica Nacional en el año 2004. Es egresada de la Maestría en Redes y Networking

de la Universidad Católica de Quito, y su campo de investigación se encuentra relacionado con temas de telecomunicaciones para el sector eléctrico.



Gioconda Guanacaury Rodríguez Pazmiño.- Nació en Quito, Ecuador en 1974. Recibió su título de Ingeniera en Telecomunicaciones del Instituto Superior Politécnico José Antonio Echeverría, de la ciudad de La Habana, Cuba en el año 1998, y su campo de investigación se

encuentra relacionado con temas de telecomunicaciones para el sector eléctrico.