UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

APLICACIÓN DEL ESTÁNDAR IEC 61850 EN LOS SISTEMAS DE PROTECCIONES Y MEDICIONES ELÉCTRICAS EN SUBESTACIONES DE ALTA TENSIÓN

PRESENTADO POR:

JOSÉ JOEL BERNAL CRUZ

NILSON EDUARDO HERRERA RUÍZ

JORGE DONACIANO MONTEAGUDO GUEVARA

PARA OPTAR AL TÍTULO DE:

INGENIERO ELECTRICISTA

CIUDAD UNIVERSITARIA, AGOSTO 2017

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. ROGER ARMANDO ARIAS ALVARADO

SECRETARIA GENERAL:

MSC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO:

ING. FRANCISCO ANTONIO ALARCÓN SANDOVAL

SECRETARIO:

ING. JULIO ALBERTO PORTILLO

ESCUELA DE INGENIERÍA ELÉCTRICA

DIRECTOR:

ING. ARMANDO MARTÍNEZ CALDERÓN

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO ELECTRICISTA

Título:

APLICACIÓN DEL ESTÁNDAR IEC 61850 EN LOS SISTEMAS DE PROTECCIONES Y MEDICIONES ELÉCTRICAS EN SUBESTACIONES DE ALTA TENSIÓN

Presentado por:

JOSÉ JOEL BERNAL CRUZ

NILSON EDUARDO HERRERA RUÍZ

JORGE DONACIANO MONTEAGUDO GUEVARA

Trabajo de Graduación Aprobado por:

Docente Asesor:

ING. HUGO MIGUEL COLATO RODRÍGUEZ

SAN SALVADOR, AGOSTO DE 2017

Trabajo de Graduación Aprobado por:

Docente Asesor:

ING. HUGO MIGUEL COLATO RODRÍGUEZ

AGRADECIMIENTOS.

EN PRIMER LUGAR, AGRADEZCO A DIOS TODOPODEROSO.

Por haberme acompañado en toda mi carrera y no abandonarme nunca en los momentos más difícil fue mi fortaleza para continuar, gracias por llenar de vida a toda mi familia y que todos puedan ver este logro.

A MI MADRE.

Leticia Cruz por creer en mí, dándome su apoyo incondicional sin dudar ni un segundo que lograría llegar hasta donde estoy mil gracias madre por enseñarme que en la vida se lucha hasta mas no poder para lograr las metas, no hay manera como pagar ese enorme apoyo que me diste, nada más puedo llenarte de orgullo al verme triunfar en mi carrera.

A MI PADRE.

Norman de Jesús Sorto por siempre apoyarme y demostrarme el gran amor y aprecio que me tienes, sé que estarás más que orgulloso al ver triunfar tu hijo aquel niño que siempre tuvo miedo de enfrentar al mundo y que ahora gracias a ti ha llegado muy lejos mil gracias mi viejito…

A MIS HERMANOS.

Por ser parte importante de mi vida y que con sus consejos me han ayudado a afrontar los retos que se me han presentado

A MI AMADA MAYRA DIAZ

Durante todo este tiempo me ha demostrado su amor y su fe en que puedo llegar y lograr mis metas, gracias por ser ese apoyo que tanto necesite para seguir adelante, gracias por nunca abandonarme en los momentos tan difíciles que he vivido en estos últimos años, gracias por ser la mejor novia del mundo.

A MIS COMPAÑEROS DE TESIS.

Jorge Monteagudo y Nilson Herrera, porque cada una con sus valiosas aportaciones hicieron posible este proyecto de tesis y así haber logrado culminar nuestro gran objetivo con perseverancia y dedicación.

A MI DOCENTE ASESOR.

Ingeniero Hugo Colato, por creer en mis compañeras y en mí; por toda la colaboración, confianza, apoyo y dedicación que nos brindó durante el proceso de nuestra tesis y en el transcurso de mi carrera.

Finalmente, gracias a todas las personas que de manera directa o indirecta nos brindaron su apoyo en la realización de este proyecto.

¡¡¡GRACIAS!!!

JOSÉ JOEL BERNAL CRUZ.

AGRADECIMIENTOS

A Dios todo todopoderoso por haberme permitido culminar la carrera y brindarme fuerzas para no desistir en los momentos más difíciles y concluir mi carrera.

Gracias a mis Padres, por la confianza y el apoyo brindado en todo momento, por los valores y principios que me han inculcado, sin duda alguna en el trayecto de mi vida me han demostrados su amor incondicional, corrigiendo mis faltas y celebrando mis triunfos.

A mis hermanos por todos sus consejos que me han ayudado durante todos estos años de estudio, por haber creído en mí y brindarme su apoyo de forma incondicional.

A mi asesor, Ing. Hugo Miguel Colato por darme su apoyo y asesoría para poder culminar este trabajo de graduación. Así también, a todos los docentes de la EIE-FIA que contribuyeron a mi formación profesional.

A todos mis compañeros que estuvieron a lo largo de mi formación académica, a todos ellos muchas gracias. Así como también, trabajadores administrativos y de la EIE, que con su vital colaboración y su apoyo brindado durante la realización de mi carrera.

DIOS LOS BENDIGA
JORGE DONACIANO MONTEAGUDO GUEVARA

AGRADECIMIENTOS

A DIOS TODO PODEROSO

Por darme las fuerzas y la convicción para alcanzar mis sueños y protegerme siempre.

A MI FAMILIA

Por formar parte de un núcleo indispensable del cual surgen mis raíces para darle sentido a la vida.

A LA UES

Por la formación, disciplina y la inculcación de valores.

A LA FACULTAD DE INGENIERIA

Por los conocimientos adquiridos y la oportunidad de conocer profesores y amigos

¡¡¡GRACIAS!!!

NILSON EDUARDO HERRERA RUIZ.

CONTENIDO

Contenido de tablas.

Contenido de figuras.

Glosario.

BAHIA	Campo en él se encuentra el conjunto de equipos necesarios para conectar un circuito al sistema.
CID	Configured IED Description
CT	CT transformador de corriente de media, en los que en condiciones normales de operación de corriente secundaria es proporcional a la primaria, pero ligeramente desfasada, lo cual se busca medir fielmente
Dispositivo Físico	Es quien se conecta físicamente con la red IP puede contener uno o varios dispositivos lógicos y puede trabajar tanto como servidor, proxy o concentrador.
Dispositivos Lógicos	Está compuesto por un conjunto de nodos lógicos y servicios que están relacionados. Se asocian directamente con un dispositivo real. Por ejemplo, un interruptor, un seccionador, o una protección, etc. O sea, a partir de este objeto es que se puede modelar cualquier equipo de la subestación.
DNP 3.0	Distributed Network Protocol (Protocolo de red distribuido).
Equipo de patio	equipo eléctrico que se encuentra en el campo o bahía de una subestación
HMI	Human –Machine Interface.
ICD	IED Capability Description.
ICCP	Inter Control Center Protocol (Protocolo para la comunicación entre Centros de Control).
IEC	La comisión internacional de electrónica es la organización líder en el mundo en preparar y publicar normas de tecnología eléctrica y electrónica.

IED	(Intelligent Electronic Device), Describe la configuración de los IEDs, Access Points, dispositivos lógicos y nodos lógicos
Interruptor	Los interruptores o disyuntores son dispositivos mecánicos de interrupción capaces de conducir e interrumpir corrientes tanto condiciones normales como de cortocircuito.
LAN	Una red de área local es la interconexión de una o varios ordenadores y periféricos.
Lenguaje SCL	Lenguaje de programación de IEDs que usan el protocolo IEC 61850.
MMS	Estándar desarrollado específicamente para aplicaciones industriales que sirve para el intercambio de datos en ambientes de producción.
MODBUS	Protocolo de comunicaciones basado en la arquitectura Maestro/esclavo.
Nivel de Bahía	Aquí es donde están instalados los IEDs a los equipos de protección y medición.
Nivel de Proceso	Generalmente estos buses se crean en una red de anillo. Debido a la confiabilidad que debe tener el BUS es recomendable utilizar dos anillos para duplicar la confiabilidad y utilizar switches confiables
Nodo	En informática un nodo es un punto de intersección o unión entre varios elementos que confluyen en el mismo lugar
Nodos Lógicos	Es un conjunto de datos y servicios que se relacionan con una función específica de la subestación. La norma define

	los LNs para las distintas funciones de control, protección, medición, etc. Lo que se define es la interface externa. La norma lo que no define es el funcionamiento interno de los LN.
Protecciones	Evitan la destrucción de dispositivos interconectados.
Protocolo	Método establecido para el intercambio de datos entre equipos electrónicos
RTU,	Remote Terminal Unit (Unidad terminal remota).
SCADA	Supervisory Control And Data Acquisition (supervisión, control y adquisición de data).
SAS	Sistema de automatización de subestaciones.
SCD	Substation Configuration Description
Sistema Eléctrico de Potencia	Es un sistema de suministro eléctrico cuyos niveles de tensión dependen de cada país.
SSD	System Specification Description
PT	Transformador de tensión en el que en condiciones normales de operación la tensión secundaria es proporcional a la primaria, pero ligeramente desfasada, lo cual se busca medir fielmente
WAN	Una red de área amplia es un tipo de red de ordenadores capaz de cubrir distancias muy grandes de comunicación

Introducción.

En El Salvador los sistemas de protección y medición están basados en sistema SCADA implementados bajo el estándar IEC 101/IEC 104, el cual no permite la interoperabilidad de los equipos entre diferentes fabricantes. Para superar dicha limitación los ingenieros e investigadores en el campo de calidad de energía han desarrollado el estándar IEC – 61850, que permite la interoperabilidad en los diferentes niveles de la subestación eléctrica.
El presente trabajo está constituido por cuatros capitulo como se describe a continuación:

En el Capítulo uno se describe los tremas de líneas de transmisión, donde se menciona los niveles de tensión de operación del sistema eléctrico, equipos de protección, medición y comunicación de los parámetros eléctricos y anormales dentro de la subestación, conceptos generales del Estándar IEC – 61850, como la arquitectura de la subestación e interfaces lógicas la cuales permite la asignación de funciones para la comunicación, los nodos lógicos y sus funciones para protección y control.

En capitulo dos se describen, las diez mejores prácticas para el diseño de un sistema comunicación en la subestación bajo el Estándar IEC– 61850, como la segmentación de la red operativa la cual puede ser física o virtual para evitar la saturación de información en el sistema, agregación de equipos de comunicación de serie a Ethernet, la importancia de la alimentación a través de Ethernet simplificando la instalación y el ahorro de espacios, la sincronización del tiempo donde existen diferente tipos de protocolo para sincronizar los equipos de comunicación como son el NTP, IEEE 1588, selección de equipos con parámetros para el entorno para soportar los riesgos ambientales según la IEC – 618650- 3 e IEEE 1613, capas de seguridad esta nos permitirán proteger la información de diferentes ataque de la red.

En el capítulo 3 se propone un laboratorio de interoperabilidad basado en el Estándar IEC – 61850 donde tratan los requisitos físicos y ambientales del local, como también de los equipos, el hardware y software necesarios para el laboratorio y las pruebas de conformidad.

En el capítulo 4 se realiza un presupuesto de cuanto se invertirá para la implementación de dicho laboratorio.

Justificación.

Dado que los sectores de generación y distribución de energía eléctrica son considerados sectores que mueven el desarrollo en nuestro país, aún no se encuentran bajo la norma IEC61850 la cual en muchos otros países de latino américa viene siendo requerido por los múltiples beneficios y la creciente necesidad de contar con un sistema eléctrico fiable, eficiente en medición, protección en tiempo real, evitar fallas y dejar a sectores industriales sin el suministro eléctrico.

Es por esta razón que se hace necesario identificar al instante las fallas causadas en la red y corregirlas.

La norma IEC61850 viene a implementar la fiabilidad y el tiempo de respuesta en recuperar el sector afectado. El cual tiene que ver con la velocidad de reacción de los dispositivos de medición y protección en el instante en que ocurre cualquier acontecimiento en la red.

Con la aplicación de la Norma IEC61850 dentro de las subestaciones, permitirá a los entes del sector eléctrico, contar con un sistema más fiable en tiempo de respuesta a una falla, ahorro en el cableado y comunicación vía Ethernet, interoperabilidad en dispositivos de diferente fabricante al momento en que un dispositivo falle y deba ser reemplazado por otro sin importar el tipo de fabricante o marca de este.

CAPÍTULO I

Conceptos generales sobre el Estándar IEC – 61850

1.0 Aspectos generales.

En este capítulo se presentan la descripción de la líneas de alta tensión, esquema de la subestación de energía eléctrica, los equipos de protección, medición y comunicación, redes Ethernet, arquitectura de comunicación, centro de monitorio SCADA, protocolo de comunicación basado en el estándar IEC 61850 y normas requeridas para la aplicación de dicho estándar, con el objetivo de lograr un ambiente seguro, tanto para los equipos como el personal, que realiza trabajo dentro de las subestaciones eléctricas. Se enfocan en base a las recomendaciones de algunas normas como: las ISOS, IEEE, NEMA, etc. Como una observación especial ya que la ubicación es dentro de las subestaciones donde existe radiación electromagnética emitida, ya sea por fuentes artificial o natural, que posee corrientes eléctricas que varían rápidamente, como la subestación misma y el sol.

1.1 Descripción general de la línea de alta tensión.

En conceptos generales el proceso desde la producción hasta el consumo por el usuario final es el siguiente:

- La energía generada, ya sea hidroeléctrica, geotérmica o térmicamente, se transporta en grandes bloques a través de las Líneas de Transmisión, las cuales se interconectan por medio de subestaciones ubicadas tanto en los centros de generación, como en los sitios donde se hace la reducción que permite distribuir la energía a los consumidores finales.
- El transporte de grandes cantidades de energía corresponde al negocio de Transmisión el cual se hace a altos niveles de tensión.
- Antes de llegar al usuario final, la energía eléctrica se transforma a niveles de voltaje medios y a través de redes, nuevas subestaciones y nuevos transformadores, se lleva hasta los puntos de consumo. Este transporte de bloques menores de energía con destino al usuario final se denomina Distribución.
- La actividad de comercialización se encarga de comprar energía a los generadores, pagar el servicio de transporte a Transmisores y Distribuidores y venderla al usuario final.

La Transmisión eléctrica generalmente se transmite mediante los sistemas de corriente alterna. Hoy en día, los niveles de voltajes de transmisión son generalmente considerados 115kV y superiores. Voltajes Inferiores como 46 KV y 34 KV generalmente se consideran voltajes de sub-transmisión, pero que son ocasionalmente se utiliza sobre largas líneas con cargas ligeras. Voltajes menos de 34 KV son generalmente utilizados para distribución. Voltajes por encima de 230 KV son considerados extra alta tensión y requieren diferentes diseños en comparación con los equipos utilizados en Voltajes más bajos. Líneas de transmisión aérea son de alambre no aislado, por lo que el diseño de estas líneas requiere mínimo autorizaciones a observarse para mantener la seguridad. Una línea de sobrecarga

eléctrica es una línea de transmisión de energía eléctrica suspendida por Torres o postes. Dado que la mayoría del aislamiento se proporciona por vía aérea, líneas eléctricas son generalmente el método de costo más bajo de la transmisión de grandes cantidades de energía eléctrica.

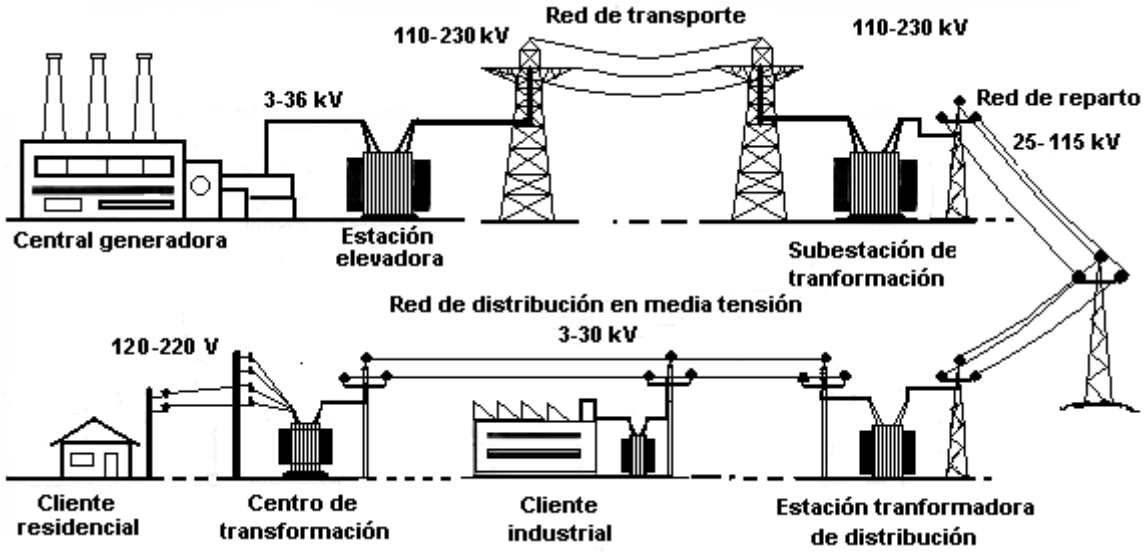


Figura 1: Esquema de la red de transmisión de energía eléctrica.

1.1.1 Esquema general de una subestación de alta tensión.

Las subestaciones eléctricas son escenarios esenciales dentro del sistema de potencia ya que son instalaciones con un conjunto de dispositivos y circuitos que tienen la finalidad modificar las variables de tensión y corriente y de dar un medio de interconexión y despacho entre la líneas del sistema, Al ser las subestaciones tan importantes se debe analizar la confiablidad que se tiene al brindar el servicio así como la importancia de la subestación, de aquí nace las distintas configuraciones y la necesidad de proteger y medir los propiedades de los elementos y dispositivos que la conforman.

En una subestación eléctrica se encuentra muchos dispositivos, los cuales cumplen funciones distintas. En la imagen 2, se puede observar los dispositivos más importantes de la subestación.

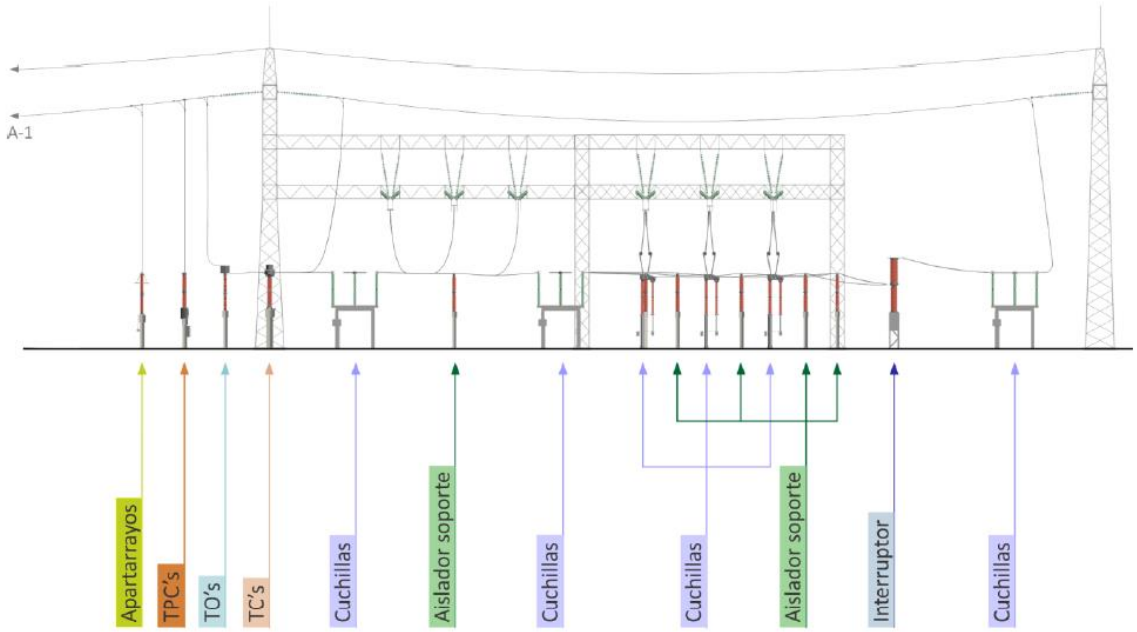


Figura 2: Dispositivos principales de la subestación eléctrica.

1.1.1.1 Tipos de subestaciones y funciones

La subestación eléctrica es de suma importancia para el sistema de generación, transmisión y distribución eléctrica. Según hay cuatro tipos principales de subestaciones eléctricas.

- **La subestación del switchyard** en una estación de generación, conecta los generadores a la red de transmisión y también proporciona energía fuera del sitio a la planta. Los puestos de generación de tienden a ser grandes instalaciones que normalmente son diseñadas y construidas por los diseñadores de plantas de energía y están sujetas a esfuerzos de planificación, finanzas y construcción diferentes de los proyectos de subestación de rutina.
- **La subestación del cliente** funciona como la fuente principal de suministro de energía eléctrica para un cliente comercial particular. Los requisitos técnicos y el caso de negocios para este tipo de instalaciones dependen más de los requisitos del cliente que de las necesidades de servicios públicos.
- **La subestación del sistema** implica la transferencia de energía a gran cantidad a través de la red. Algunas de estas estaciones sólo proporcionan instalaciones de conmutación (sin transformadores de potencia), mientras que otras también realizan conversión de voltaje. Estas estaciones grandes suelen servir como puntos finales para las líneas de transmisión que se originan en los puestos de distribución del generador y proporcionan la energía eléctrica para los circuitos que alimentan las estaciones del transformador. Son parte integrante de la fiabilidad e integridad a largo plazo del sistema eléctrico y permiten mover grandes cantidades de energía de

los generadores a los centros de carga. Las subestaciones del sistema son instalaciones estratégicas y por lo general muy costosas de construir y mantener.

- **Las subestaciones de distribución** son las instalaciones más comunes en los sistemas de energía eléctrica y proporcionan los circuitos de distribución que abastecen directamente a la mayoría de los clientes. Por lo general se encuentran cerca de los centros de carga, lo que significa que por lo general se encuentran en o cerca de los barrios que suministran el servicio al consumidor final.

En la Figura 2, se presenta una representación visual de cómo se usan las subestaciones eléctricas dentro de la red eléctrica. La subestación se representa como una caja gris.

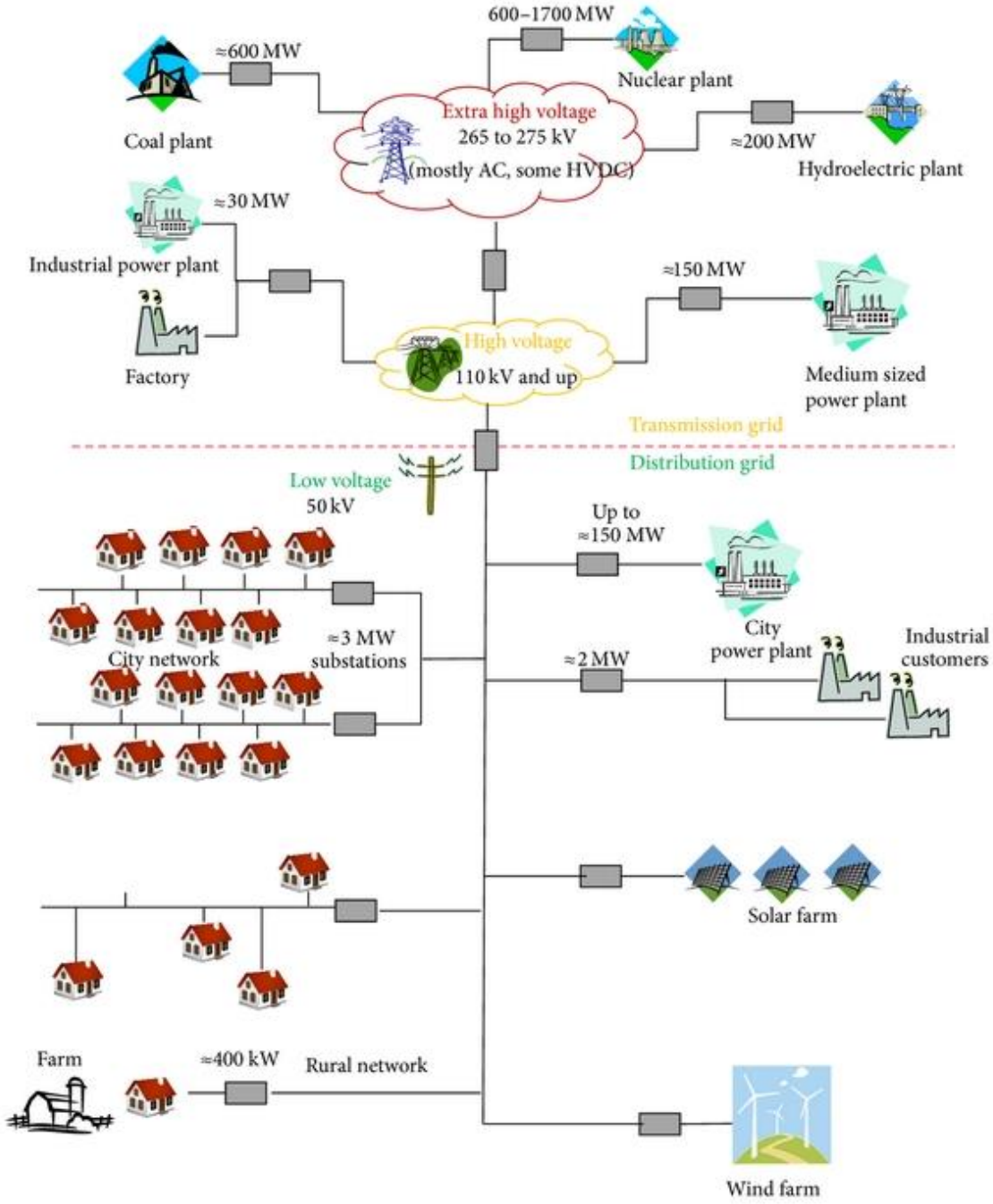


Figura 3: Subestación en la red de energía eléctrica.

Las funciones de las subestaciones indican claramente que puede considerarse como infraestructura crítica, especialmente para las subestaciones de la red de transmisión, interconectando muchos sistemas. Como tal, requiere una protección física y cibernética adecuada para garantizar un funcionamiento sin interrupciones y sin problemas.

1.2 Sistema de protecciones.

Un sistema de protección es el conjunto de dispositivos y elementos interrelacionados (y sus funciones) que permiten o aportan al objetivo del mismo: proteger el equipo de potencia que corresponde o al sistema de potencia.

Los equipos de protección se utilizan en los sistemas eléctricos de potencia para evitar la destrucción de equipos o instalaciones por causa de una falla que podría iniciarse de manera simple y después extenderse sin control en un efecto cadena. Los sistemas de protección deben aislar la parte donde se ha producido la falla buscando perturbar lo menos posible la red, limitar el daño al equipo fallado, minimizar la posibilidad de un incendio, minimizar el peligro para las personas, minimizar el riesgo de daños de equipos eléctricos adyacentes.

Un sistema de protección tiene los siguientes componentes principales:

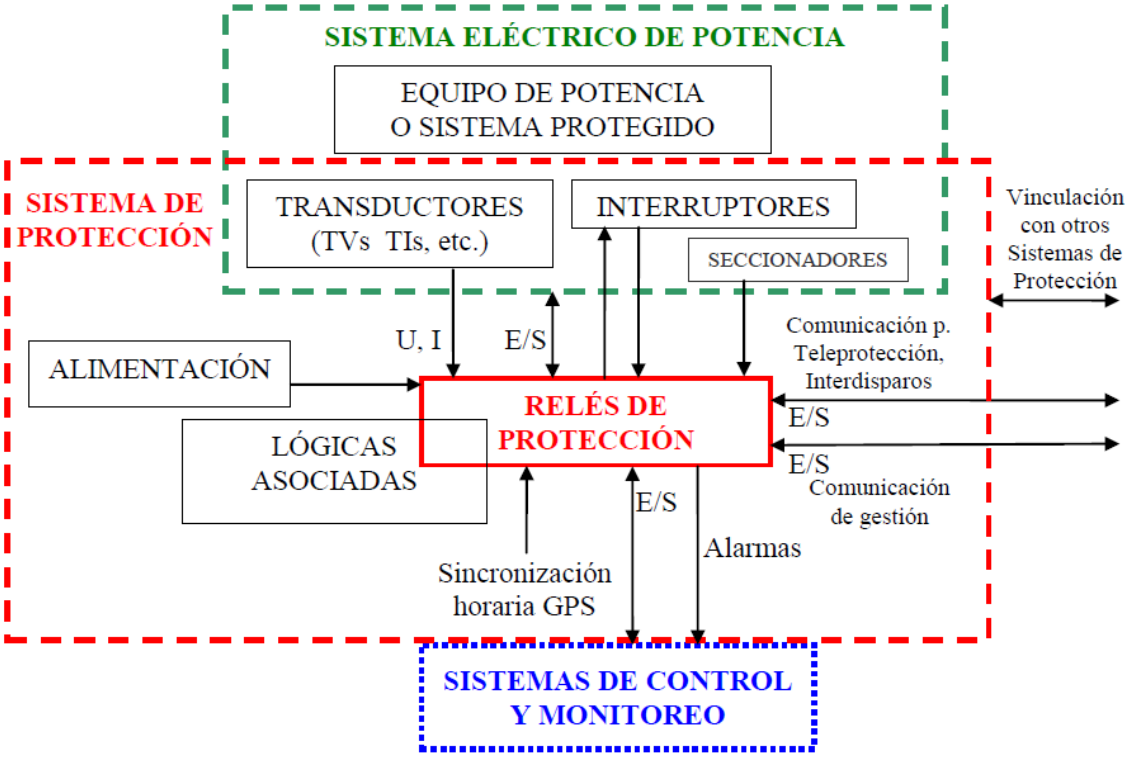


Figura 4: Componentes de un sistema de protección.

1.2.1 Sistema de protecciones de líneas de transmisión.

Para la protección de línea serán utilizados IEDs, adecuados para protección de líneas con carga elevada, y líneas con varios terminales, en las que los requisitos de disparo sean de uno, dos y/o tres polos. La función principal de la protección diferencial de corriente de fases segregadas, que ofrece una excelente sensibilidad ante faltas de alta resistencia, y una selección segura de fases. Un completo esquema de protección de distancia con tele

protección, es incluido como protección independiente o de respaldo ante fallos de comunicación del extremo remoto.
La biblioteca de funciones con las funciones básicas y opcionales es mostrada en la Tabla 1.

Funciones básicas	Funciones de aplicaciones básica	Funciones de aplicaciones opcionales
Registro de disturbios	Protección Diferencial	Protección de Frecuencia
Lista de Eventos	Reconexión	General U/I
Tiempo de Sincronización	Sincronismo	Control de equipo
Medición	Fallo de fusible	
Lógica Configurable	Localizador de falta	
Contador de Eventos	Falta a tierra direccional	

Tabla 1: Funciones de la protección de la línea de transmisión.

1.2.1.1 Protección Diferencial (87L).

La protección principal de la línea de transmisión es protección diferencial (87L), cuya función es del tipo de fases dividas con restricción por corriente, donde la corriente diferencial es la suma vectorial de todas las corrientes medidas tomadas separadamente para cada fase. Por otro lado, se toma como corriente de restricción la mayor corriente de fase en cualquiera de los terminales de la línea, y es común para las tres fases. En la característica Idif contra Irestr pueden ser definidos varios tramos de recta configurables con diferentes pendientes.

Los valores de la amplitud y ángulo de fase de la corriente para la protección diferencial deben muestreados al menos 20 veces por cada ciclo (sampled valúes) en cada IED. Sin embargo, el intercambio de comunicación se hace sólo cada 5ms, esto significa que, en nuestro sistema de 60 Hz, los valores de medida se codifican en telegramas digitales conteniendo cada uno cinco muestras consecutivas y se intercambian entre los IEDs de los extremos de la línea. Además, en cada telegrama hay espacio para hasta ochos señales binarias, lo cual será utilizado para la transmisión de señales de TDD (Transferencia de Disparo Directo). La comunicación dúplex entre los IEDs es implementada en canales digitales de 64 kbit/s conforme a la norma ITU (CCITT) PCM. El formato usado para los telegramas es el C37.94 y cada telegrama contiene encabezado y fin (8 bits cada uno), los datos transmitidos (n x16 bits) y una sección para verificación de la validez del telegrama.

1.2.2 Causas de funcionamiento anormal en los sistemas de potencia.

En los sistemas de potencia puede ser afectado por muchas situaciones anormales que produzcan una operación fuera de las condiciones normales, estas posibles causas pueden ser:

- Falla de los componentes del sistema.
- Situaciones de carácter imprevisto (tormentas)
- Errores de operación (manual o automático)

Esas situaciones provocan efectos muy variado en los sistemas de potencias tales como:

- Mal servicio
- Perdida de la estabilidad
- Daños de los equipos

Las compañías eléctricas son las encargadas de desempeñar las funciones del sistema de potencia, siendo importante para ellas eliminar las situaciones anormales de operación. Las interrupciones del servicio, y la variación de los parámetros de red (tensión, corriente, frecuencia, etc.) fuera de los límites, son consecuencia común de una operación anormal causando enormes inconvenientes técnicos y económicos

Una clasificación sencilla de las anormalidades de acuerdo a su severidad con que afectan al sistema de potencia los podemos observar en la figura 5:

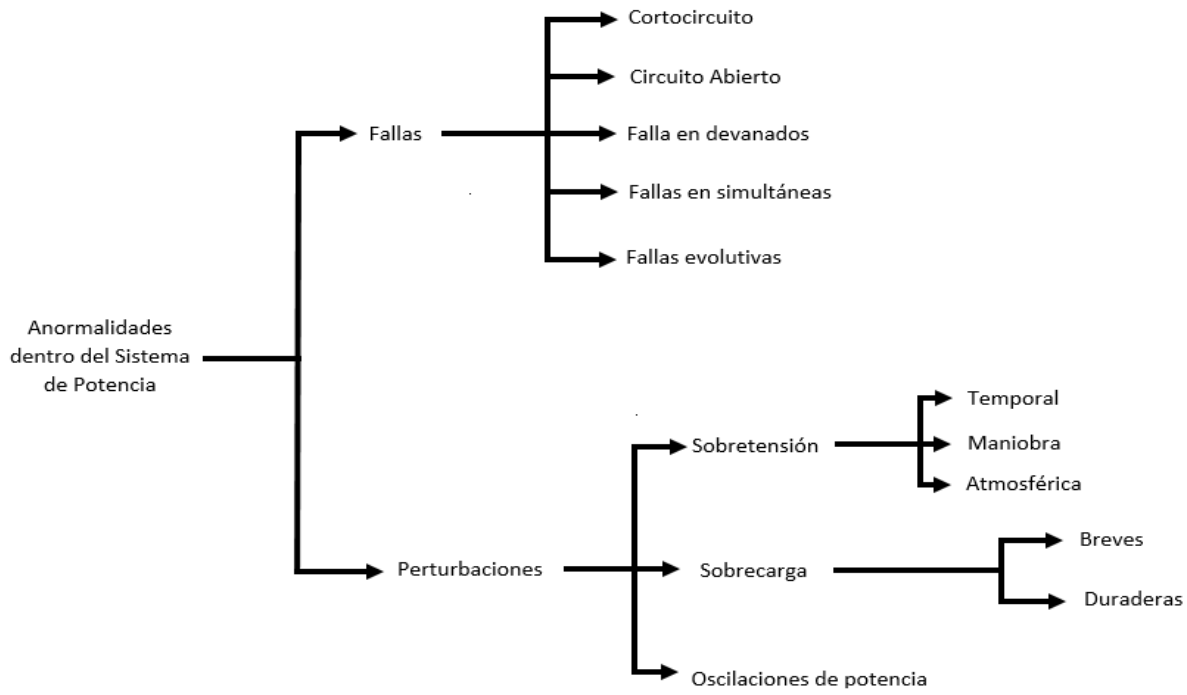


Figura 5: Anormalidades en los Sistema de Potencia.

1.3 Sistema de medición.

La importancia de los instrumentos eléctricos de medición es incalculable, ya que mediante el uso de ellos se miden e indican magnitudes eléctricas, como corriente, carga, potencial y energía, o las características eléctricas de los circuitos, como la resistencia, la capacidad, la capacitancia y la inductancia. Además, que permiten localizar las causas de una operación defectuosa en aparato eléctrico en los cuales, como es bien sabido, no es posible apreciar su funcionamiento en una forma visual, como en el caso de un aparato mecánico.

Estos equipos de medida se energizan directamente a partir del campo electromagnético de la línea; si la corriente cae de 120 Amperios, las unidades continúan operando hasta por 12 horas (gracias a una batería incorporada). Asimismo, en caso de pérdida de comunicación, poseen memoria interna, que almacena toda la información en el período sin comunicación; una vez restablecidos estos canales, se descargan al sistema todas las variables, que incluyen ángulo de la catenaria, temperatura de la línea, voltaje, corriente y potencia, entre otras.

1.3.1 Sistema de medición de línea de transmisión.

Los equipos de medición en la línea modernos han permitido que estos dispositivos incorporen sistemas de localización satelital GPS, para establecer con exactitud el lugar donde la unidad está instalada y aportar un panorama general en conjunto con información complementaria generada, por ejemplo, mediante estaciones meteorológicas (que entregan datos como velocidad del viento, humedad relativa del aire, presión, etc.). En este caso, una estación meteorológica instalada en la estructura de la torre puede comunicarse vía radio 2.4 GHz o Bluetooth con el dispositivo de medición, el que se encarga de reenviar la información (tanto de la línea misma como de las condiciones ambientales que la rodean).

La medición directamente en la línea tiene una relevancia tecnologías, lo cual permite que los datos precisos y oportunos, un operador puede detectar a tiempo eventuales sobrecargas por exceso de temperatura, lo que permite balancear la transmisión a una línea paralela bajando la carga en la línea exigida, prolongando su vida útil y evitando perdidas de eficiencia. Un exceso de temperatura o viento extremo genera elongación en la catenaria produciendo condiciones de ineficiencia, incluso riesgos para objetos o estructuras físicas cercanas.

El uso de estas tecnologías no entrega variables a considerar, sino que entrega datos reales y precisos de la realidad que acontece en los sistemas, disminuyendo las asimetrías de información entre generadores y transmisores de energía, entre otras ventajas. Si una línea de transmisión es golpeada por un rayo, la unidad de medición informará de cualquier cambio en las variables que provoque este fenómeno de la naturaleza.

Las tecnologías de medición para líneas de Media y Alta Tensión IN SITU, en el mundo son contadas con una mano. Las diferencias entre ellas son decidoras y están dadas

principalmente por su robustez, confiabilidad y, por, sobre todo, por su precisión en la medición.

1.4 Sistema de Comunicación.

Podemos definir a un sistema de comunicación como un conjunto de dispositivos interconectados que realizan acciones las cuales permiten que las personas puedan comunicarse o conectarse entre sí. Las nuevas tecnologías emergentes hicieron que el sistema de comunicación a través de protocolos abiertos es más utilizado en los procesos industriales.
La importancia del nuevo modelo de redes eléctricas radica en la optimización del recurso energético, maximizando el rendimiento de la red y reduciendo el consumo, permitiendo a las operadoras gestionar con eficiencia el sistema y a los usuarios hacer un uso racional de la misma.

Entre los principales objetivos de la norma IEC 61850 se encuentra el empleo de un modelo de intercambio de información entre los diferentes dispositivos que componen la red eléctrica, añadiéndoles capacidades de monitorización, análisis, control y comunicación al sistema. Esto permitirá a las operadoras tomar acertadas y rápidas decisiones en base a los datos, para así mejorar la eficiencia y optimizar procesos y costos.

Este trabajo proporcionará un estado de la técnica de las partes relevantes de la Red Inteligente, centrándose principalmente en la automatización de la subestación en el dominio de transmisión, así como protocolos y el centro de control.

1.4.1 Principales componentes de sistema de comunicación.

En la automatización de subestaciones eléctricas, el centro de operaciones (o centro de control maestro o estación maestra SCADA) recibe y procesa datos de varias subestaciones y toma las acciones de control de subestación remota apropiadas. El sistema de estación maestra puede utilizar alguna vez una arquitectura abierta y distribuida. También puede haber varias estaciones maestras y, por consiguiente, pueden utilizarse diferentes topologías para interconectarlas para sincronizar los datos operativos de la red. Cada estación maestra (tripulada) está soportada con una estación maestra de respaldo / emergencia (no tripulada) y se sincroniza continuamente con una base de datos de estaciones maestras primarias.
Los principales elementos de la estación maestra SCADA (o maestro SCADA) son la interfaz HMI (Human Machine Interface), los servidores de aplicaciones, el firewall, la interfaz de comunicación (para comunicarse con los concentradores RTU / datos) y el servidor de comunicaciones externas / M2M Gateway Con otros centros de control). Estos elementos se conectan en red dentro del maestro SCADA a través de la LAN dedicada en tiempo real. Los servidores de aplicaciones incluyen servidores que admiten todas las aplicaciones del sistema de gestión de energía (EMS) o del sistema de gestión distribuida (DMS).

Se proporciona redundancia para los elementos de hardware y software de las estaciones maestras SCADA (por ejemplo, LAN redundante) y subestaciones (por ejemplo, ordenador crítico redundante), así como para la red de comunicaciones M2M.

1.4.2 Capa de comunicación.

La capa de comunicación en las redes inteligentes sirve como núcleo de todo el sistema de monitoreo remoto. No sólo recoge datos operativos de los dispositivos de campo y envía los datos a los servidores SCADA, sino que también transmite comandos desde el centro de control a las unidades de control para accionar el equipo. El énfasis de la capa de comunicación es describir protocolos y mecanismos apropiados para el intercambio interoperable de datos entre los componentes de la red inteligente.
Los requisitos clave de un sistema de comunicación rápido, robusto y fiable incluyen.

I. Identificación de flujos de tráfico de comunicación: fuente / destino / cantidad.
II. topología del sistema (por ejemplo, estrella, malla, anillo, bus).
III. Esquemas de direccionamiento de dispositivos.
IV. Características del tráfico de red de comunicación (ancho de banda, retardo, latencia, confiabilidad y manejo de errores).
V. Requisitos de desempeño.
VI. Cuestiones relativas al calendario.
VII. Confiabilidad / copia de seguridad / conmutación por error.
VIII. Requisitos operativos (por ejemplo, seguridad y gestión de la red).
IX. Cuantificación de los requisitos de resistencia a interferencias electromagnéticas.

Otro requisito crítico y la tendencia reciente en la integración de la subestación y la arquitectura de automatización es el uso de interfaces de comunicación estándar para asegurar la interoperabilidad entre los diferentes componentes de los proveedores, así como con el equipo heredado. La falta de protocolos estándar puede conducir a errores de comunicación o la incompatibilidad entre diferentes dispositivos. Las industrias que han invertido en sistemas de comunicación SCADA, propietarios y orientados a proveedores, abordan problemas de escalabilidad graves, ya que se limitan a una selección limitada de equipos cuando cambian los requisitos.

Para mitigar tales problemas, los protocolos de comunicación abiertos (por ejemplo, IEC 60870-5-101 / 104 y DNP 3.0) y la comunicación de centro de control a centro de control (por ejemplo, ICCP IEC60870-6 / TASE.2) se hicieron cada vez más populares entre Fabricantes de equipos SCADA y proveedores de soluciones en los sistemas de monitoreo de datos.

1.4.3 Tecnologías de la comunicación.

En las subestaciones convencionales, se utilizan buses de comunicación serie o protocolos propietarios para la HMI local, así como para la comunicación SCADA remota. La comunicación moderna en la subestación es la transmisión de datos dentro y entre la estación, la bahía y el nivel de proceso. La comunicación entre estos 3 niveles se denomina comunicación vertical y se realiza mediante bus de estación Ethernet de alta velocidad y bus de proceso. El bus de estación facilita la comunicación entre el nivel de la estación y el nivel de la bahía. La comunicación dentro de un nivel se considera horizontal. Las redes de comunicación dentro de las subestaciones a menudo tienen enlace de datos de nivel inferior, protocolos de capa física y múltiples protocolos de capa de aplicación que se ejecutan en la parte superior de TCP / IP.

Los sistemas SCADA tradicionales tenían un modelo de comunicación maestro-esclavo. Hoy en día, con la disponibilidad de protocolos de comunicación en red, como IEC 61850, es posible soportar simultáneamente a múltiples clientes ubicados en diferentes ubicaciones remotas, aunque complica quién tiene el control del equipo. La figura 6 muestra un ejemplo de dicha red. Estas redes permiten la integración tanto del centro de control como de los sistemas de información empresariales.

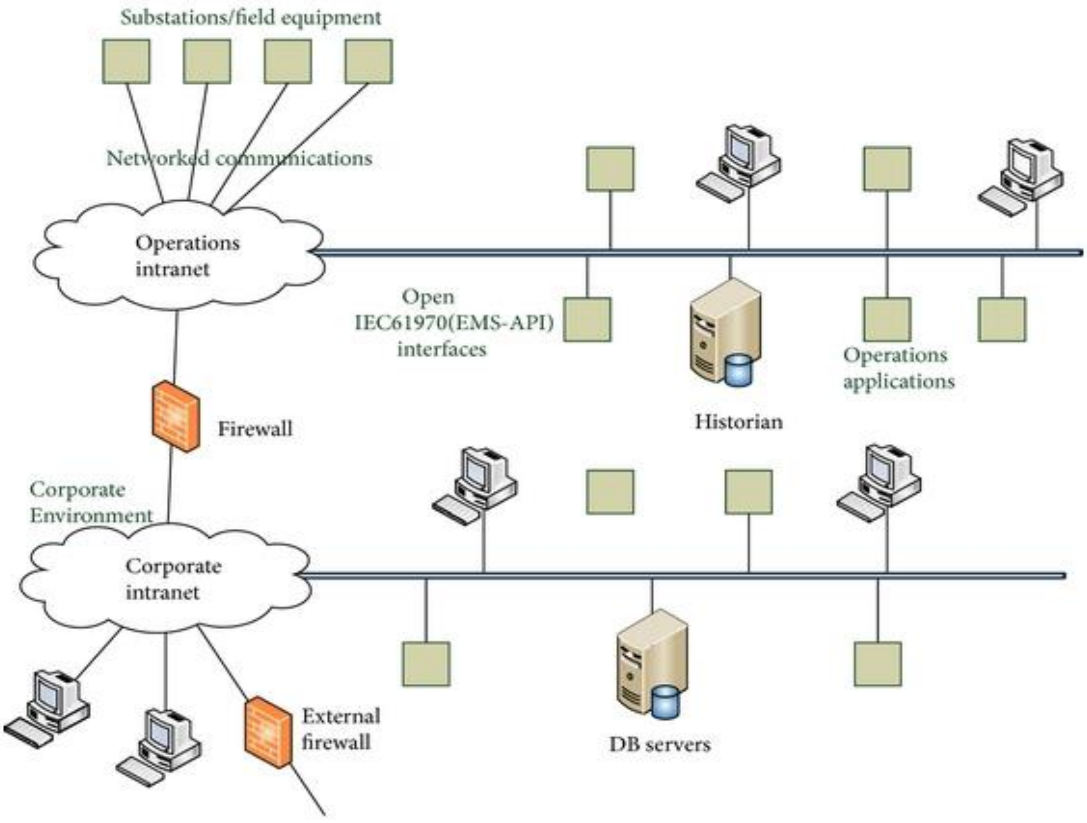


Figura 6: Comunicaciones SCADA en red.

Basándose en la topología de la red de distribución, la tecnología apropiada debe elegirse entre diferentes soluciones. Las redes de comunicación de servicios públicos comprenden tecnologías inalámbricas y cableadas. Para la interconexión de la subestación con el centro de control o entre la red eléctrica se pueden emplear cables de cobre (por ejemplo, señales DSL de banda ancha o de banda ancha), fibra óptica (por ejemplo, señales Ethernet para LAN de banda ancha), líneas telefónicas arrendadas o comunicaciones celulares y satelitales Componentes de la subestación. La nueva tendencia de desarrollo son las tecnologías de radio de espectro ensanchado que pueden operar en bandas ISM sin licencia en las bandas de 900 MHz, 2,4 GHz y 5,6 GHz o con licencia en otras bandas cercanas.

Los criterios para la selección de la tecnología más apropiada son los requisitos de ancho de banda y demora para el enlace de comunicación, y si una solución global o regional está dirigida o no. Además, los sistemas inalámbricos y por satélite están sujetos a escuchas telefónicas, por lo que el uso de medidas de seguridad adecuadas está indicado para evitar la pérdida de información confidencial.

Las redes de comunicación SCADA tienden a estar en línea con las tecnologías de redes estándar en el futuro. Los protocolos basados en Ethernet y TCP / IP están reemplazando los antiguos estándares propietarios. Las estrategias de migración que están disponibles hoy en día tienen que ser identificadas, con el fin de pasar de la tecnología de legado a los protocolos estándar. Es poco probable que una sola tecnología proporcione una solución completa para todas las comunicaciones, por lo que la interoperabilidad y la compatibilidad de diferentes tecnologías será el requisito clave para todas las futuras generaciones de sistemas.

1.4.4 Protocolos de comunicación.

Un reciente esfuerzo en las interfaces de comunicación de un centro de control es el protocolo OPC. En general, permite el intercambio general de datos entre aplicaciones de automatización y control, sistemas / dispositivos de campo, así como aplicaciones empresariales y de oficina. Fue desarrollado por la industria de automatización para estandarizar la comunicación de datos de planta en tiempo real entre dispositivos de control de diferentes fabricantes. Específicamente, OPC es un conjunto de estándares industriales para la interconectividad de sistemas, proporcionando una interfaz común para comunicaciones entre aplicaciones de software de varios proveedores que es aplicable en una amplia gama de industrias que abarcan desde industrias de procesos hasta automatización de subestaciones y muchas otras. Más recientemente, el protocolo OPC UA, se introdujo con el fin de apoyar la interoperabilidad y la independencia de la plataforma.

La comunicación entre centros de control se realiza a través del ICCP (Inter Control Center Communication Protocol) o ELCOM, y se basa en TCP / IP. El ICCP es un protocolo abierto y estandarizado basado en la IEC 60870-6 y el elemento de servicio de aplicación de Telecontrol 2 (TASE.2). Los datos intercambiados son principalmente información en tiempo real del sistema, como valores analógicos, valores digitales y valores de

acumuladores, junto con comandos de control de supervisión. La transferencia de datos puede tener lugar en ambas direcciones entre dos centros de control. Ambos centros de control pueden iniciar interacciones / transferencias de datos. El protocolo soporta la transferencia espontánea de datos, la transferencia periódica de datos y la transferencia de datos bajo petición.

Para la comunicación dentro de la subestación se utiliza ampliamente la IEC 61850 desarrollada por WG 10. Es un estándar para la automatización de la utilidad eléctrica, definiendo la comunicación entre IED dentro de una subestación. Se desarrolla dentro de la IEC TC 57 y se compone de 10 partes. Proporciona protocolos de comunicación, modelos de datos, estándares de seguridad, etc. Aunque el alcance de la IEC 61850 se centró originalmente en l
La automatización de la subestación y en la comunicación correspondiente, se están llevando a cabo conversaciones para determinar la IEC 61850 para el protocolo de comunicación Subestación a Maestro. Además, las aplicaciones están disponibles utilizando varios componentes de IEC 61850 para la comunicación de subestación a subestación de área amplia.

El DNP3 es un protocolo de comunicación en serie y especifica la capa de enlace de datos, la capa de aplicación y una pseudo-capa de transporte. Se utiliza sobre todo en utilidades eléctricas en Norteamérica, y ofrece características similares como IEC 60870-5-104, que es más popular en Europa. Su alcance es permitir la interoperabilidad entre equipos de telecontrol compatibles. Modbus es otro protocolo de comunicación en serie que está comúnmente disponible para la interconexión de dispositivos electrónicos. Modbus es muy conocido, fácil de implementar y ampliamente utilizado en todas las industrias. Sin embargo, como la mayoría de los protocolos en serie, Modbus no ofrece seguridad y no hay forma estándar de proporcionar información sobre los datos que transporta.

1.5 Descripción del Estándar IEC- 61850.

Cuando se trata de un proyecto relacionado con el diseño de un sistema de automatización de subestación (Substation Automation System – SAS), las compañías eléctricas buscan una solución que ofrezca las mejores ventajas actuales, pero que a su vez sea una solución duradera en el tiempo desde un punto de vista tecnológico.

En ese sentido, la norma IEC 61850 ha sido concebida para ser una solución válida tanto para el presente como para el futuro. A día de hoy, el uso de gateways permite la coexistencia y el entendimiento en una misma subestación entre dispositivos IEC 61850 y aquellos que no lo son. Asimismo, mediante la definición de un modelo de datos y de un conjunto de servicios de comunicación estandarizados, la norma posibilita la implementación de soluciones multi-vendedor, asegurando la interoperabilidad entre dispositivos de distintos fabricantes. El estándar IEC 61850 está pensado no sólo para

subestaciones de nuevo diseño, sino también para la renovación y ampliación de subestaciones ya existentes.

En la figura 7 se identifica claramente lo que se puede lograr con la aplicación de la norma, se define la estructura para la Protección y el Control, la comunicación entre dispositivos (IEDs), la representación de los almacenamientos de las fallas en los dispositivos en formato comtrade, la sincronización de los dispositivos a través de protocolo de comunicación como NTP (Network Time Protocol), SNTP (Simple Network Time protocol) e IEEE 1588 (PTP precisión Time Protocol) se toma como base el estándar Ethernet (IEEE 802.3), a la vez la comunicación se basa en el estándar TCP-IP, se establece el lenguaje de descripción de la subestación y se define el sistema de configuración.

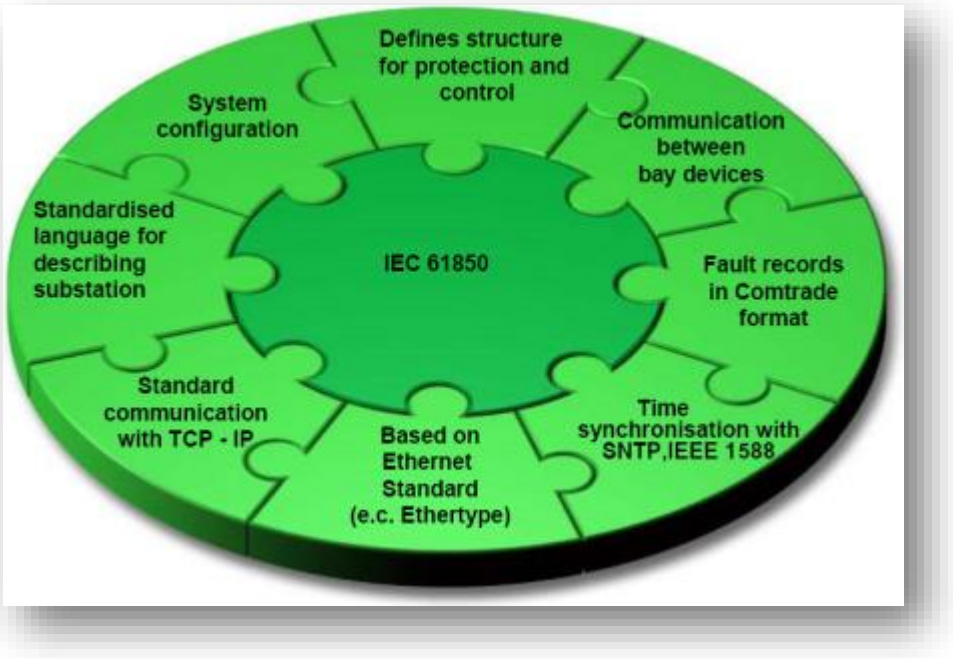


Figura 7: Loque se puede lograr con el estándar IEC 61850.

Estas y otras ventajas que ofrece la norma la convierten en una solución atractiva en la implementación de sistemas de automatización en subestaciones eléctricas. Ahora bien, a la hora de abordar un proyecto de este tipo, existen una serie aspectos a tener en cuenta; aspectos algunos de ellos determinantes a la hora de garantizar con mayor probabilidad el éxito en la ejecución del mismo.

1.5.1 Arquitectura de la subestación.

Tal y como se muestra en la Figura 8, una subestación puede dividirse en tres niveles funcionales distintos: nivel de subestación, nivel de bahía y nivel de proceso.

- El nivel de proceso es aquel en el que se sitúan los equipos primarios, tales como sensores, transformadores de corriente, transformadores de tensión, interruptores y seccionadores.
- En el nivel de bahía se ubican los equipos de protección, control y monitorización.
- El nivel de subestación es aquel donde se sitúan las unidades centrales de subestación que se conectan con los centros de control.

Bajo la norma IEC 61850, en estos niveles se pueden encontrar distintos dispositivos electrónicos inteligentes (Intelligent Electronic Devices - IEDs) con funciones de protección, control, supervisión, medición y comunicación principalmente. De modo que podemos encontrar IEDs típicos tales como: computadores de subestación (HMI), RTUs (Remote Terminal Units), Gateway, equipos de monitorización, relés de protección, unidades de control de bahía, contadores, transformadores de instrumentación digitales, MUs (Merging Units), entre otros.

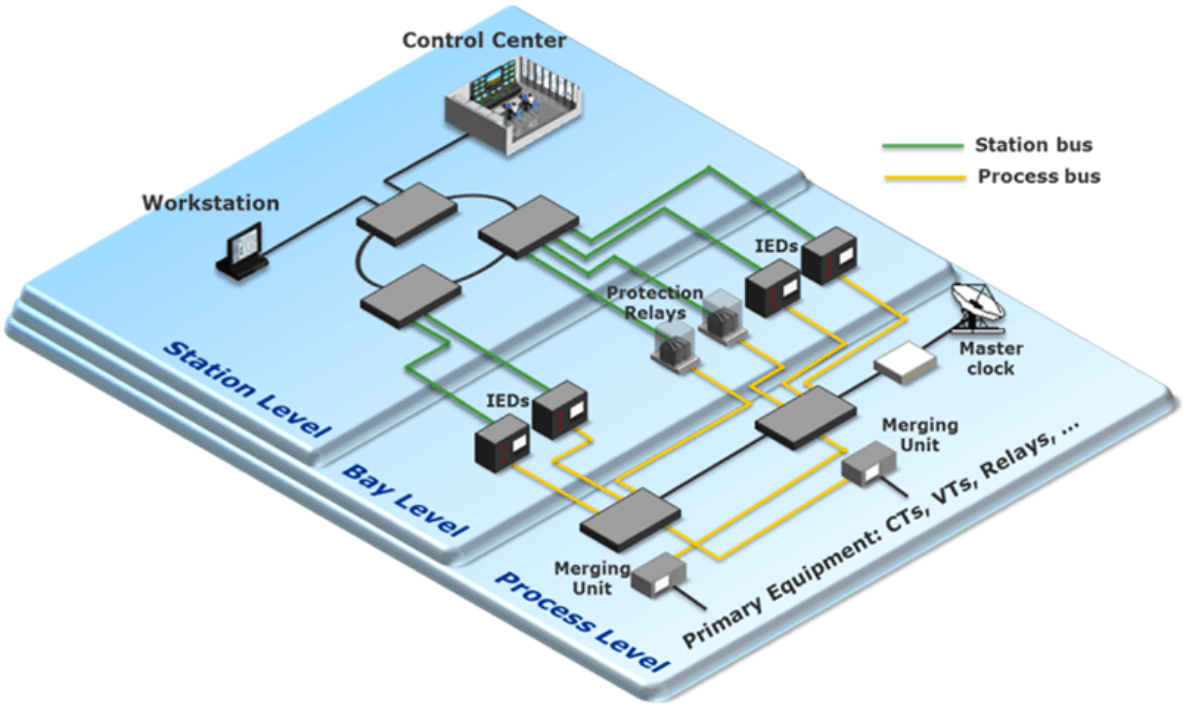


Figura 8: Arquitectura de la Subestación.

1.5.1.1 Componentes del sistema de Automatización de Subestaciones.

El sistema SAS utiliza cualquier número de dispositivos integrados en una matriz funcional con el propósito de monitorear, controlar y configurar la subestación.

Los componentes del sistema SA son como se ilustra en la Figura 9 donde VT, CT y PT representan voltaje, corriente y transformador de potencia, en consecuencia. En la siguiente

sección, describimos los componentes de la subestación remota y los componentes del centro de operaciones.

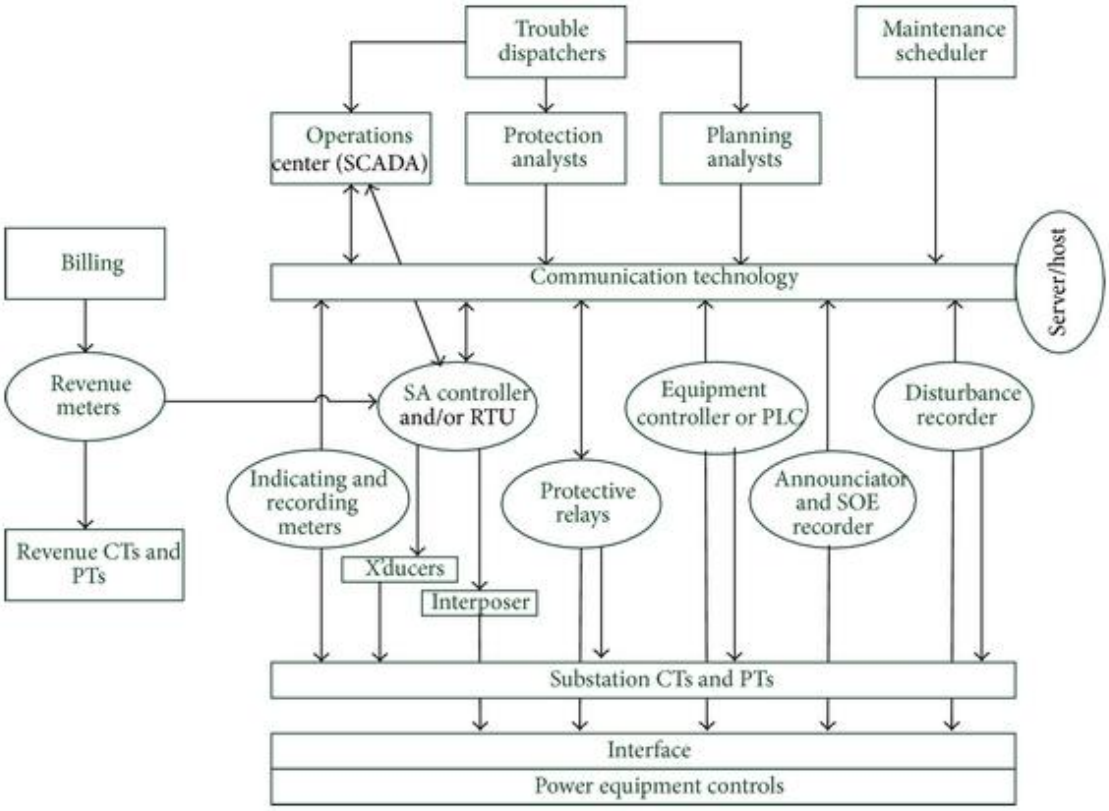


Figura 9: Diagrama funcional de sistema de automatización de subestación.

1.5.1.2 Componentes de la Subestación Remota.

Los componentes SAS presentes en la subestación son los siguientes.

- Dispositivos electrónicos inteligentes (IED) basados en microprocesadores, que proporcionan entradas y salidas al sistema mientras realizan algún servicio de control o procesamiento primario. Los IED comunes son relés de protección, indicadores de medición de carga y / u operador, medidores de ingresos, controladores lógicos programables (PLC) y controladores de equipos de potencia de varias descripciones.
- También pueden estar presentes dispositivos dedicados a funciones específicas para el sistema SAS, como transductores, sensores de posición y grupos de relés de interposición.

- Los dispositivos dedicados a menudo utilizan un controlador (controlador SA) o un equipo de interfaz como una unidad terminal remota convencional (RTU) como medio para conectarse al sistema SAS.
- También puede estar presente una pantalla de subestación o una estación de usuarios (HMI local), conectada o parte de una computadora de la subestación (servidor local).
- Conexiones comunes de comunicación con el mundo exterior como centros de operaciones de servicios públicos, oficinas de mantenimiento y / o centros de ingeniería. La mayoría de los sistemas SAS se conectan a una estación maestra del sistema de control de supervisión y adquisición de datos (SCADA) que sirve las necesidades en tiempo real para operar la red de servicios públicos desde uno o más centros de operaciones. SAS también pueden incorporar una variación de la unidad terminal remota SCADA (RTU) para este fin o la función RTU puede aparecer en un controlador SA o en un ordenador host de subestación.

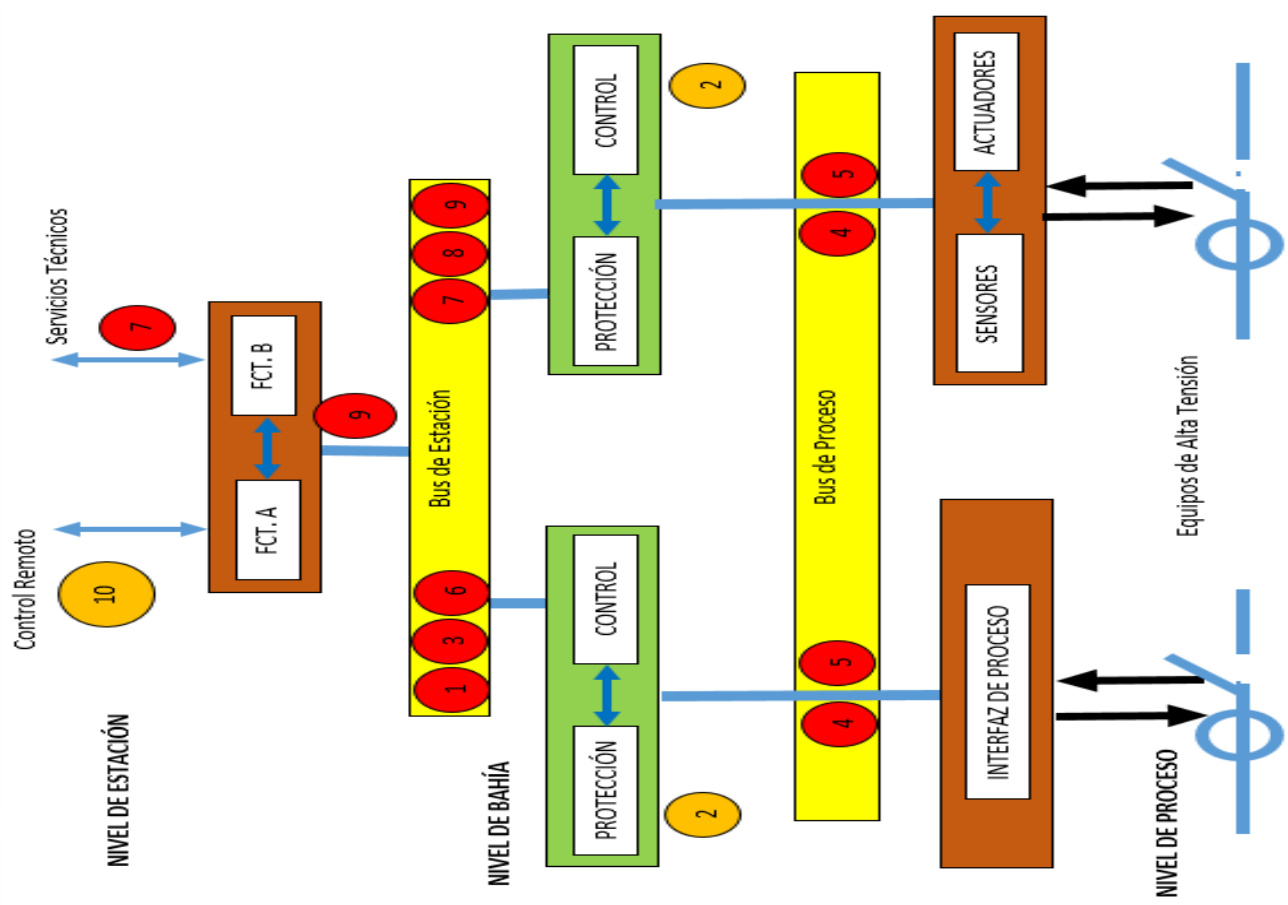
1.5.2 Niveles e interfaces lógicas.

Para permitir una libre asignación de funciones, la interoperabilidad debe esta proporcionada entre funciones, las cuales residen en equipos de distintos proveedores. Las funciones se dividen en pequeñas partes, que se localizan en distintos equipos físicos, pero de forma que se mantenga la comunicación de unas con otras. Estas partes que forman una función se denominan nodos lógicos (LN).

Las funciones (funciones de aplicación) de los SAS son control y supervisión, al igual que protección y supervisión de los equipos primarios. Otras funciones (funciones del sistema) están relacionadas con el sistema propiamente dicho, como por ejemplo la supervisión de la comunicación.
Las funciones se pueden asignar a tres niveles:

- **Nivel de estación**: Consiste en un ordenador para la subestación con su base de datos, pantallas para los operadores, interfaces de comunicación remota, etc.
- **Nivel de Bahía**: Compuesto por las unidades de protección, control y medida de posición.
- **Nivel de proceso**: Compuesto por módulos remotos de I/O, sensores inteligentes, relees de actuación, etc.

Entre estos niveles y dentro de los mismos existen unos interfaces lógicos de comunicaciones que conforman la red de comunicaciones del SAS. Estos interfaces están representados en la figura 10 estando fuera los números 2 y 10 fuera del alcance de la norma.



Lista de todos las posibles interfaces de comunicación de una subestación contempladas en el Estándar IEC 61850

N°	INTERFACES
1	Datos de protección entre nivel de estación y nivel de bahía
2	Datos de protección entre teleprotecciones
3	Datos de internos (sin especificar) del nivel de procesos
4	Datos de medida(de TC y TP) entre nivel de proceso y nivel de bahía
5	Datos de control entre nivel de proceso y nivel de bahía
6	Datos de control entre nivel estación y nivel de bahía
7	Datos de teleconfiguración y telesupervisión
8	Datos de protección entre niveles de bahía
9	Datos de control internos entre niveles de estación
10	Datos de control entre nivel de estación y los centros de control

Figura 10: Interfaces de comunicación en un sistema de automatización de subestaciones.

1.5.3 Nodos lógicos y funciones.

El principal objetivo del estándar IEC 61850 es proporcionar interoperabilidad entre los equipos IEDs de distintos fabricantes, de forma más precisa, entre las funciones que tienen lugar en la subestación y residen en los equipos físicos de distintos fabricantes.

La información, dentro del entorno de subestaciones, se intercambia entre los equipos que forman los sistemas de automatización de subestaciones, es decir los datos fluyen entre las funciones y sub-funciones de estos equipos. En el nuevo estándar lo que se propone es representar todas las funciones y equipos utilizados en el sistema, por medio de nodos lógicos (LN, *Logical Nodes)*. De esta forma toda la información de las subestaciones se estructura en unidades atómicas, los LNs. Además, también existe la posibilidad de poder incorporar nuevos nodos lógicos en el futuro, siempre y cuando siga las reglas definidas en el estándar.

Para alcanzar los requisitos principales de asignación y distribución libre de funciones, todas las funciones deben de descomponerse en nodos lógicos. Para poder intercambiar datos entre los distintos nodos, la norma define las conexiones entre nodos a través de conectores lógicos (LC, *Logical Connections*). En la figura se muestra los enlaces entre los nodos lógicos. Cada LN se asigna a una función y a un equipo (PD, *Physical Device)*, pudiendo existir varias funciones dentro de un mismo equipo. Los equipos se conectan a través de conexiones físicas (PC, *Physical Connections)*, de forma que un nodo lógico es parte de un equipo físico, y una conexión lógica es parte de una conexión física.

El estándar se define un total de 92 *logical nodes*, divididos en 6 grupos principales:

- Nodos lógicos para las funciones de protección.
- Nodos lógicos para el control.
- Equipos físicos.
- Seguridad del sistema y de los equipos.
- Nodos lógicos relacionados con los equipos primarios.
- Nodos lógicos relacionados con los servicios del sistema.

Indicador	Grupo de Nodos Lógicos	Función	cantidad
L	Nodos lógicos del sistema		3
P	Funciones de protección	PTOC, PIOC, PDIS, PDIF, etc.	28
R	Funciones relacionadas con Protecciones	RREC, RSYN, etc.	10
C	Control Supervisado	CSWI, CILO, CALH, CPOW	5
G	Funciones Genéricas	GGIO, GAPC, GSAL	3
I	Interface y Archivo	IHMI, ITCI, IARC, ITMI	4

A	Control Automático	ATCC, ANCR, ARCO, AVCO	4
M	Medidores y Medidas	MMXU, MMTR, MHAI, MSQI	8
S	Sensores y Monitorización	SIMG, SARC, SPDC	4
X	Equipos de conmutación	XCBR, XSWI	2
T	Transformadores de instrumentación	TCTR, TVTR	2
Y	Transformadores de potencia	YPTR, YLTC, YEFN, YPSH	4
Z	Equipo adicional	ZBAT, ZGEN, ZMOT, etc.	15
		Totales	**92**

Tabla 2: Nodos Lógicos y sus funciones definidos en el estándar IEC 61850.

Todos los nombres de los nodos lógicos empiezan con la letra indicadora del grupo al que pertenecen.

1.5.4 Modelo jerarquizado de las funciones del IED.

Cada nivel cuenta con capacidad de operación, pero esta operación está condicionada a la disponibilidad operativa, así como los respectivos permisos jerárquicos de los niveles inferiores inmediatos de la subestación.

El Modelo de Información de la Norma IEC 61850 representa el conocimiento asociado a las funciones de la subestación y los dispositivos donde se implementan estas funciones. Este conocimiento se hace visible y accesible a través de las distintas propiedades de la Norma IEC 61850. El modelo describe de una manera abstracta una comunicación orientada a la representación de una función real o dispositivo

Para representar de manera virtual algún aspecto de la realidad se utilizan los modelos, cuyo propósito es ayudar a entender y describir el funcionamiento de los objetos en el mundo real mediante una representación simplificada.

La Norma IEC 61850 realiza estas representaciones utilizando un modelo jerárquico de datos e informaciones definidas mediante conceptos de programación orientada a objeto. La estandarización de un modelo jerárquico de datos permite que la información sea entendida entre los integrantes dentro de un grupo de diálogo, en este caso, entre los dispositivos encontrados en la subestación.

En la figura 11 se puede observar como el estándar IEC 61850, utiliza el concepto de virtualización en la creación del modelo de datos, modelando la información de equipos reales encontrados en las subestaciones, proporcionando una imagen del mundo físico al sistema de automatización de las subestaciones. Este modelo de datos tiene una organización jerárquica, que consta de cinco niveles como se aprecia en la figura, como

ejemplo se aprecia que el (XCBR) representa a un interruptor y el (MMXU) representa una medición eléctrica.

- **El nivel 1**, que corresponde al servidor, es el nivel más alto y representa al dispositivo físico (IED) el cual contiene la información y posee un punto de conexión al mundo exterior a través de la red de comunicación.
- **El nivel 2,** corresponde al dispositivo lógico, permite la subdivisión de un dispositivo físico en varias partes distintas, cada una de las cuales recibe el nombre de dispositivo lógico, esta subdivisión permite la organización de los datos de pendiendo de su aplicación o función, lo cual permite identificar y gestionar los datos más fácilmente. El número de dispositivos lógicos no está definido en la norma, los fabricantes son libres de implementar soluciones particulares.
- **El nivel 3,** es el nodo lógico; el proceso de virtualización, los dispositivos y las funciones de aplicación se descomponen en nodos lógicos, y se organizan al interior de los dispositivos lógicos. Los nodos lógicos corresponden a funciones establecidas en los dispositivos físicas. Todos los nodos lógicos normalizados tienen un nombre de 4 caracteres.
- **El nivel 4**, es el objeto de datos, de acuerdo a su funcionalidad, cada nodo lógico contiene un cierto número de datos, en la norma se define que objeto de datos debe contener cada nodo lógico, y los datos tienen estructura y sintaxis bien definida.
- **El nivel 5**, es el Atributo de datos, cada objeto de datos contiene atributos específicos, los cuales contienen información detallada del valor del objeto de datos. Dado que muchos de los objetos tienen siempre los mismos atributos de datos la norma define las clases comunes de datos, una CDC define que atributos se incluyen en un tipo específico de datos.

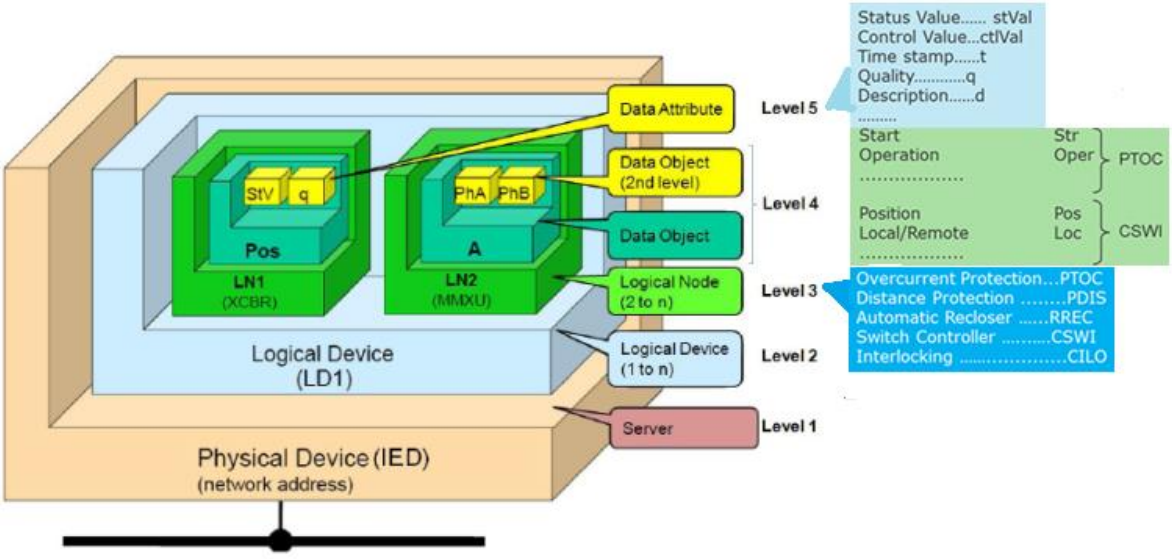


Figura 11: Modelo jerarquizado de las funciones de IED.

1.5.5 Clases genéricas de datos.

Los datos que compones a los nodos lógicos tienen, a su vez distintos atributos asociados. El apartado 7.3 del estándar IEC 61850 define las clases genérica de los datos como estructuras para tipos de datos que comparten la organización y los tipos de atributos, aunque tengan distinto significado.

Clases de valor medido					
Nombre de Atributo	**Tipo de Atributo**	**FC**	**TrgOP**	**Valor/Rango de Valor**	**M/O/C**
Nombre de Datos	clases de datos heredado (IEC 61850-7-2)				
Atributo del Datos					
Atributo de la medición					
insMAg	valor analógico	MX			O
mag	valor analógico	MX	DCHG		M
range	enumerador	MX	DCHG	normal |alto|bajo|alto-alto|bajo-bajo	O
q	calidad	MX	DCHG		M
t	estampado de tiempo	MX			M
Sustitución					
subEna	Booleana	SV			PICS-SUBST
subMag	valor analógico	SV			PICS-SUBST
subQ	calidad	SV			PICS-SUBST
subID	cadena visible 64	SV			PICS-SUBST
Configuración, Descripción y Extensión					
units	Unit	CF		Unidades de medida y múltiplos.	O
db	INT32U	CF		0 … 100000	O
zeroDb	INT32U	CF		1 … 100000	O
rangeC	configuración de rango	CF			GC_CON
magSVC	configuración de la escala del valor	CF			AC_SCAV
angSVC	configuración de la escala del valor	CF			AC_SCAV
angRef	enumerador	CF		V |A| otros …	O

smpRate	INT32U	CF			O
d	cadena visible 255	DC		texto	O
dU	cadena visible 255	DC			O
cdcNs	cadena visible 255	EX			AC_DLNDA_M
cdcName	cadena visible 255	EX			AC_DLNDA_M
dataNS	cadena visible 255	EX			AC_DLN_M
Servicios					
Los siguientes servicios son heredados de la IEC 61850-7-2. Se especializan restringiendo el servicio a atributos con una función especifica					
Modelo de servicio	**Servicio**	**el servicio se aplica a Attr con FC**		**Observaciones**	
Modelo de Datos	SetDataValues	DC, FC, SV			
	GetDataValues	ALL			
	GetDataDefinition	ALL			
Modelo de conjunto de datos	GetDataSetValues	ALL			
	SetDataSetValues	DC, FC, SV			
Modelo del informe	Informe	ALL		El conjunto de datos se utiliza para definir el contenido de reporte	

Tabla 3: Clases genéricas de los datos de medición

1.5.6 Dispositivos lógicos.

El concepto de equipo lógico se introduce por motivos de comunicación entre nodos lógicos. Un equipo lógico es principalmente una composición de nodos lógicos y otros servicios adicionales (GOOSE, ajustes de grupos,...) como se muestra en la figura 12:

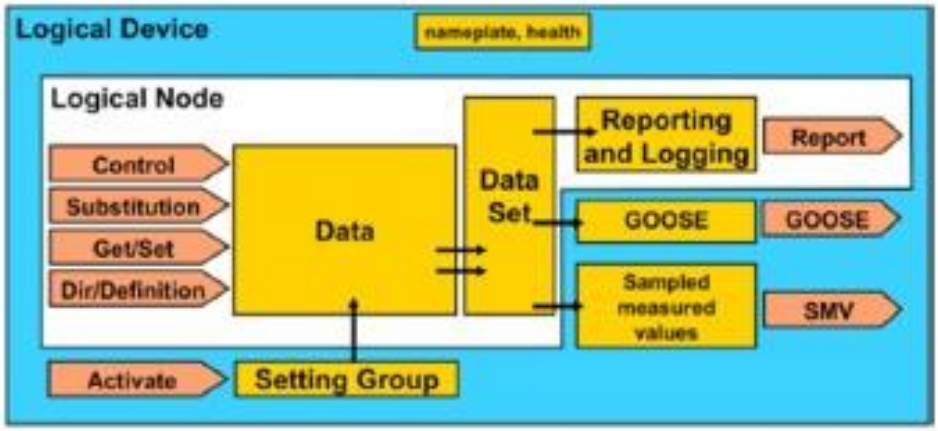


Figura 12: Bloque de un Dispositivo Lógico.

1.5.7 Modelos de servicios Abstractos de Comunicación

En las partes IEC 61850-8 y 9 del estándar se describe un conjunto de modelos y servicios de comunicación con el objetivo de permitir el intercambio de la información del modelo de datos entre los diferentes IEDs. El objetivo es el despliegue de la automatización del sistema eléctrico mediante el envío de agrupaciones de datos de los LN de los diferentes IEDs. En la figura 13 se pueden observar los modelos abstractos y servicios de comunicación definidos en el estándar, todos ellos finalmente mapeados y encapsulados sobre una red física Ethernet.

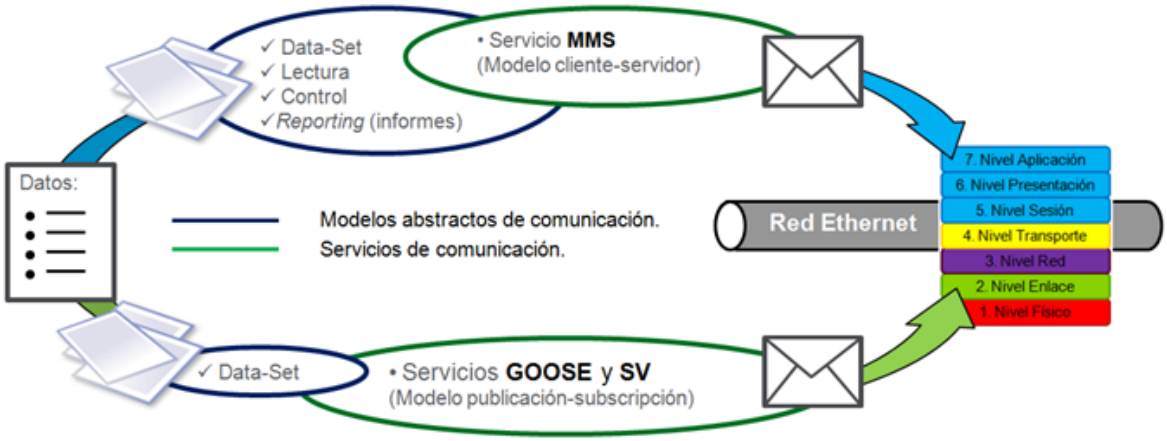


Figura 13: Modelo de Servicio Abstractos de Comunicación.

Los tres primeros modelos forman parte del servicio MMS, basado en el modelo cliente-servidor. El servidor es el equipo que contiene la información mientras que el cliente accede a ella, y los modelos de lectura y escritura se utilizan para acceder a los datos y a sus atributos. El modelo de control es una especialización del servicio de escritura, el cual permite la gestión de atributos que tienen están definidos en esta clase y permiten una acción sobre el equipo final. El modelo de informes se utiliza para el intercambio de un grupo de información orientada a eventos, en la que la información es transmitida espontáneamente cuando el valor del dato es modificado. Hoy en día, todos estos modelos se mapean sobre el protocolo MMS en la capa 7 OSI Ethernet.

El resto de servicios están basados en el modelo publicación-suscripción. En IEC 61850, el término de comunicación punto a punto se introduce para hacer hincapié en que la comunicación entre el publicador y el suscriptor implica una comunicación entre equipos. Estos servicios de comunicación se utilizan para el intercambio de información de carácter crítico. El equipo, que es la fuente de información, publica la misma, y cualquier otro equipo que necesite esta información la puede recibir suscribiéndose a ella. El servicio

GOOSE, Generic Object Oriented Substation Event en inglés, es un servicio de transmisión rápida de información de eventos hacia múltiples equipos. En lugar de utilizar un servicio de comunicación con confirmación de recibo, la información intercambiada es enviada por repetición regularmente asegurándose así la llegada al suscriptor. El servicio de transmisión SV, Sampled Valúe en inglés, es utilizado cuando se necesita transmitir señales analógicas de campo, tales como intensidad, tensión o cualquiera de sus derivados, utilizando comunicaciones digitales. Las señales analógicas son muestreadas y trasmitidas. Tanto el servicio GOOSE como SV se encapsulan sobre capa 2 OSI Ethernet.

1.5.8 Eventos genéricos de la subestación (GSE).

Es el servicio que permite la comunicación de eventos genéricos de la subestación a varios dispositivos IED dentro del sistema, de manera simultánea, rápida y segura. Está relacionado con acciones automáticas que requieran el intercambio de información con una importante restricción temporal. Para poder proporcionar este servicio la norma establece dos bloques de control. El hub, que permite él envió de mensajes tipo GOOSE, basado en un mecanismo proveedor/suscriptor y el GsCB que permite el envío de mensajes GSSE de características similares al GoCB pero con tratamiento de distinto tipo de información.

Este servicio permite la transmisión de valores instantáneos de medidas analógicas, minimizando el tiempo que transcurre desde el muestreo hasta la recepción del mensaje. Para ello se debe de tener en cuenta la disposición física de los dispositivos que van a comunicarse entre sí. Donde se debe conocer bien que los dispositivos se van a comunicar, el tipo de mensaje y los requerimientos de tiempo de estos mensajes. La norma IEC 61850-5 define los tipos de mensaje que van a circular dentro de la red de comunicación y los clasifica según su rendimiento como se muestra en la tabla 4.

Tipo	Nombre	Ejemplo	Desempeño Requerido
1ª	Mensajes Rápidos: TRIP	Disparos	10 ms: Vano de distribución 3 ms: Vano de protección y transmisión
1B	Mensajes Rápidos: Otros	Comandos, interacción con proceso, excepto disparos. Interfaces lógicas 3, 5 y 8	100 ms: Vano de distribución 20 ms: Vano de protección y transmisión
2	Mensaje de velocidad media	Valores r.m.s calculados a partir de señales tipo 4	Menor a 100 ms. La estampa de tiempo del mensaje es importante pero el tiempo de transmisión no es critico
3	Mensajes lentos	Funciones de control lentas, transmisión de registros de eventos, lectura o escritura de ajustes, alarmas, medidas no eléctricas	Menor a 500 ms
4	Mensajes de datos muestreados sin procesar	Datos transductores y transformadores de medida	Protección y control: entre 480 y 1.920 muest/seg Medición: entre 1.500 y 12.000 muest/seg

5	Transferencia de Archivos	Archivos de secuencia de eventos, información, ajuste, etc.	No hay límite de tiempo. Son subdivididos en bloques típicamente de 512 bits para la transmisión
6	Mensajes de Sincronización	Sincronización de tiempo en la red	Precisión de ajuste del reloj interno: ±1ms (eventos) y ±25 μs a ± 1 μs (muestreo)
7	Mensajes de comando con control de acceso	Comandos a partir de una IHM remota o local	Basado en el tipo 3, con procedimientos de seguridad adicional

Tabla 4: Eventos genérico dentro de la subestación según el estándar IEC 61850-6.

Donde podemos mencionar los siguientes eventos en los Sistemas SAS:

- SV: Tipo 4. Mensajes de muestreo de datos. Los mensajes de muestreo contienen información de los valores presentes en un tiempo determinado, por ejemplo, voltaje, corriente, impedancia, etc.
- GOOSE: Tipo 1, 1A. Prioritarios, de alta velocidad. Contienen generalmente funciones con instrucciones de disparo, apertura, cierre, etc.
- MMS: Tipo 2,3y5. Mensajes de mediana y baja velocidad con funciones de transferencia de archivos.

1.5.9 Lenguaje de configuración

El lenguaje de comunicación SCL (Substation Configuration Language), es un lenguaje de descripción para la comunicación de IED's en la Subestación Eléctrica. Es un lenguaje basado en formatos XML que provee una formal descripción de los IED's. Con este lenguaje de comunicación toda la información intercambiada en la red de comunicación de las subestaciones se puede describir y preservar para su utilización en cualquier etapa del ciclo de vida del sistema

La ingeniería de un sistema de automatización de subestaciones puede comenzar ya sea con la asignación de dispositivos pre configurados de forma offline para cambiar partes, productos o funciones, o con el diseño de la funcionalidad de proceso, donde las funciones se asignan posteriormente a dispositivos físicos basándose en capacidades funcionales de dispositivos y Sus capacidades de configuración. A menudo, se prefiere un enfoque mixto: una parte de proceso típica tal como una bahía de línea está prediseñada y, a continuación,

El resultado se utiliza dentro de la funcionalidad del proceso tan a menudo como sea necesario. Para SCL, esto significa que debe ser capaz de describir:

A. Una especificación del sistema en términos del diagrama de una sola línea, y asignación de nodos lógicos (LN) a partes y equipos de la línea única para indicar la funcionalidad necesaria.
B. IEDs pre configurados con un número fijo de nodos lógicos (LNs), pero sin vinculación a un proceso específico. Sólo puede estar relacionada con una parte de función de proceso muy general.

C. IEDs pre configurados con una semántica pre configurada para una parte de proceso de una determinada estructura, por ejemplo, un alimentador de línea GIS de doble barra.
D. Completar la configuración del proceso con todos los IED vinculados a funciones de proceso individuales y equipos primarios, mejorados por las conexiones de puntos de acceso y posibles vías de acceso en subredes para todos los posibles clientes.
E. Como punto d) anterior, pero adicionalmente con todas las asociaciones predefinidas y conexiones de servidor cliente entre nodos lógicos en el nivel de datos. Esto es necesario si un IED no es capaz de crear dinámicamente asociaciones o conexiones de informes (ya sea en el cliente o en el servidor). Caso e) es el caso completo. Ambos casos d) ye) son el resultado después de la ingeniería SAS, mientras que el caso a) es una especificación funcional de la ingeniería SAS, y b) y c) son posibles resultados después de la ingeniería de IED.

El alcance de SCL como se define en esta norma está claramente restringido a estos propósitos:

1) **Especificación funcional SAS** (punto a) anterior),
2) **Descripción de la capacidad de IED** (puntos b) y c) anteriores), y
3) **Descripción del sistema SAS** (puntos d) ye) anteriores)

Con el fin de diseñar el sistema, la ingeniería de comunicación y la descripción de la comunicación del sistema de ingeniería para las herramientas de ingeniería de dispositivos de una manera estandarizada.

1.5.10 Modelo SCL.

El SCL en todo su alcance se describe un modelo de:

- La estructura primaria del sistema: funciones que se utilizan aparatos primarios, y cómo los aparatos están conectados. Esto resulta en una designación de todos a paramenta cubierto como funciones de automatización de subestaciones, estructurado de acuerdo con la norma IEC 61346-1.
- El sistema de comunicación: cómo IED están conectados a subredes y redes, y en cuál de sus puntos de acceso de comunicación (puertos de comunicación).
- La comunicación a nivel de aplicación: ¿Cómo se agrupan los datos en conjuntos de datos para el envío, ¿cómo los IED's desencadenan el servicio de envío y los que lo desean?, que datos de entrada de otros IEDs se necesitan?
- Cada IED: qué dispositivos lógicos se configuran en cada IED, que los nodos lógicos de los cuales clase y tipo pertenecen a cada dispositivo lógico, y que informa con que los datos y que (pre-configurados) asociaciones están disponibles; el cual se registrarán los datos.

- Instanciable nodo lógico (LN) tipo definiciones. Los nodos lógicos definidos en la parte 7 en estándar IEC 61850, tienen los datos obligatorios, optativos y de usuario definidos (externos) (DO), así como servicios opcionales, y por lo tanto no son replicables. En este documento se definen LNTypes instanciables, que contienen como molde el realmente disponible los datos y los servicios.
- Las relaciones entre nodos lógicos instanciados y sus IEDs de alojamiento en un lado y la subestación (función) partes en el otro lado.

1.5.11 Descripción de los tipos de archivos SCL.

El proceso de ingeniería de la subestación exige que el SCL sea capaz de describir la especificación funcional de la subestación, describir las capacidades de los IED que son utilizados y describir el sistema final configurado en todos sus detalles.

El estándar propone dos tipos de tareas a realizar por las herramientas de ingeniería:

- Configurador de IED. Es específico del fabricante y debe ser capaz de importar y exportar ficheros SCL, así como proporcionar los ajustes específicos del IED y generar su fichero de configuración para cargarlo en el IED.
- Configurador del Sistema. Es independiente de los IEDs y debe ser capaz de importar y exportar ficheros SCL. Debe ser también capaz de leer el fichero de especificación del sistema para tomarlo como base del diseño o para compararlo con un diseño realizado.

El lenguaje SCL determina el uso de varios tipos de ficheros durante el proceso de ingeniería. Los principales son:

- ICD (IED Capability Description): describe las capacidades de ingeniería y funcionalidades de un IED sin ninguna configuración concreta. Un IED que cumpla el estándar debe ir acompañado de su ICD.
- SSD (System Specification Description): describe la especificación del sistema con el unifilar, las funciones de la subestación y los nodos lógicos que se necesitan.
- SCD (Substation Configuration Description): describe el conjunto del sistema configurado con la información de los IEDs configurados, el subsistema de comunicaciones y la descripción de la subestación.
- CID (Configured IED Description): describe la configuración completa de un IED dentro del proyecto concreto y toda la información necesaria para que el "Configurador de IED" lo cargue sobre el IED.

1.5.12 Estructura del Estándar

El Estándar IEC 61850 es considerado el estándar por excelencia para la automatización de equipos de Subestaciones Eléctricas de diversos fabricantes; fue diseñado como el único protocolo ofrece una completa solución de comunicación para Subestaciones Eléctricas y la principal característica que ofrece es la interoperabilidad entre los equipos. En la actualidad se vienen realizando investigaciones de diferentes grupos de trabajo que pertenecen al Comité Técnico (TC57), para la constante evolución del estándar.

En la figura 14, observamos la estructura del protocolo IEC 61850, en la cual podemos observar las partes del estándar, con las características más relevantes de cada parte.

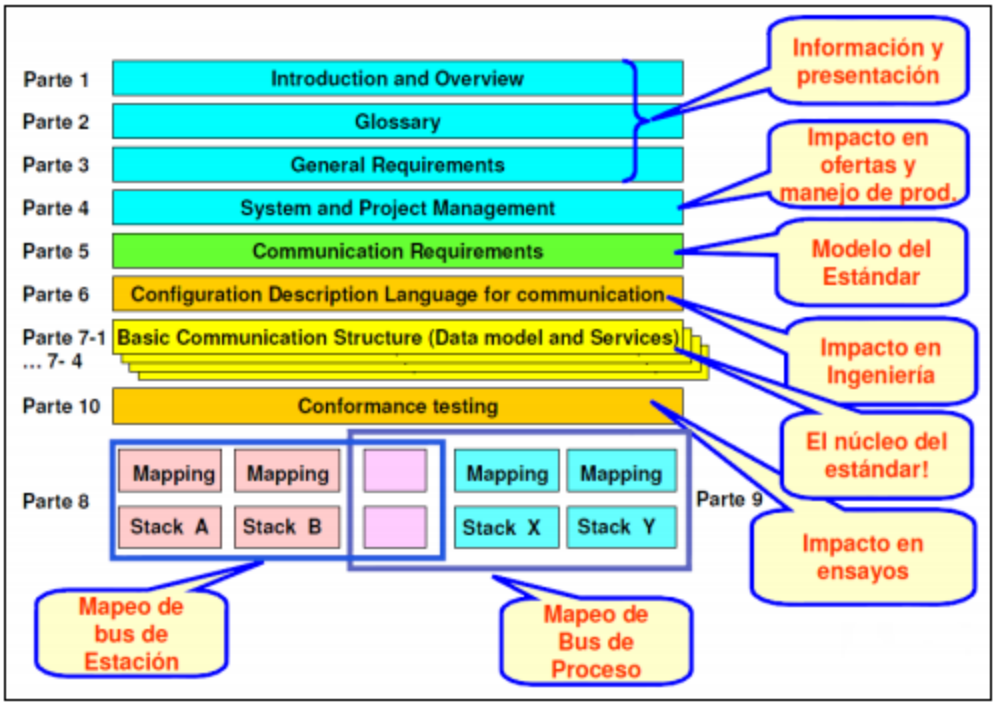


Figura 14: Estructura del Estándar IEC61850.

CAPÍTULO II

Las diez mejores prácticas para el diseño de un sistema comunicación en la subestación bajo el Estándar IEC– 61850

2.0 Introducción

Durante los últimos años, dos tendencias han convergido que han causado muchas utilidades para reevaluar su infraestructura de comunicaciones de la subestación. Una tendencia es la migración de la red eléctrica de un sistema fiable, pero inflexible a la "red inteligente", que promete adaptabilidad y eficiencia. También se requiere la comunicación bidireccional de datos, algo que no es posible con las redes eléctricas tradicionales.

La otra tendencia es la creciente adopción por parte de la industria de las tecnologías de red Ethernet para sus comunicaciones. Donde se estima que la adopción de la industria que las redes Ethernet está creciendo a un> 12 por ciento más TACC (compuesta de crecimiento anual).

Como resultado de estas tendencias, muchos servicios públicos se enfrentan a tener que diseñar y poner en práctica infraestructuras de comunicaciones que son diferentes a cualquier cosa que han participado antes.

Este documento, le guiará a través de cada una de las mejores prácticas, lo que explica la importancia de cada uno de ellos y proporcionar orientación sobre la forma de aplicarla a sus necesidades.

2.1 Segmento de redes operativas

Una forma de aumentar el rendimiento y evitar la saturación de la red es la utilización de VLANs (Red de Área Local Virtual) y el QoS (Calidad de servicio) para garantizar la entrega de mensajes en caso de congestión. Separar el tráfico de mensajes en VLANs permite disminuir el dominio de colisión y el dominio broadcast de manera a minimizar el peligro de congestión de la red. Por ejemplo, separar los mensajes GOOSE de protección en una VLAN y los de control en otra VLAN. El QoS es un conjunto de requisitos de servicios que la red debe cumplir para asegurar un nivel de servicio adecuado para la transmisión de los datos.

Segmentar una red consiste en dividirla en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento, tomando en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo.

Un segmento es un bus lineal al cual están conectadas varias estaciones. Las características son:

- Cuando se tiene una red grande se divide en trozos llamados segmentos.
- Para interconectar varios segmentos se utilizan bridges o routers.
- Al dividir una red en segmentos, aumenta su rendimiento.
- A cada segmento y a las estaciones conectadas a él se le llama subred.

Cuando se segmenta una red, se están creando subredes que se auto gestionan, de forma que la comunicación entre segmentos solo se realiza cuando es necesario, mientras tanto, la subred está trabajando de forma independiente.

El dispositivo utilizado para segmentar la red debe ser inteligente, ya que debe ser capaz de decidir a qué segmento va a enviar la información que llego a él. Se pueden utilizar hubs, repetidores, bridges, routers, gateways.

La segmentación de una red se hace necesaria cuando:

- Se va a sobrepasar el número de nodos que la topología permite.
- Mejorar el tráfico de una red.

2.1.1 Segmentación física.

No disponer de dispositivos que permitan el acceso seguro a la red OT, no configurarlos correctamente, desplegarlos con configuraciones por defecto y/o la falta de políticas de segmentación de red, hacen que los equipos, procesos y sistemas ubicados en el entono de operaciones sean más vulnerables a amenazas tanto externas como internas.

Es por ello que la incorporación de dispositivos que fortifiquen el acceso perimetral y la correcta segmentación de redes, sea unas de las contramedidas básicas que deben considerarse dentro de una estrategia de defensa en profundidad.

En la figura 15 se observa cómo los entornos IT (normalmente niveles 4 y 3 según la normativa ISA95) y OT (niveles 1 y 2) están comunicados por varios switches, pero todos los equipos se encuentran en el mismo rango de direcciones IP (el 192. 168.1. X).

Para reducir o eliminar esta vulnerabilidad se suelen implantar diferentes dispositivos o mecanismos que persiguen justo eso, segmentar y/o fortificar las redes industriales. Entre estos destacan los routers con listas de control de acceso, los switches inteligentes, los firewalls, la creación de DMZs (zona desmilitarizada). A partir de la arquitectura representada en la figura 15, a continuación se presentan varias alternativas para conseguir que las redes IT y OT queden segmentadas y fortificadas mediante el despliegue de algunos de estos dispositivos.

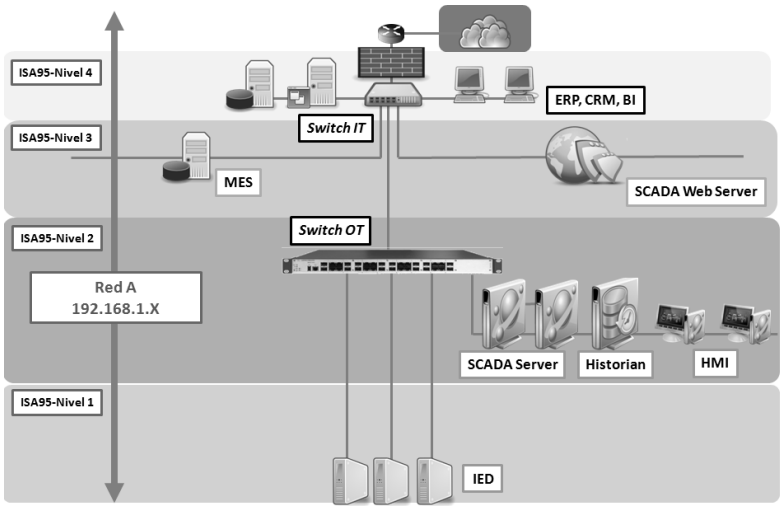


Figura 15: Arquitectura de la segmentación física con zona desmilitarizada.

La primera opción que se propone para segmentar ambas redes es la inclusión de un firewall que además permita encaminar tráfico entre las redes IT y OT. Un firewall es un dispositivo que monitoriza y controla el tráfico que fluye entre dos redes. Intercepta el tráfico no autorizado comparando cada unidad de información (paquete, segmento, datagrama o trama, dependiendo del nivel al que trabaje) con una serie de reglas predefinidas.

En la figura 16 se observa cómo entre la red A, IT (192.168.1.X) y la red B OT (193.167.1.X), se ha creado una red intermedia, la DMZ, con su propio rango de direcciones IP (202.168.1.Y). En esta red intermedia se ubican las aplicaciones y/o información que es necesario que sea compartida por los usuarios de las redes IT u OT (las soluciones MES o un Historian-Replicado para que los datos de proceso sean accesibles desde IT) o los servidores que deben estar accesibles desde el exterior (SCADA Web Server).

Para fortificar los niveles 1 y 2, es decir, para proteger el proceso y posibles ataques a los dispositivos de control, se incluyen lo que se denominan Firewalls industriales DPI (Deep Packet Inspection). Como se aprecia en la figura 16, este tipo de firewalls se ubican entre los sistemas SCADA y los IEDs asegurando su disponibilidad y por tanto la del proceso. El hecho de que realicen DPI significa que permiten segmentar tráfico especificando protocolos típicamente industriales (Modbus TCP/IP, Ethernet IP, OPC, etc.). Además, se pueden configurar reglas de acceso teniendo en cuenta dicho protocolo. Por ejemplo, si el protocolo utilizado es Modbus TCP/IP es posible definir una regla que no permita a un maestro ejecutar las "function codes" 05 "write cole" y 06 "write register" sobre un esclavo. O si se utiliza OPC para comunicar, el firewall es el responsable de asignar un único puerto sobre OPC para realizar comunicaciones seguras entre clientes y servidores

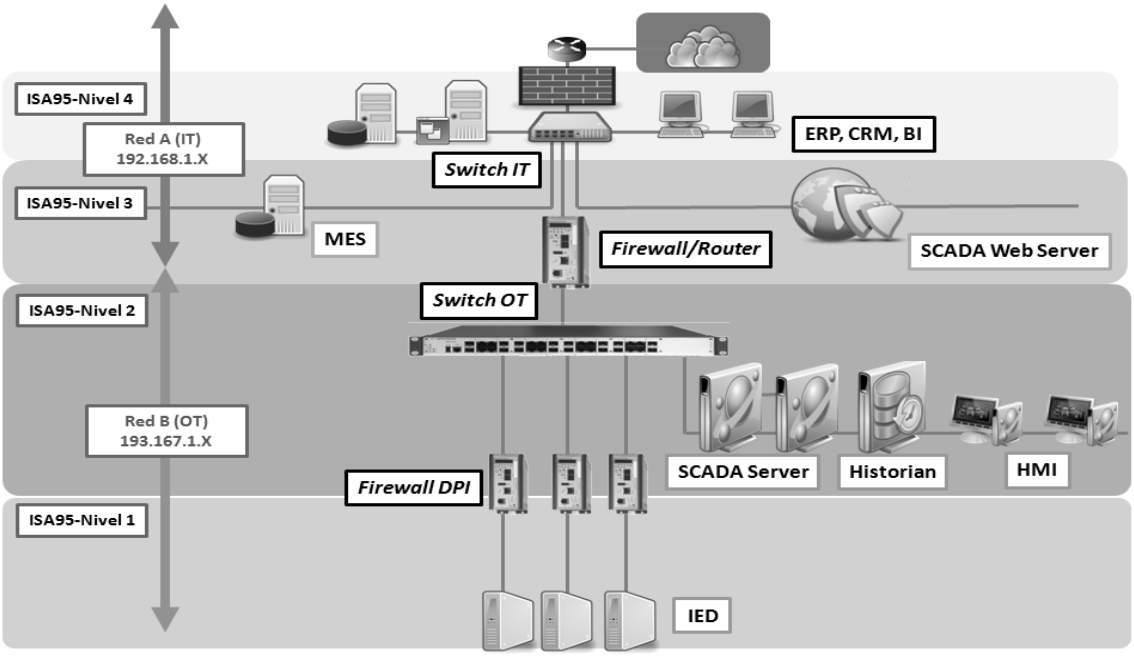


Figura 16: Arquitectura con firewalls ubicados entre los sistemas SCADA y los IEDs asegurando su disponibilidad y el proceso.

2.1.1.1 Tipos de segmentación física

Para realizar las tareas de supervisión, maniobras y control llevado a cabo por las labores diarias de los operadores, relacionado con la subestación, tales como: control local de la subestación, comunicación, y manejo de datos.

Es en el nivel de control de subestación donde se encuentra el protocolo de comunicación IEC-104 para enviar las telemetrías y ofrecer los servicios de seguimiento y control de las subestaciones eléctricas.

2.1.1.2 Segmentación mediante el Estándar IEC-104 (VSAT).

El ambiente de las subestaciones eléctricas manejaba el control bajo las premisas de redes seriales en protocolos RS-485 para utilizar buses de control que permitían la integración de los equipos a un centro de recopilación de datos como lo son las RTU para su posterior retransmisión al SCADA. Este tipo de control ha venido variando con el tiempo, y debido a las necesidades de las atenciones vía redes de los inconvenientes que se puedan presentar dentro de las operaciones cotidianas de las subestaciones eléctricas.

Esto permite entonces la entrada de equipos de conmutación de paquetes y el protocolo IEC -104 que trabaja bajo ambiente TCP/IP para que surjan dentro de las subestaciones eléctricas conexiones remotas para configuración de equipos y redes más rápidas para el control basadas en fibra para dar un mayor nivel de seguridad en caso de perturbaciones eléctricas o sobre corriente que forman parte del día a día en una subestación.

Donde IEC 60870-5-104 (IEC 104) es una extensión del protocolo IEC 101 con cambios en los servicios de la capa de transporte, de la capa de red, de la capa de enlace y de la capa física para satisfacer la totalidad de accesos a la red. El estándar utiliza la interfaz de red TCP/IP para disponer de conectividad a la red LAN (Red de Área Local) con routers con diferentes protocolos de enrutamiento (RDSI, X.25, Frame relay, etc.) también se puede usar para conectarse a la WAN (Wide Area Network). La capa de aplicación IEC 104 se conserva igual a la del IEC 101 con algunos de los tipos de datos y los servicios no utilizados

Generalmente para los sistemas de energía se utiliza el protocolo IEC 104 para el centro telecontrol y el protocolo IEC 101 para la interacción con las remotas de campo. El protocolo TCP se utiliza para garantizar la confiabilidad de los datos que son de vital importancia debido a que la respuesta y la interacción entre el SCADA y los sistemas de control de las subestaciones de transmisión requieren la mayor rapidez y eficacia posible, debido a que las operaciones son medidas en milisegundos. Como ya se ha explicado, el protocolo IEC-104 maneja una diversidad de datagramas y estilos de transmisión que pueden ser aprovechados para el envío de los datos, para un medio de transporte particular en el caso a tratar, este medio de transporte viene siendo soportado por sistemas satelitales particularmente por el servicio de redes VSAT el cual será explicado a continuación.

Vsat “very small aperture terminal” es una terminal de apertura muy pequeña que brinda servicios fijos por satélite (geoestacionario), utilizada para la comunicación de datos interactivos y por lotes en diversos protocolos, operación de redes con conmutación de paquetes, servicios de voz, transmisión de datos y videos y operación en red en una vasta área, y entre sus principales características se tienen:

- No requieren disponer de infraestructura previa.
- Soportan aplicaciones multimedia integradas en PC (voz, datos, imágenes).
- Interconexión de redes locales, comunicaciones de voz/fax, vídeo conferencias /transmisión de imágenes, etc.
- La calidad y disponibilidad del enlace vía satélite son muy superiores a los medios tradicionales de comunicación.

En la figura 17 se demuestran los diferentes elementos que participan en el funcionamiento de las redes VSAT:

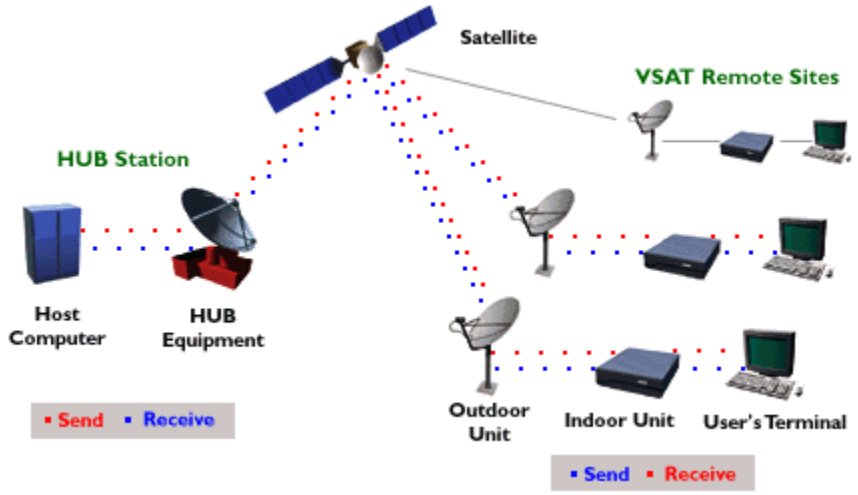


Figura 17: Segmentación Vsat.

La estación terrena VSAT, está compuesta por dos elementos: Unidad Exterior (Outdoor Unit), que es el interfaz entre satélite y VSAT y la unidad Interior (Indoor Unit), que es el interfaz entre el VSAT y el terminal de usuario o LAN. Básicamente la Unidad Exterior se compone de una antena, sistemas electrónicos, amplificadores de transmisión, sintetizador de frecuencia, dúplex, amplificador de potencia, etc.

Los parámetros necesarios en la Unidad Interior son los números, tipos y velocidad de los puertos, se componen a su vez de dos segmentos muy particulares para poder trabajar, estos segmentos se encuentran por lo general en los sistemas satelitales y se conocen como segmento espacial y segmento terreno.

Es el único canal por donde se realiza la comunicación con las consiguientes ventajas y desventajas que conlleva. Es un canal compartido por lo que necesitaremos usar alguna técnica o protocolo de acceso al medio (FDMA, TDMA, DA-TDMA). Es el único punto de la red que no puede ser manejado con total libertad por el instalador de una red VSAT. Debe ser contratado a empresas o consorcios proveedores de capacidad espacial.

Entre sus desventajas podemos mencionar que se necesitan antenas grandes para trabajar con la misma, de 1 a 3 metros, y que es susceptible de recibir y causar interferencias desde satélites adyacentes y sistemas terrestres que compartan la misma banda (Se necesitaría en algunos casos recurrir a técnicas de espectro ensanchado y CDMA).

Visto que las redes Vsat permiten la transmisión de telemetrías de control y monitoreo, y además tomando en cuenta la necesidad creciente de supervisión de las subestaciones eléctricas, en el caso particular de subestaciones de locaciones foráneas donde se hace de difícil acceso la entrada de medios de comunicación como la fibra óptica o las microondas, basamos una propuesta de un sistema de transmisión bajo el protocolo de comunicación IEC-104 de tipo desbalanceado, lo cual permitirá la interrogación de múltiples locaciones hacia un centro remoto utilizando la topología estrella bajo el servicio TDM/TDMA.

Un sistema desbalanceado permitirá optimizar recursos a nivel de transmisiones de datos en la red, el maestro es el SCADA quien se encarga de interrogar a cada uno de los esclavos mediante direcciones ASDU que vienen empaquetadas en el protocolo TCP por medio del IEC 104 y son predefinidas para el canal de comunicación particular que va a interrogar.

Por otro lado a nivel de la estación remota es necesario que se establezca la misma dirección ASDU para que exista la interrogación, además se debe mencionar que la mayor carga de datos a la red será enviada para el inicio de la comunicación, ya que en este momento se realiza una interrogación general desde el centro maestro para poder conocer cada una de las alarmas y las condiciones generales de la subestación.

Una interrogación periódica que sólo envía 1 byte de datos para asegurar que la remota sigue transmitiendo y así no ser declarada fuera de servicio. Esto se hace fundamental ya que las remotas deben tener un 99.99% de disponibilidad debido a que manejan operaciones importantes dentro de una subestación.

En el concepto de que las redes de servicios VSAT bajo TDMA poseen un centro de monitoreo central, que interroga a las demás estaciones remotas, o pequeñas VSAT, lo cual permitiría centralizar la información de múltiples subestaciones a un centro de control particular para realizar el control y monitoreo de las telemetrías requeridas.

Para algunos casos y debido a que algunas remotas se encuentran en protocolo IEC-101 el cual básicamente tiene salidas de conexión serial, bien sea RS-232 o RS-485 se necesitarán convertidores de protocolo que existen en el mercado actualmente que se encargan de agregar la capa de transporte al IEC-101 mediante el protocolo TCP pasando así a ser protocolo IEC-104 los mismos entregan una salida Ethernet que puede ser conectada a las IDUs para de ésta manera lograr la interrogación del centro de control.

Lo importante de establecer conexiones mediante el protocolo TCP es que las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Todas estas aplicaciones son de suma importancia en las subestaciones eléctricas debido a que garantizan seguridad de datos que necesitan ser entregados con un alto nivel de fiabilidad, además de brindar la posibilidad de la segmentación que es de suma importancia debido al costo de los enlaces satelitales.

En resumen, la cantidad de equipos necesaria para la transmisión de los datos y garantizar las comunicaciones de las redes VSAT para llevar la información de las subestaciones eléctricas es la siguiente:

- HUB central de monitoreo.
- Estaciones remotas VSAT con antenas de al menos 2.4 metros
- IDUs con puertos Ethernet.
- Convertidores de protocolo IEC-101 – IEC-104 para el caso de las subestaciones que lo requieran.

Como se ha visto es posible establecer interrogaciones de las remotas hacia las subestaciones foráneas, donde no es posible llevar medios de comunicación convencionales, mediante las redes VSAT, se podrá incrementar el nivel de supervisión de este tipo de subestaciones, aumentado de esta manera la calidad de servicio prestado por las empresas eléctricas e incrementando la capacidad de respuesta ante fallas lo cual es de suma importancia para mejorar el negocio y la rentabilidad del mismo.

2.1.1.3 Segmentación Celular.

Con el crecimiento continuo de la Iniciativa de la Red Inteligente, muchas compañías eléctricas están buscando nuevos enfoques para conectar subestaciones remotas, fuentes de energía renovables y su distribución automatización en una red segura y común. Aunque una red de comunicaciones de fibra óptica, la primera opción para conectar estas instalaciones a un lugar central de control y monitoreo, debido a su inherente La conectividad segura y la inmunidad de los niveles severos de EMI típicamente encontrados dentro de la conexión eléctrica, ambiente ruidoso de una subestación, o la proximidad cercana de las líneas eléctricas trifásicas de alto voltaje de alto voltaje, la distribución, el gasto, los problemas de derechos de paso y la dificultad de construir la infraestructura de fibra para distantes y ampliamente separadas es a menudo prohibitivo y no práctico.

Administrar y acceder a equipos remotos en muchos lugares físicamente diversos puede ser costoso y difícil, Junto con la obvia necesidad de maximizar el tiempo de actividad del sistema de transmisión y distribución de confiabilidad de la entrega de energía, mientras que reduce costes de funcionamiento y de mantenimiento. Estos requisitos son una consideración para muchas utilidades.

Frente a las crecientes expectativas de servicio al cliente ya la creciente supervisión del desempeño del sistema, como problemas cada vez mayores de interferencia que afectan a sus servicios de radio y servicios inalámbricos existentes, muchas subestaciones SCADA, La automatización de la distribución y los ingenieros de medición a distancia están viendo

los routers celulares como una alternativa viable A los populares enlaces de radio desplegados para su uso en los 900 MHz (servicio licenciado y sin licencia), 3,6 GHz y 5 GHz, así como enlaces de radio de microondas o de telefonía por cable T-1 / DS-1 y E-1.

Con el advenimiento de enrutadores celulares compatibles con la categoría IEC 61850-3 y con clasificación de subestación, ahora se convierte práctico y rentable para proporcionar una comunicación sencilla de implementar, fiable y altamente segura Red SCADA, las instalaciones de generación de energía renovable, la red de distribución, la red de automatización y la medición remota a la central de control y monitorización de la compañía.

Un enrutador celular es un dispositivo de red de comunicaciones para el enlace ascendente de datos Ethernet o una combinación de Ethernet y RS-232 y RS-485, a través de una WAN de radio celular cifrada de banda ancha (Wide Area Red) a la PSTN (Red Telefónica Pública Conmutada), a través del teléfono celular 2G / 3G o 4G LTE seleccionado por el usuario proveedor de servicio. Además de la radio celular interna, estos dispositivos pueden incluir una combinación de una capa 2. Así como un enrutador de capa 3 con un firewall seguro para la protección contra la posibilidad de una infracción de seguridad cibernética o intrusión en la red. La capacidad de datos seriales es deseable para aquellas aplicaciones donde las RTUs, IEDs, medidores, relés de protección, registros de datos u otros equipos terminales deben ser Sin conexión a la red, sin necesidad de una unidad de servidor terminal externa. Una fibra óptica Interfaz que utiliza transmisores ópticos SFPs (Small Form-Factor Pluggable) instalables en el campo, para Una conexión altamente versátil y resistente al futuro a cualquier planta de cable multimodo o mono modo, para uso como El circuito de comunicaciones de conmutación primaria o secundaria en el caso de una pérdida del enlace de radio celular.

Muchos operadores de sistemas, particularmente aquellos con subestaciones ubicadas remotamente, tienen la capacidad de proporcionar fibra óptica con el enrutador celular a través de una red óptica existente como se observa en la figura 18. El enlace de fibra óptica se utiliza generalmente como el camino de comunicaciones primario entre la subestación y el control de cabecera de la utilidad y el monitoreo instalaciones. En el caso de un fallo dentro de la planta de cable óptico, se produce un fallo automático al enlace de radio celular, proporcionando un nivel extremadamente alto de tolerancia a fallos, y reduciendo significativamente la posibilidad de un solo punto de falla dentro de la red de crear una pérdida completa de comunicaciones entre la subestación SCADA, equipos y cualquier otro lugar.

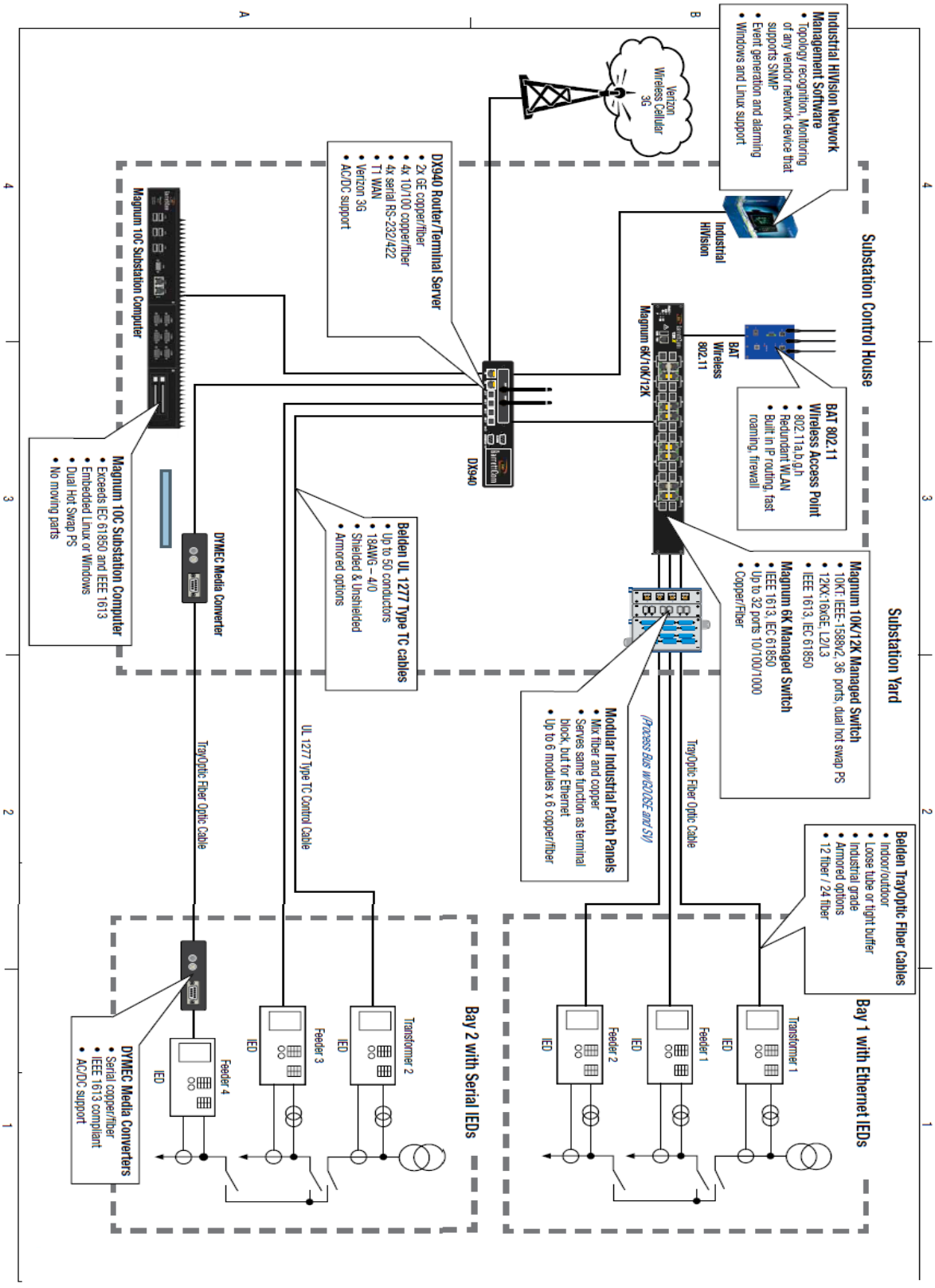


Figura 18: Segmentación Celular.

Para niveles aún más altos de disponibilidad y fiabilidad de la red, algunos routers celulares pueden estar equipados con dos tarjetas SIM (Subscriber Identity Module), para operar con dos proveedores de servicios celulares distintos. Por si la comunicación primaria experimentar un fallo, en los servicios celulares de la red del proveedor primario, el router cambiará automáticamente al proveedor secundario de servicios. Así se mantiene las pérdidas de conexión mínima a cero en WAN celular.

2.1.2 Segmentación Virtuales redes de área local (VLAN).

En una red de área local (LAN), todas las estaciones de trabajo conectadas a un mismo switch, o a un grupo de switches conectados entre sí, comparten el mismo dominio de difusión. Esto hace que cualquier paquete de difusión enviado a la LAN es replicado en todos los puertos del switch o grupo de switches. Este hecho hace que el rendimiento de la red baje considerablemente debido al uso del ancho de banda para el envío de los mensajes de difusión.

Es muy habitual que dentro de una misma LAN (dominio de difusión) haya usuarios pertenecientes a distintos grupos de trabajo (Medición y Protección). Normalmente los mensajes de difusión sólo incumben a los dispositivos pertenecientes a un mismo grupo de trabajo. A cada usuario le llegan mensajes de otros grupos de trabajo que no le incumben, y que usan un ancho de banda que no puede ser aprovechado para enviar otros mensajes.

Al igual que en subredes, conmutadores de nivel 3 y routers se utilizan para configurar y hacer cumplir la VLAN, lo que limita los datos dentro y fuera de la VLAN. Dispositivos de múltiples VLAN pueden conectarse a un interruptor, y los dispositivos en la misma VLAN puede facilidad comuniquen entre sí.

Como puede verse en la siguiente figura 19, hay dos formas de solucionar estos problemas:

- Utilización de routers: El router es un dispositivo que aísla dominios de difusión, es decir, los mensajes de difusión de una LAN no son propagados más allá del router.
- Implementación de redes de área local virtual de (VLANs)

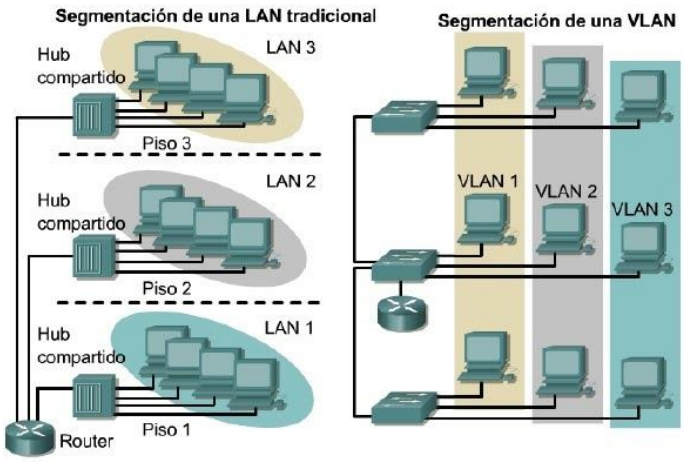


Figura 19: Comparación de una segmentación tradicional y con un segmentación VLAN

Una VLAN está formada por un grupo lógico de estaciones, físicamente unidas a uno o más switches, y que se gestionan como una subred. Cada estación sólo puede comunicarse con otras estaciones de su grupo. Aunque una estación puede pertenecer a m de un grupo.

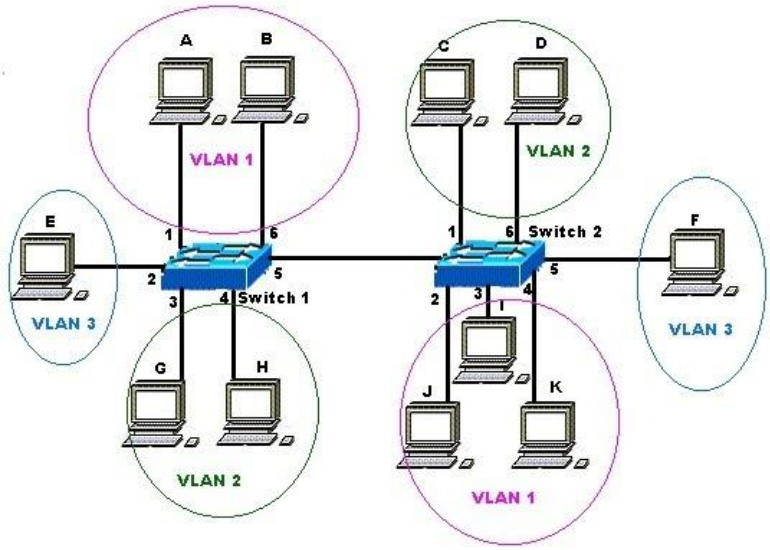


Figura 20: Comunicación entre subredes que pertenecen a diferentes grupos.

Las principales ventajas que aporta una VLAN son:

- Mejora en la velocidad de la red al optimizar la gestión de los puertos.
- Gestión más eficaz del ancho de banda de la LAN.
- Aumento de la seguridad de la red.

2.1.2.1 Tipos de VLANs.

Existen varias formas de establecer una VLAN dependiendo de la forma de agrupar los nodos de la red:

- **VLAN estáticas** o basadas en agrupación por puertos: La asociación de nodos se realiza a los puertos del switch. Cada VLAN incluye los equipos conectados a puertos concretos de cada switch. Es sencilla de implementar (funciona a nivel físico), pero dificulta las labores de administración, ya que cambiar un equipo de puerto o de switch implica reconfigurar la VLAN a la que pertenece el nuevo puerto.
- **VLAN dinámicas basadas en agrupación por direcciones MAC**: Los nodos se agrupan lógicamente especificando su dirección MAC. Cada VLAN incluye los equipos cuya dirección MAC pertenece a un conjunto de direcciones MAC, con independencia del puerto del switch al que estén conectados. Mejora la seguridad de la red y si se cambia un equipo de puerto la red sigue funcionando sin tener que modificar la configuración del switch, pero cada vez que se sustituye un equipo por otro hay que incorporar la dirección MAC de la nueva

tarjeta en la configuración de la VLAN aumentando el trabajo de administración.

- **VLAN dinámicas basadas en agrupación por tipo de protocolo**: El campo Ethertype de la trama Ethernet especifica que protocolo de nivel superior está encapsulado en la carga útil de la trama. Se pueden segmentar la red en VLANs de acuerdo al tipo de tráfico que transmite cada una de ellas (por ejemplo, una VLAN puede encargarse del tráfico IP y otra del tráfico IPX).
- **VLAN dinámicas basadas en agrupación por direcciones IP**: Los nodos se agrupan según su dirección IP. Cada VLAN corresponde a un conjunto de direcciones IP. Es similar a las VLAN por direcciones MAC, pero permite una administración más flexible ya que las direcciones IP no son exclusivas de cada equipo. Para crear este tipo de VLANs son necesarios switches que trabajen a nivel 3 de red de la arquitectura de comunicaciones. Este tipo de switches son más caros.

La distribución de las tramas a la VLAN adecuada se realiza mediante el etiquetado de cada trama con un identificador indicando la VLAN a la que va destinada. En las VLAN estáticas (basadas en la agrupación por puertos), los switches relacionan cada uno de sus puertos VLAN-aware con la VLAN que interconecta. Cuando un switch recibe una trama, lee el campo de la etiqueta de VLAN y lo compara con los identificadores de VLAN que tiene asociados a cada uno de sus puertos, distribuyendo la trama por el puerto correspondiente. En ningún caso reenviará la trama por el resto de los puertos.

En una red de área local pueden coexistir elementos de interconexión VLAN-aware con VLAN- unaware y dependiendo de dichos elementos, los enlaces entre ellos pueden ser de dos tipos:

- **Enlace trunk**: Es un enlace entre dispositivos VLAN-aware; es decir, dispositivos que soportan VLANs. Los enlaces trunk se utilizan en la conexión de switches VLAN-aware y en la conexión de un switch con el router. El enlace trunk o troncal, como puede verse en la figura, encamina el tráfico de todas las VLANs implementadas en el dispositivo VLAN-aware proporcionando un método eficaz para distribuir la información a otros dispositivos como se observa en la figura 21.

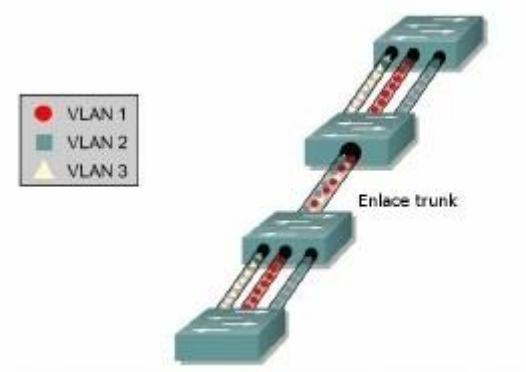


Figura 21: Enlace Trunk

- **Enlace de acceso**: Un enlace de acceso conecta un dispositivo VLAN-aware con otro VLAN- unaware; es decir, es un enlace entre un dispositivo que soporta VLANs y otro que no. Los enlaces entre un switch y los equipos conectados a él son también enlaces de acceso. Cuando se tiene una red de área local en la que existen enlaces trunk y enlaces de acceso, se dice que es una red de área local de enlaces híbridos, como se observa en la figura 22.

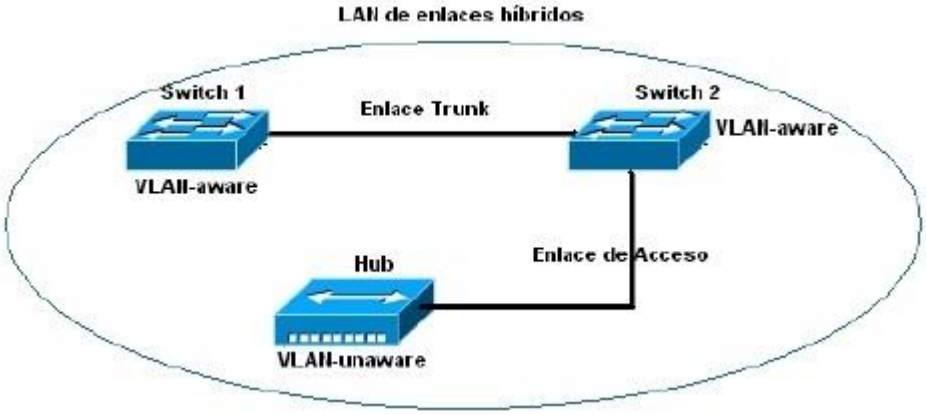


Figura 22: Enlace de Acceso

Si en una VLAN existe un enlace de acceso, todas las estaciones finales conectadas al dispositivo VLAN-unaware sólo pueden pertenecer a la misma VLAN a la que pertenece el puerto por el que se conecta el dispositivo a la LAN, puesto que el elemento de interconexión al que están conectados no permite la división en VLANs al ser VLAN-unaware.

En la red de la figura 23, todas las estaciones del switch 3, únicamente pueden pertenecer a la VLAN1, puesto que el puerto 3 del Switch2 está definido como perteneciente a la VLAN1 al ser un elemento VLAN-aware. Todas las estaciones del Switch 3 (VLAN-unaware) deben pertenecer a la misma VLAN puesto que sus puertos no entienden de VLANs.

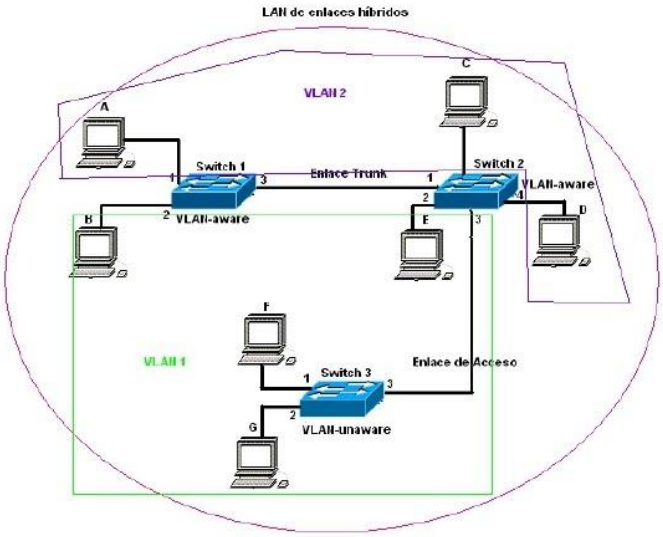


Figura 23: Segmentación virtual mediante VLANs

En la red anterior, la VLAN1 y la VLAN2 están en la misma red de área local, pero separadas una de otra de forma lógica, es decir, las estaciones de la VLAN1 no pueden conectarse con las de la VLAN2, salvo que se utilice un elemento de interconexión de nivel 3 o de red, es decir, un router.

2.1.2.2 Pautas para la configuración de VLANs

A continuación, se desglosan las distintas acciones que se deben realizar a la hora de configurar VLANs en una red de área local:

1. **Identificar el número de VLANs que se quieren crear**. El número máximo de VLANs depende del switch.

2. **Determinar cuántos y cuáles son los equipos que pertenecerán a cada VLAN**. En caso de trabajar con VLANs estáticas habrá que indicar los puertos que se usarán para cada VLAN. Si se trabaja con VLANs dinámicas basadas en agrupación por dirección MAC habrá que determinar las direcciones MAC de los equipos pertenecientes a cada VLAN.

3. **Si fuera necesario, establecer cuál será el puerto del switch que se usará para enlace trunk.**
4. **Conectar físicamente los dispositivos de la red.**

- Conectando el switch en modo consola, realizar las siguientes acciones:
- Implementar las políticas de seguridad: Creación de diferentes usuarios
- Asignación de dirección IP al switch (Esto permitirá acceder de manera remota a través de Telnet, SSH o HTTP)

5. **Configurar las VLANs en el switch** siguiendo los siguientes pasos:

- **Paso 1.** Añadir, modificar o eliminar las VLAN que se deseen configurar. Hay que tener en cuenta que, por defecto, el switch tiene ya una VLAN llamada VLAN administrativa (VLAN1) a la cual se le asignan todos los puertos del switch. Y a ésta deberán de estar conectados todos los dispositivos que quieran, mediante acceso remoto, acceder a un terminal del switch.
- **Pasó 2**. Indicar los equipos que pertenecen a cada VLAN. Si se está definiendo una VLAN estática habrá que asignar puertos a las VLANs. Dado que por defecto todos los puertos están asignados a la VLAN1, sólo se deberán asignar puertos a las demás VLANs. En caso de tratarse de VLANs dinámicas basados en agrupación por direcciones MAC habrá que indicar las direcciones MAC correspondientes a cada VLAN.
- **Paso 3.** Configurar un puerto trunk para a partir de su conexión con un router permitir la interconectividad entre VLANs

6. **Configurar las VLANs en el route**r. El switch aísla totalmente una VLAN de otra, por lo que se necesita conectar el switch con un router para poder interconectar a las VLANs entre sí:

- Confirmar que se ha especificado un puerto trunk en el switch (ya se ha hecho en el apartado anterior).
- Especificar en una interface del router tantas subinterfaces como VLANs se quiera interconectar.
- Conectar físicamente mediante cableado el puerto trunk del switch con el puerto del router.

7. **Configurar los equipos pertenecientes a VLANs** Aparte de configurar switches y router, también se deben configurar los equipos conectados a las VLANs. En cada equipo se debe asignar:

- La dirección IP. Se debe tener en cuenta que la dirección IP debe estar en la misma subred que la dirección IP del subinterfaz correspondiente del router, y que diferentes VLANs corresponden a diferentes subredes.
- La máscara de red o subred.
- La puerta de enlace debe indicar la subinterfaz correspondiente de router.

Nota: Las acciones 1 a 6 pueden realizarse conectándose al switch mediante Telnet, SSH o HTTP, asegurándose de que la conexión se realiza a través de un equipo que está conectado a un puerto que, una vez configuradas las VLANs, seguirá perteneciendo a la VLAN1, ya que si no fuera así se perdería conectividad cuando el puerto se asignara a otra VLAN.

8. **Para comprobar la configuración de las VLANs** se pueden realizar las siguientes pruebas:

- Si se conectan dos PCs a puertos que pertenecen a la misma VLAN y se hace un ping, ambos responden.
- Si se conectan los dos PCs en puertos que pertenecen a diferentes VLANs y se hace un ping no responden (se ha perdido la conectividad).
- Si se intenta realizar un ping o un acceso remoto (a través de Telnet, SSH o http) al switch desde un puerto que no pertenezca la VLAN 1 no se consigue respuesta debido a que el switch no puede dar conectividad entre VLANs.

Nota: Los comandos específicos que se utilizarán para realizar estas acciones dependen de los modelos de switch y router de los que se disponga.

2.2 Agregar dispositivos de comunicaciones serie a Ethernet Infraestructura

Las redes de comunicación dentro de la subestación típica pueden dividirse en dos grupos clave: El subsistema SCADA (Supervisión y Adquisición de Datos), utilizado para la interconexión de todos los IED de la subestación (Intelligent Electrical Devices) y RTUs (Remote Terminal Units), tales como equipos de medición, control y protección de retransmisión en una red común de comunicaciones; Y el subsistema de seguridad física, consistente en video CCTV para vigilancia, detección y monitoreo de perímetro y control de acceso, para respaldar los requisitos de seguridad en el sitio.

Las subestaciones son únicas en que el entorno en el que se instala el equipo electrónico es extremadamente duro, con graves transitorios de tensión procedentes de interruptores automáticos y otros aparatos de conmutación y altos niveles de interferencia electromagnética (EMI) que emanan de grandes transformadores de potencia y otros equipos de alto voltaje. Dado que el equipo de comunicaciones para el SCADA y los subsistemas de seguridad suele estar situado en un refugio sin acondicionar, o al aire libre en recintos a prueba de mal tiempo, está expuesto a un rango muy amplio de temperatura y humedad de funcionamiento con condiciones de condensación. En este ambiente severo, el equipo de transmisión de fibra óptica reforzado es ampliamente utilizado, en gran parte debido a su inmunidad inherente a niveles intensos de interferencia eléctrica.

Se han introducido recientemente conmutadores Ethernet de capa 2 gestionada por subestación y enrutadores de capa 3 con firewalls SCADA que emplean módems de radio celulares integrales para proporcionar circuitos de comunicaciones altamente seguros y fiables internos y externos a la subestación. Estos dispositivos son particularmente útiles para instalaciones de red de fibra óptica dedicada a servicios privados

Aunque los extensores de cable de cobre CAT-5E / UTP y cable coaxial Ethernet están disponibles y ampliamente utilizados para muchas aplicaciones relacionadas con la seguridad física, normalmente no se emplean para sistemas de seguridad de subestaciones, debido a su relativa falta de rechazo de EMI en estos entornos eléctricamente ruidosos, así como su susceptibilidad a bucles de tierra debido a posibles problemas de diferencia de voltaje.

2.2.1 Equipos de comunicación de rendimiento de subestación: la norma IEC – 61850 – 3.

Para mantener altos niveles de confiabilidad, el equipo de comunicaciones dentro de la subestación debe ser capaz de Sobrevivir a largo plazo en este tipo de ambiente operativo adverso, y sin degradación al rendimiento o confiabilidad. Dos estándares clave y universalmente empleados definen los requisitos ambientales para Todo el equipo de

comunicaciones dentro de una subestación eléctrica: IEC 61850-3 para Ethernet compatible Equipos de comunicaciones e IEEE 1613 para equipos heredados no Ethernet. Equipos que cumplan estos se refiere a los requisitos de la subestación.

Los adaptadores serie a Ethernet deben conectan equipos basados en serie a través de una red Ethernet, lo que le permite realizar operaciones como las siguientes:

- Sustitución de cable empleando Ethernet
- Lograr que los puertos COM conecten PC/servidores con dispositivos serie remotos sobre Ethernet
- Comunicar simultáneamente con múltiples dispositivos serie de una red
- Utilizar Ethernet para sustituir conexiones de módem de conexión telefónica preexistentes
- Administrar el puerto de consola de equipos remotos (servidores, routers, conmutadores, centralitas, etc.) sobre Ethernet o a través de conexiones fuera de banda
- Usar la conversión serie-Ethernet para conectar equipos PLC serial a Ethernet
- Conectar equipos con señalización serie vía Ethernet empleando adaptadores serie-Ethernet

La creciente demanda de equipos interconectado por fibra óptica los fabricantes han introducido una línea de productos con comunicación vía Ethernet para subestaciones, tales como: conmutadores de capa 2, los enrutadores de capa 3, los convertidores de medios y los módems de datos en serie de fibra óptica. Estos IEC 61850- 3 y los productos IEEE 1613 probados y certificados son ampliamente utilizados para las redes SCADA de la subestación y para Aislamiento óptico de cámaras de video CCTV eléctricamente delicadas y otros equipos relacionados con el subsistema de protección de la seguridad frente a los efectos nocivos de la EMI y los transitorios de alta tensión Subestación Los conmutadores Ethernet de la capa 2 administrada se utilizan para crear VLAN dentro de la red SCADA, Seguridad y vigilancia, y cualquier otro requisito de comunicaciones, como la telefonía VOIP, Etc. Los routers de capa 3 se emplean para soportar los cortafuegos de seguridad SCADA.

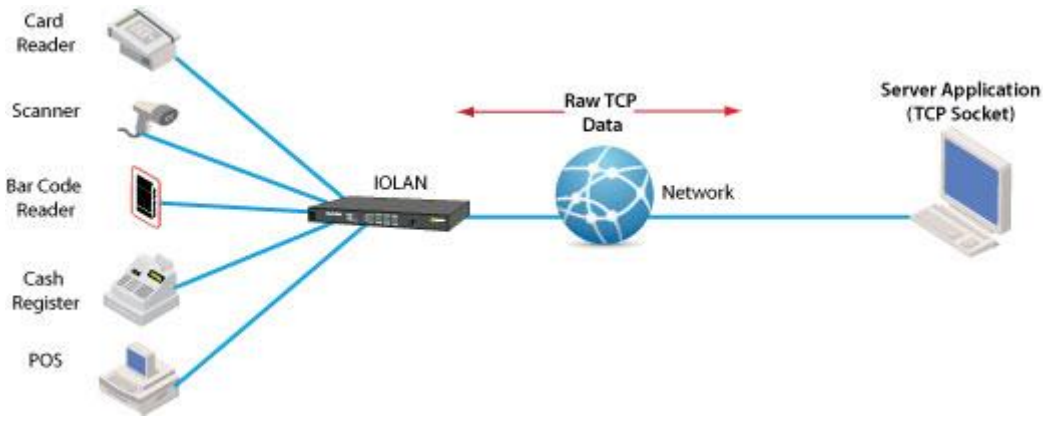


Figura 24: Conexión de dispositivo TCP RAW mediante un dispositivo serial a Ethernet.

2.2.2 Cumplimiento para el subsistema de seguridad física equipo de comunicación

Cualquier equipo de comunicaciones utilizado como parte del sistema SCADA de la subestación Ethernet es invariablemente necesario para cumplir con IEC 61850-3, debido a la importancia crítica de esta aplicación. Como tal, el equipo localizado "dentro del patio" es usualmente especificado por la utilidad a esta norma. El equipo compatible con IEC 61850-3 es eléctricamente, mecánicamente y térmicamente muy robusto, y está diseñado para proporcionar altos niveles de fiabilidad dentro del difícil entorno de la subestación. Sin embargo, esto tiene un costo. Un número relativamente limitado de proveedores y el costo del equipo es significativamente mayor en comparación con la no-subestación de grado industrial de hardware.

	IOLAN SDS1	**IOLAN SDS2**	**IOLAN SDS4**
Procesador	MPC852T, 66 MHz, 87 MIPS		
Memoria			
MB de RAM	32	32	32
MB flash	8	8	8
Puertos de interfaz			
Número de puertos serie	1	2	4
Interfaz de puerto serie	seleccionable por software EIA232 / 422/485 en DB9M, RJ45, DB25M o DB25F	Seleccionable por software EIA-232/422/485 RJ45	
Sun / Solaris	Seguridad en el sol / Oracle Solaris '- no "señal de ruptura" enviado durante el ciclo de alimentación causando servidor costosa reinicios o el tiempo de inactividad		
Velocidades de puerto serie	50 puntos básicos a 230 Kbps con el apoyo velocidad de transmisión personalizable		
Bits de datos	compatibilidad con el protocolo 5,6,7,8, 9 bits		
Paridad	Impar, par, marca, espacio, Ninguno		
Control de flujo	Hardware, software, Ambos, Ninguno		
Protección de puerto serie	Protección contra descarga total de 15 Kv electrostática (ESD)		
Puerto de consola local	RS232 en el puerto serie		
Red	10 Base T / 100 Base TX Ethernet RJ45		
	Software de velocidad seleccionable Ethernet 10/100 Auto		

	Seleccionable por software / half dúplex completo / Auto		
El aislamiento de Ethernet	El aislamiento magnético de 1,5 KV		
Poder			
Fuente de alimentación	120 V de CA (EE.UU.), 230V AC Adaptador (Internacional) de alimentación de pared incluido		
Opciones de Alimentación	Potencia a través de la energía externa 9-30V DC, 4, 8 vatios utiliza socket barril de 5,5 mm x 9,5 mm x 2,1 mm estándar, en el poder sobre cable serie		
Tensión de entrada nominal	12v DC		
Rango de voltaje de entrada	9-30V DC		
IOLAN poder sobre Serial	9-30V DC		
Alimentación del dispositivo externo a través del puerto de serie	De + 5V DC regulada, 1W Max		
Consumo de energía típico @ 12V DC (vatios)	1.7 (no incluye la energía para dispositivos conectados al puerto serie)	2.1	2.4
Especificaciones ambientales			
Salida de calor (BTU / HR)	5.8	7.2	8.2
MTBF (horas) *	123192	188596	150124
Temperatura de funcionamiento	0 C a 55 C, 32F a 131F		
Temperatura de almacenamiento	-40C a 66C, 40F a 150F		
Humedad	5 a 95% (sin condensación) tanto para el almacenamiento y funcionamiento.		
Chasis	SECC Zinc lámina revestida de metal (1 mm)		
Índice de protección	IP40		
Montaje	Pared o montaje en panel, montaje en carril DIN kit opcional		

Tabla 5: Característica del convertidor de conexiones serie a Ethernet.

Es importante tener en cuenta que el equipo de comunicaciones Ethernet con clasificación IEC 61850-3, subestación puede ser integrada de forma óptica y eléctricamente con equipos de comunicaciones Ethernet no basados en la subestación. Dado que la red SCADA dentro de la subestación está casi siempre interconectada a una instalación de supervisión, el subsistema que respalda los requisitos de seguridad física en la Comparte y hace uso efectivo de la plataforma de red SCADA.

2.2.3 Caso de estudio: subsistema de equipo de comunicaciones de seguridad física tipo de subestación.

El proceso de implementar una serie de subsistemas de monitoreo y detección de seguridad física estandarizados para cumplimiento NERC-CIP-014 en numerosas subestaciones dentro de su amplio sistema de transmisión y distribución. Varias de estas subestaciones soportan una tensión de transmisión de 115 KV.

Los criterios básicos y los requisitos más destacados para el subsistema de seguridad física fueron los siguientes:

- Integración perfecta del subsistema de seguridad física con la red / plataforma SCADA existente / antigua de la subestación basada en Ethernet
- Utilizar las cámaras de video IP de video IP instaladas recientemente y las cámaras CCTV IP convencionales
- Utilizar cámaras de CCTV analógicas de alta resolución heredadas con un canal de control de zoom panorámico de datos en serie separado
- Instalar un sistema de control de acceso basado en IP para la admisión de personal de mantenimiento autorizado al sitio
- Proporcionar vigilancia y detección electrónica basada en IP en todo el perímetro de la instalación de la subestación
- Utilizar equipos de transmisión de fibra óptica siempre que sea posible para el subsistema de seguridad física, para eliminar la posibilidad de interferencia eléctrica / EMI y bucles de tierra debido a emisiones radiadas y conducidas emanadas de transformadores de potencia de alto voltaje, disyuntores,
- Equipo dentro de la subestación
- Emplear enlaces de radio de microondas de 5 GHz libres de licencia para aquellos enlaces de cámaras de video IP de CCTV donde la dificultad de instalar un nuevo cable de fibra óptica puede ser prohibitiva.
- Crear VLANs separadas para el video CCTV, el sistema de control de acceso y el equipo de vigilancia perimetral, y cualquier otro equipo que sea accesorio de la red SCADA de la subestación
- Proporcionar un NVR (Network Video Recorder) para almacenar / archivar el video de la instalación

El sistema de red SCADA basado en Ethernet en muchas de estas subestaciones emplea una combinación de interruptores heredados de la capa 2 administrados conforme a la subestación 10/100 y 100/1000 Mbps / IEC 61850-3. Muchos de estos conmutadores proporcionan una interfaz de sólo cobre para los datos Ethernet, con sólo los puertos de enlace ascendente que soportan una interfaz de fibra óptica con óptica mono modo fija. Varios de los conmutadores de nueva generación dentro de algunos de los sitios proporcionan una combinación de interfaces de cobre y óptica para los datos de Ethernet, con los puertos ópticos basados en SFP (Small Form Factor Pluggable), para una mayor

flexibilidad en términos de selección de usuario Compatibilidad con fibra óptica y distancia de transmisión óptica / pérdida de trayectoria.

Las imágenes térmicas y las cámaras de vídeo IP convencionales tienen alimentación PoE y derivan su potencia de operación de +48 VDC de los convertidores de medios montados en estanterías industriales. Para aquellos switches gestionados en los que no se dispone de una interfaz Ethernet óptica, las salidas de los convertidores de medios multicanales se conectan directamente a los puertos de cobre de estos conmutadores. Estos convertidores de medios se colocan conjuntamente con los conmutadores utilizados para la red SCADA dentro del refugio del equipo de la subestación, y están montados en bastidor para un uso óptimo del rack disponible. Los convertidores de medios multicanal Proporcionan la máxima cantidad de canales y la densidad dentro de cada chasis de jaula de tarjeta montado en bastidor.

Cuando los conmutadores gestionados proporcionan una interfaz Ethernet óptica, los convertidores de medios situados en el extremo del campo o borde de la red están ópticamente conectados directamente a los puertos de entrada óptica Ethernet del conmutador, eliminando la necesidad de convertidores de medios en el extremo del enlace del enlace, Simplificando así el diseño y mejorando la fiabilidad global del sistema.

2.3 La importancia de la alimentación a través de Ethernet

Del mismo modo que el par de hilos que transporta las señales telefónicas POTS (Plain Old Telephone System) hasta su hogar suministra energía suficiente para el audífono, el sistema de discado y timbre de su teléfono, Poe facilita la entrega de energía DC mediante cableado Ethernet estándar (CAT5 y superior). Se trata de una potencia suficiente para alimentar un número creciente de dispositivos de uso habitual, además del equipo de TI. Entre dichos dispositivos figuran teléfonos VoIP, cámaras de seguridad, puntos de acceso inalámbricos, quioscos POS remotos, Servidores de Dispositivos y Extensores Ethernet.

Existen dos tipos principales de dispositivos que se utilizan en un entorno PoE: el equipo de fuente de alimentación (PSE) y el dispositivo alimentado (PD). El PSE suministra la corriente y el PD la acepta. Un PSE PoE suministra un máximo de 15,4 vatios de corriente a 48 v de CC. Un PSE PoE+ suministra un máximo de 30 vatios de corriente a 48 v de CC. Un PD puede tener un requisito máximo de entrada de corriente de 12,95 vatios. Esto incluye la degradación de la corriente a su paso por el cable. El estándar 802.3af exige un cable de cuatro pares. El cable CAT5 tiene cuatro pares trenzados, aunque solo dos de los pares se usan para datos. La especificación 802.3af permite utilizar los dos pares sobrantes o los pares de datos para transportar electricidad.

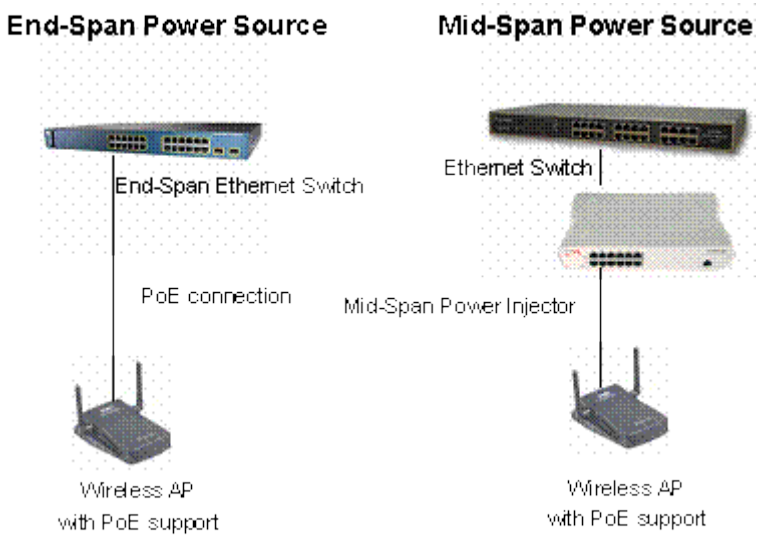


Figura 25: Equipos alimentado sobre Ethernet

En la figura 25 se observa, que la electricidad "inyectada" al cableado puede ser hecha mediante switches LAN/WAN que incorporan circuitería para suministro de energía. Como alternativa, si no desea sustituir los conmutadores de LAN existentes, o si solo desea suministrar corriente a algunos segmentos, es posible conectar paneles de parche de alimentación o inyectores "intermedios" entre el conmutador y el dispositivo alimentado (PD). El PD final debe soportar PoE. Muchos de los conmutadores PoE tienen capacidad de gestión de energía de tal modo que los equipos PoE conectados a este puede ser reencendidos. Esto es ideal para aplicaciones de gestión remotas donde los equipos de TI, como servidores y enrutadores, pueden requerir ser reencendidos a fin de normalizarse.

En la actualidad, hay dos estándares de PoE:

- IEEE 802.3af proporciona como máximo 15,4 W por puerto.
- IEEE 802.3at proporciona como máximo 25,5 W. Este sistema se conoce como High PoE.

Con el sistema PoE IEEE 802.3af, el equipo de suministro eléctrico proporciona una potencia máxima de 15,4 W por puerto, pero parte de esta potencia se perderá utilizando un cable de par trenzado. Por tanto, la potencia máxima garantizada para el dispositivo alimentado es de solo 12,95 W.

El estándar IEEE 802.3af también especifica diferentes niveles de potencia para los dispositivos PoE, conocidos como clases de potencia. Si el equipo de suministro eléctrico admite esta clasificación de potencia, el volumen de potencia suministrado a cada puerto se adapta automáticamente a la clase de potencia (1-4) del dispositivo alimentado que se conecte. La clase 0 es la predeterminada y proporciona un máximo de 15,4 W. Las clases de 1 a 3 proporcionan una potencia inferior a la clase predeterminada, mientras que la clase

4 proporciona más potencia, aunque solo está disponible para los dispositivos alimentados conformes con el estándar IEEE 802.3af.

Si el dispositivo alimentado no es compatible con la clasificación de potencias, el equipo de suministro eléctrico proporcionará por defecto una potencia de clase 0 (15,4 W).

La siguiente tabla muestra el consumo eléctrico en el equipo de suministro eléctrico y el dispositivo alimentado.

Clase	Uso	Nivel de salida de potencia en el equipo de suministro eléctrico (PSE)	Niveles de potencia máxima en el dispositivo alimentado (PD)
0	Predefinido	15,4 W	0.44 – 12-95 W
1	Opcional	4,0 W	0.44 – 3.84 W
2	Opcional	7,0 W	3.84 – 6.49 W
3	Opcional	15,4 W	6.49 - 12,.95 W
4	Opcional: Solo IEEE 802.3at	30 W	12,95 – 25.5 W

Tabla 6: Valores de las diferentes clases de PoE para utilizar al calcular la potencia disponible de un sistema

2.3.1 Ampliación más allá de 100 metros.

En el caso de dispositivos remotos que necesiten recibir alimentación y datos pero que estén situados a más de 100 metros de cable, los administradores de redes disponen de varias opciones. Pueden añadir un armario de datos remoto, utilizar ampliadores de LAN que conviertan Ethernet a DSL, utilizar conversores de UTP a coaxial o instalar tecnología inalámbrica. O bien pueden disfrutar de las ventajas que ofrece el cable de fibra óptica para ampliar la distancia de la red.

La fibra amplía las distancias de red hasta las 100 millas (160 km) por enlace sin el deterioro de datos a larga distancia que produce el cableado de cobre. Los ampliadores de LAN permiten ampliar las distancias de la red hasta las 6 millas (10 km), pero todo aquello que quede más allá de 328 pies (100 metros), experimentará una velocidad de transmisión de datos significativamente inferior. En lugar de 100 Mbps, la velocidad de datos caerá a tan solo 2,3 Mbps. Además, el cableado de fibra ofrece ventajas de seguridad. No genera emisión electromagnética y es muy difícil de pinchar. Y dado que no es susceptible a la interferencia eléctrica o a la pérdida de datos debida a la temperatura o a las condiciones atmosféricas, la fibra es extremadamente fiable.

La fibra puede tenderse desde un armario de datos existente hasta un área con acceso a alimentación. Un Conversor de Medios PoE puede alimentarse mediante CC de 48 V o CA de 120 a 240 V. El conversor de medios se conecta a la fuente de alimentación y al cable de fibra. La Ethernet de cobre (cable UTP o STP) puede ampliarse otros 100 metros hasta el PD. El Conversor de Medios PoE convierte los datos de fibra a cobre, incorpora corriente y la transmite al PD.

Cuando tenga que ampliar los servicios Ethernet más allá de los límites genéricos que establece la norma IEEE 802.3, de 100 m y el coste de un cableado de fibra sea prohibitivo, los Extensores Ethernet son la solución perfecta. Los extensores Ethernet de Perle amplían de forma transparente las conexiones Ethernet 10/100/1000 en cableado de cobre. Use el cableado de par trenzado único (CAT5/6/7), coaxial o cualquier cableado de cobre existente previamente usado en circuitos de alarma, circuitos E1/T1, RS-232, RS-422, RS-485 y aplicaciones CCTV y CATV. Un Extensor Ethernet PoE puede operar como un PD o un PSE.

En resumen, los beneficios de la tecnología PoE son:

- Utilice un solo cable para conectar su equipo - simplifique instalación y ahorre espacio.
- No hay necesidad de pagar por un costoso servicio de electricista, o demorar su instalación por asuntos de disponibilidad del mismo - ahorre tiempo y dinero.
- El equipo puede ser movido a cualquier lado donde haya un cable LAN - minimice el corte de servicio.
- Más seguro - sin tensión de red eléctrica en cualquier parte.
- Un UPS puede garantizar el suministro de energía aún durante los cortes de la red eléctrica.
- Los equipos pueden ser apagados o reencendidos remotamente - no hay necesidad de un botón de *reset* o interruptor de energía.

2.4 Sincronización de la hora

Para resolver problemas de sincronización son implementadas protocolos de sincronización como NTP, IRIG-B, IEEE 1588. El empleo de las redes IEEE 802.3 como soporte de comunicación de los SAS genera dudas cuanto al método de sincronización más adecuado. De esta manera, este proyecto tiene como objetivo el estudio de alternativas cuanto a los métodos y protocolos de comunicación que serán empleados en un sistema de automatización con base en la norma IEC 61850. Por lo tanto, serán estudiados los protocolos NTP/SNTP, IRIG-B y el IEEE 1588.

La evolución del sistema eléctrico tuvo como consecuencia la necesidad del incremento y la complejidad de las funciones de control de los SAS. Por consiguiente, es necesario que la coordinación de eventos en relación del tiempo sea efectuada de forma sincronizada. Los propósitos para la sincronizaron son los siguientes:

- Permitir y asegurar que el evento ocurra en una determinada secuencia o en tiempo predeterminado.

- Recuperar las informaciones registradas, relativas a eventos sucedidos, para que luego puedan ser analizados los problemas ocurridos y proponer las soluciones.

Inicialmente el protocolo NTP (Network Time Protocol) fue utilizado en aplicaciones que poseen exigencias de resolución máxima de sub-milisegundo. Sin embargo, existen ciertas tareas temporalmente críticas de los SAS, que exigen mayores resoluciones que no pueden ser atendidas por el protocolo NTP.

Por otro lado, el protocolo IRIG-B, que tiene como fuente de referencia el GPS, atiende a la resolución exigida para las tareas críticas de tiempo real empleadas por los SAS. La adopción del padrón IRIG-B demanda la existencia de una red separada exclusiva para el transporte de las señales periódicas utilizadas para la sincronización de los relojes internos de los IEDs.

Para resolver los problemas asociados a los protocolos IRIG-B y NTP se están realizando investigaciones de la aplicación del protocolo IEEE 1588 en sistemas distribuidos que exigen resoluciones temporales del orden de nanosegundos. El protocolo IEEE 1588 es la norma de sincronización de alta precisión de tiempo, también es conocido como PTP (Precision Time Protocol).

En la Tabla 7 se muestra una comparación entre los protocolos mencionados.

Protocolo	Precisión	Interconexión	Hardware y software
NTP	1 – 10 ms	Ethernet LAN o WAM	Hw o Sw servidor, Sw Cliente
IRIG	1 -10 ns	Cable coaxial	Hw Maestro y esclavo
IEEE 1588	10 – 100 ns	Ethernet LAN	Hw Maestro y esclavo

Tabla 7: Comparación de los diferentes protocolos para el sincronismo.

2.4.1Protocolo NTP.

NTP (*Network Time Protocol*) es el método de sincronismo del dominio público más importante. Este protocolo permite la sincronización de los relojes de los dispositivos de una red como servidores, estaciones de trabajo, enrutadores y otros equipamientos a partir de una referencia de tiempo confiable. La exactitud proporcionada depende de la extensión y la complejidad de la red. Si la red es una LAN, normalmente se obtiene una precisión de milisegundos, mientras que, en una WAN, el retardo se puede incrementar en unas decenas de milisegundos.

El funcionamiento de NTP consiste en obtener diversas muestras de las informaciones de determinados servidores. Asimismo, se elige la mejor referencia de tiempo entre los servidores que suministran tiempos correctos de modo a garantizar homogeneidad de tiempo. En conjunto con otros servidores NTP, se forma una topología simple, confiable, robusta y escalable para la sincronización de tiempo.

En la Figura 26 se muestra la organización total del modelo de servidor de tiempo NTP. La estampa de tiempo es intercambiada entre un cliente y otros servidores y clientes de subred en intervalo de algunos segundos o varias horas. Estos son usados para determinar desplazamiento individual y offset de reloj, como para proveer el error estimado. Luego, el filtro del reloj es para reducir salto imprevisto de acuerdo a los procesamientos de los desplazamientos y offset de cada servidor.

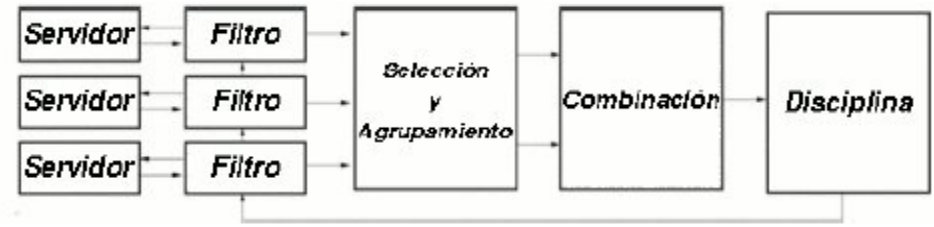


Figura 26: los componentes de NTP.

También es importante mencionar que contrario a la creencia, NTP no está basado en los principios de sincronización de máquinas uno con otro. Sin embargo, está basado en los principios de mantener a todas las máquinas de la red a un tiempo más cercano posible al tiempo de referencia. Esto se obtiene a través del cálculo de los datos obtenidos en los intercambios de mensajes entre el cliente y el servidor como es observado en la Figura 27.

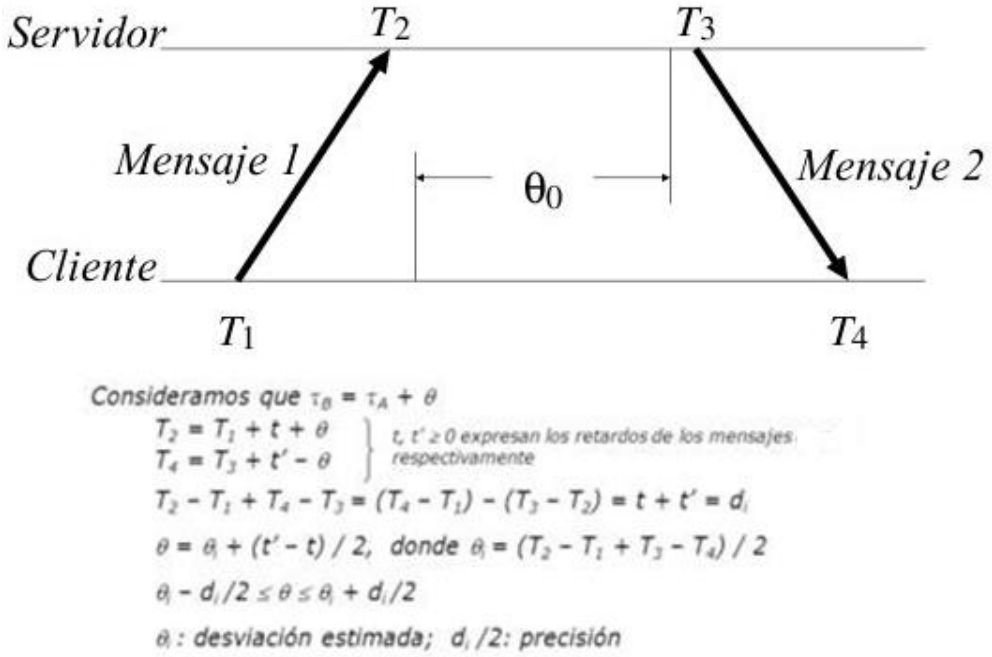


Figura 27: Intercambio de mensaje.

2.4.2 Protocolo IRIG.

Protocolo IRIG es el código de tiempo desarrollado por TeleCommunications Working Group de Inter-Range Instrumentation Group, el cuerpo estándar de Range Commander Council. Existen varios formatos y combinación de modulación de señal. Dicha codificación de la señal puede ser observada en la Figura 28:

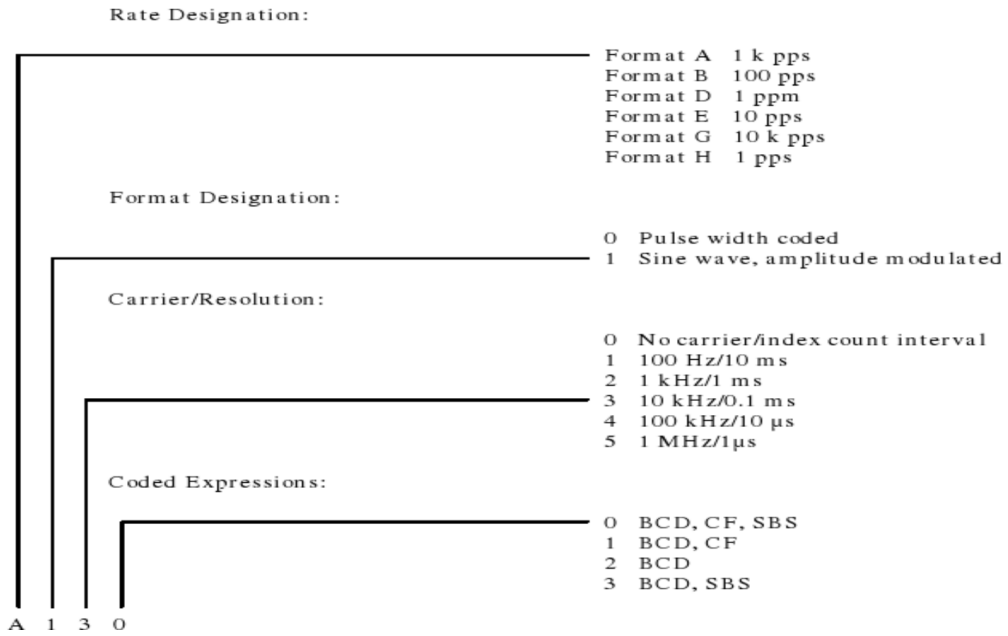


Figura 28: Codificación del Protocolo IRIG

El estándar de sincronización de tiempo en los equipamientos de utilidad eléctrica ha sido el IRIG-B, en amplitud de 1kHz modulado y formato DC variado. El IRIG-B modulado por amplitud es más seguro contra mayor tipo de interferencias y es más amigable para grandes interconexiones de redes. El código de ancho de pulso IRIG-B es más exacto para redes que son muy limitados en tamaño y en la complejidad.

En la actualidad existen distintas variables de código IRIG-B, pero generalmente en la industria de energía es utilizado el formato B123. La definición de función de control es contenida en IEEE 1344, Standard for Synchrophasor Measurement, y en este formato incluye año, lugar, offset, cualidad de tiempo y notificación de eventos.

2.4.3 Protocolo IEEE 1588.

El protocolo de tiempo preciso IEEE 1588 es utilizado para sincronizar relojes de tiempo real en los ¨nodos¨ de un sistema distribuido que se comunican por medio de una red. Este protocolo es también conocido como “PTP - Precise Time Protocol”. La tecnología es originalmente desarrollada por Agilent y fue utilizada en mediciones distribuidas y tareas de control. La utilización PTP hace que sea posible el sincronismo de menos de un

microsegundo en reloj local del sensor, actuador y otro dispositivo terminal. Además de sincronizar el reloj interno, transporta también los datos del proceso a través de la misma red.

El protocolo tiene como objetivo: a) Ser aplicable para el sistema de comunicación por LAN soportando mensajería multidifusión incluyendo, pero no limitando para Ethernet; b) Ser sistema heterogéneo que incluye reloj de varias inherentes precisión, resolución y estabilidad para sincronizar; c) Ser soporte del sistema de sincronismo de exactitud en rango de sub-microsegundo con red mínima y fuente de reloj local de la computadora.

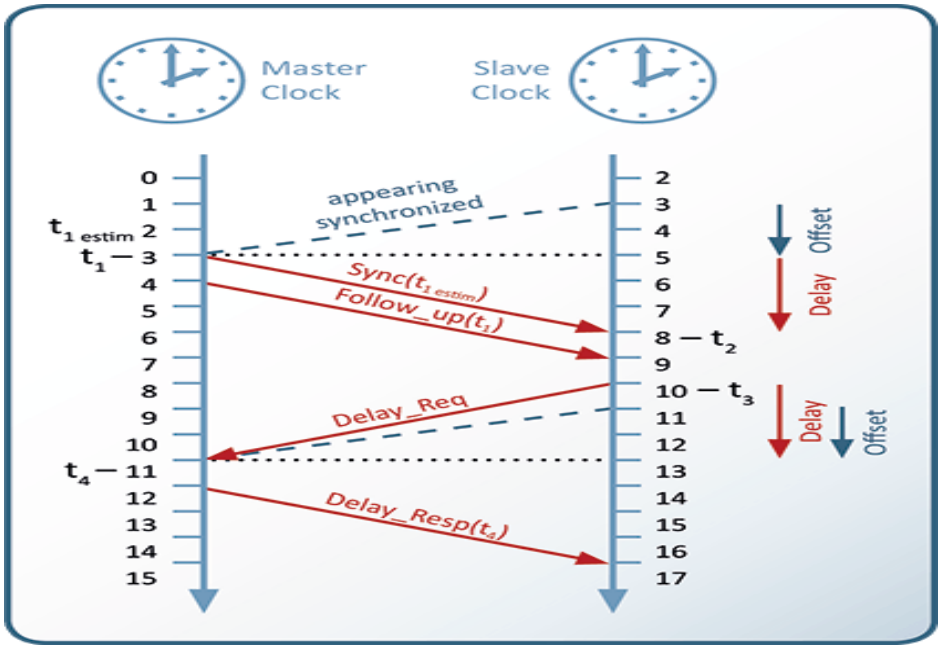


Figura 29: Funcionamiento de IEEE 1588

En la Figura 29 se muestra los intercambios de telegramas realizados entre el servidor y el cliente para el sincronismo del reloj interno el cliente. Basado en el primero y el segundo telegrama y el significado de su propio reloj, el receptor puede calcular la diferencia de tiempo entre la hora de su reloj y la hora del reloj del máster.

La red PTP configura y segmenta él mismo automáticamente. Por esto, cada nodo usa el algoritmo de "mejor reloj de máster" (BMC - Best Master Clock). Estas características son transmitidas para otro nodo con sus telegramas "Sync". Basado en esto, otros nodos son habilitados para sincronizar sus configuraciones de informaciones con sus características del actual máster y puede ajustar sus relojes como corresponde. Debido al funcionamiento de BMC, los nodos pueden ser conectados o extraídos durante el tiempo de propagación.

De modo a obtener precisión del rango de nanosegundos es necesario el soporte de hardware. El PTP también utiliza la estampa de tiempo como el NTP para el sincronismo de redes. Sin embargo, la estampa de tiempo en NTP es hecha en software, no por hardware, lo cual causa retraso de proceso asimétrico que reduce la exactitud del tiempo de transferencia. Generalmente el error de sincronización causado por software no puede ser eliminado. Teniendo solamente la solución de software, al error puede variar entre micro o milisegundos.

2.5 Selección de parámetros correspondientes y routers para el entorno.

Las subestaciones contienen valiosas piezas de equipos alojan normalmente en cobertizos de control no acondicionados en el interior del cerca. Si bien esto proporciona un cierto nivel de protección contra los elementos, las temperaturas pueden ser extremas, roedores y otras plagas pueden invadir el cobertizo, y la suciedad y la mugre se puede acumular en el equipo. Otras tensiones pueden incluir la humedad, a la corrosión y ruido electromecánico.

Por tanto, es importante seleccionar solamente conmutadores y routers que tienen la protección contra los riesgos ambientales y de otro que existen en sus subestaciones. IEEE 1613 y IEC-61850 – 3 describir las normas de dispositivos que necesitan ser satisfechas para la protección del medio ambiente. Como una utilidad el operador debe asegurarse de que la red productos que cumple o exceden todos los sectores industriales relevantes estándares como lo equipos que se observa en la figura 30.

Figura 30: Equipos que tienen la protección contra los riesgos ambientales dentro subestaciones según IEEE 1613 y IEC-61850 – 3

La norma IEC 61850 exige requisitos especiales a los componentes de red: según el lugar de montaje, deben cumplir requisitos medioambientales extremadamente elevados especificados según IEC 61850-3 e IEEE 1613. Los switches, adaptadores de medios y módulos de redundancia cumplen estos requisitos y permiten una elevada disponibilidad durante la automatización de las subestaciones como se describen en la tabla 8:

FUNCIONES DE LOS EQUIPOS EN LA SUBESTACION	
Diseño robusto para ambientes extremos	• Carcasa de aluminio IP40 resistente a la corrosión • Certificación de seguridad UL508A de equipos de control industrial • Ubicaciones peligrosas - Class1/Div2, ATEX Class1/Zone2

Funcionamiento fiable	• Sin ventilador, sin piezas móviles • Fuente de alimentación dual. Conectar para separar las fuentes de alimentación para redundancia. ▪ Protección contra polaridad inversa ▪ Protección contra sobrecargas de corriente • Resistente a los efectos de las vibraciones y choques que se encuentran en los entornos industriales
Rendimiento de Ethernet en tiempo real	• Alta velocidad de cable, conmutación por almacenamiento y reenvío, arquitectura sin bloqueo • Auto detección de velocidad y dúplex • El cruce automático de mdi/mdix funciona con cables directos y cruzados • Que no se producen retardos ni pérdidas de paquetes en caso de fallo de componentes de red con el módulo de redundancia PRP
PoE y PoE+ (en 4 puertos)	Hasta 30 vatios por puerto que pueden alimentar hasta cuatro dispositivos (PDs) clase 4 (IEEE 802.3at Tipo 2)
Elevador de voltaje de entrada	La tecnología de elevación de voltaje es compatible con fuentes de energía de 24 V garantizando el suministro de un voltaje PSE total y adecuado en todos los puertos PoE
Soportes Jumbo	Compatible con soportes Jumbo de hasta 10 KB
Eficiencia energética de Ethernet (EEE)	Eficiencia energética de Ethernet (EEE) según 802.3az. Esto ofrece ahorro de energía durante la inactividad de la red.

Tabla 8: Selección de parámetros que deben cumplir los equipos para el entorno.

2.6 La construcción de múltiples capas de seguridad.

La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema, para ello exige tres puntos que se extienden al sistema de comunicaciones cuando se integran equipos en este:

- **Secreto:** Acceso a la información y recursos solo al personal autorizado.
- I**ntegridad:** Modificación de la información y recursos solo por el personal autorizado.
- **Disponibilidad:** la información y los recursos deben estar disponibles para personal autorizados.

Sería prácticamente interminable el enumerar las posibles formas de ataque que puede sufrir un equipo conectado a una red de comunicación, bien por intervención física sobre la misma vía software. Las medidas de prevención son múltiples también, desde la vigilancia física del sistema, por ejemplo, el estado d las redes de comunicación para detectar posibles perdida de potencia en la señal o interferencia atribuibles a intervenciones sobre ella, hasta el registro de los eventos que se producen en el sistema y la vigilancia de modificaciones en archivos o procesos que son críticos para la seguridad del mismo. Todo involucra la responsabilidad de los usuarios y del administrador del sistema encargado de establecer las políticas de cuentas de usuario adecuadas y mantener actualizados los dispositivos y el software que puedan tener agujeros que comprometan la seguridad.

2.6.1 Tipos de ataques más comunes.

Los métodos de ataques descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, y a que el uso de un método en una categoría permite el uso de otros métodos en otras, por ejemplo: después de crackear una contraseña, un intruso realiza un "login" como usuario legitimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente el atacante puede también adquirir derechos de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema ante de huir.

- **Husmeo de paquetes**: es muy utilizado para capturar nombre de usuario y contraseñas, que generalmente viajan claros al conectarse al sistema de acceso remoto.
- **Curiosear**: tiene el mismo objetivo que el husmear, obtener la información sin modificarla. Sin embargo, son diferentes, además de interceptar el tráfico de la red el atacante captura los documentos, mensaje de e-mail y robar información guardada, descargando en la mayoría de los casos esa información a su propia computadora.
- **Manipulación de los datos**: esta categoría se refiere a la modificación sin autorización a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Estos tipos de ataque son particularmente serios cuando el que lo realiza ha obtenido derechos de administrado, con la capacidad de ejecutar comandos y alterar o borrar cualquier información que puede incluso terminar en la destrucción total de sistema.
- **Falsificación:** esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de manipulación, el cual consiste en conseguir el nombre y la contraseña de un usuario legitimo para., una vez en el sistema, tomar acciones en nombre de administrador.
- **Interferencia:** este tipo de ataque desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie pueda utilizarla.
- **Bombas lógicas**: es el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa a rutina que en una fecha determinada destruirá, modificará la información o provocará el cuelgue del sistema.

- **Difusión de virus**: si bien es un ataque de manipulación, difiere de ese porque puede ser introducido en el sistema por un dispositivo externo o a través de la red sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no está instalada una protección antivirus en los servidores, estaciones de trabajos.

2.6.2 Las tres áreas de la seguridad

Actualmente las empresas disponen ya de sus propias redes internas a las que dan acceso a usuarios desde el exterior, los problemas de seguridad se platean en tres áreas principales:

- **La seguridad del perímetro**: protección frente ataques del exterior generalmente basada en cortafuegos.
- **La seguridad en el canal**: donde hay que proteger los daos frente a escuchas mediante claves.
- **La seguridad de acceso:** donde se contemplan tres aspectos, la identificación del usuario, la autorización del acceso y la auditoria de las operaciones realizadas por los usuarios.

Un cortafuego es una de las vanas formas de proteger una red de otra red no fiable desde el punto de vista de la segundad. Los mecanismos reales mediante los cuales se implementan las funciones del cortafuego son muy vanados, pero en general, el cortafuego puede verse como la unión de un mecanismo para bloquear tráfico y otro para permitirlo. Algunos cortafuegos hacen especial hincapié en el primero, mientras que otros se basan fundamentalmente en el segundo

La razón para la instalación de cortafuegos es proteger una red privada de intrusos, pero permitiendo a su vez el acceso autorizado desde y hacia el exterior. Otra razón importante es que pueden proporcionar un bastión en el que centrar los esfuerzos de administración y auditoria. Por último, un cortafuego puede actuar como representante de la empresa en Internet ya que muchas compañías usan sus cortafuegos para almacenar información pública sobre los servicios y o productos que ofrece.

Una situación más peligrosa se produce si alguien es capaz de entrar en la máquina cortafuegos y reconfigurarla de modo que toda la red protegida quede accesible. Este tipo de ataque se suele denominar *destrucción* del cortafuego. Los danos derivados de este tipo de ataque resultan muy difíciles de evaluar. Una medida importante de cómo un cortafuego es capaz de soportar un ataque, es la información que almacena para ayudar a determinar cómo se produjo. La peor situación posible es que resulta de la destrucción de un cortafuego sin que queden trazas de cómo se perpetró el ataque

Una forma de ver el efecto del fallo de un cortafuego es en términos de la *zona de riesgo* que crea su fallo. Si una red se encuentra conectada a Internet directamente. Toda la red es susceptible de ser atacada (toda es una *zona de riesgo).* Eso no significa que la red se3

necesariamente vulnerable, sino que es necesario reforzar las medidas de seguridad en todas y cada una de las máquinas que forman la red Esto es extremadamente difícil a medida que aumenta el número de máquinas y el tipo de servicios de red que estas ofrecen a sus usuarios. Un cortafuego típico reduce la zona de riesgo al propio cortafuego o a un reducido grupo de nodos de la red. Simplificando notablemente el trabajo del administrador Si el cortafuego falla, la zona de riesgo puede expandirse hasta alcanzar a toda la red protegida. Si un hacker gana acceso a los cortafuegos. Puede utilizarlo como plataforma para lanzar ataques contra las máquinas de la red interna.

Se debe tener claro que un cortafuego no puede proteger de ataques que no se produzcan a través del mismo. Si una compañía posee información reservada en los ordenadores de su red interna, el cortafuego no podrá protegerla contra un ataque desde dentro. Por ello, esa la red interna debería estar aislada, o bien contar con medidas extras de protección.

2.6.3 Tipos de cortafuegos.

En la configuración de un cortafuego, la principal decisión consiste en elegir entre seguridad o facilidad de uso. Este tipo de decisión es tomado en general por las direcciones de las compañías. Algunos cortafuegos sólo permiten tráfico de correo electrónico a través de ellos, y por lo tanto protegen a la red contra cualquier ataque que no sea a través del servicio de correo. Otros son menos estrictos y sólo bloquean aquellos servicios que presentan problemas de seguridad.

Existen dos aproximaciones básicas:

- Todo lo que no es expresamente permitido está prohibido.
- Todo lo que no es expresamente prohibido está permitido.

En el primer caso, el cortafuego se diseña para bloquear todo el tráfico, y los distintos servicios deben ser activados de forma individual tras el análisis del riesgo que representa su activación y la necesidad de su uso.

En el segundo caso, el administrador del sistema debe predecir qué tipo de acciones pueden realizar los usuarios que pongan en entredicho la seguridad del sistema, y preparar defensas contra ellas. Esta estrategia penaliza al administrador frente a los usuarios. Los usuarios pueden comprometer la seguridad del sistema si no conocen y cumplen unas consideraciones de seguridad mínimas. El problema se magnifica si existen usuarios que tengan cuenta en la propia máquina que hace de cortafuegos (situación muy poco recomendable). En este tipo de estrategia hay un segundo peligro latente, y es que el administrador debe conocer todos los posibles agujeros de segundad existentes en los protocolos y las aplicaciones que estén ejecutando los usuarios. El problema se complica debido al hecho de que los fabricantes no suelen darse prisa en notificar los riesgos de segundad que presentan sus productos.

2.6.3.1 Cortafuegos a nivel de Red.

Por lo general se trata de un router o una computadora especial que examina las características de los paquetes IP para decidir cuáles deben pasar y cuáles no. Por ejemplo se podría configurar el router para que bloquease todos los mensajes que provengan del sino de un determinado competidor, así como todos los mensajes destinados al servidor de ese competidor. Los profesionales de las redes 3 menudo denominan a este proceso como lista negra.

Normalmente se vuele configurar un encaminado: para que tensa en cuenta la siguiente información para cada paquete antes de decidir si debe enviarlo.

- Dirección IP de origen y destino (cabecera IP. nivel 3)
- Puerto origen y destino (campo de datos IP. cabecera nivel 4)
- Protocolo de los datos (TCP.UDP o ICMP) (cabecera IP. nivel 3)
- Si el paquete es inicio de una operación de conexión (campo de datos IP. cabecera nivel

Si se instala y se configura correctamente un cortafuego a nivel de red. Éste será muy rápido y casi totalmente transparente para los usuarios. Para ordenadores Linux un software que permite realizar funciones de filtrado para implementar un cortafuego 3 nivel de red es el IP de cadenas o IP de contenidos.

2.6.3.2 Cortafuegos a nivel de circuito.

Se trata de una versión avanzada de los cortafuegos vistos en el punto anterior que trabajan en la capa de transponer. La seguridad en este caso está basada en el establecimiento, seguimiento y liberación de las conexiones que se realizan entre las máquinas internas y externas. Observan la conveniencia o no de la existencia de esas conexiones en función del tipo de aplicación que realiza la conexión y la procedencia de la petición. Además, realizan seguimiento en los números de secuencia de la conexión buscando aquellos paquetes que no corresponden con conexiones establecidas. Durante este seguimiento, se establece un circuito virtual entre el cliente y el servidor a través del cortafuego, que hace transparente la existencia de dichos cortafuegos.

2.6.3.3 Cortafuegos a nivel de aplicación.

Suele ser un ordenador que ejecuta software de servidor Proxy. La palabra “proxy” significa “actuar por poderes” o “en nombre de otro”. Los servidores proxy hacen precisamente esto, se comunican con otros servidores del exterior de la red en nombre de los usuarios.

En otras palabras, un servidor proxy controla el tráfico entre dos redes estableciendo la comunicación entre el usuario y él mismo y entre él mismo y el ordenador destino. De este modo la red local queda oculta para el resto de Internet. Un usuario que acceda a Internet a través de un servidor proxy aparecerá para los otros ordenadores como si en realidad fuera el servidor proxy (se muestra la dirección IP de éste). Esto combinado con un servicio NAT. Puede hacer completamente invisibles las direcciones IP de los ordenadores de la red interna hacia el exterior.

Como trabaja a nivel de aplicación, este tipo de cortafuegos es más seguro y potente, pero también menos transparente y rápido que un encaminado: Existen servidores proxy disponibles para diferentes servicios como HTTP, FTP, SMTP y Telnet. Es necesario configurar un servidor proxy diferente (aunque pueden residir en la misma máquina) para cada servicio que se desee proporcionar, de los servidores proxy más populares para las redes basadas en UNIX y Linux son TTS Internet Firewall Toolkit y SOCKS.

Al implementar un servidor proxy a nivel de aplicación, los usuarios de la red deberán utilizar programas clientes que puedan trabajar con un proxy. Los diseñadores han creado mucho; protocolos TCP IP, como HTTP, FTP, pensando en la posibilidad de utilizar un proxy. En la mayoría de los navegadores web. Los usuarios pueden establecer fácilmente sus preferencias de configuración de un proxy a utilizar.

Desgraciadamente no todos los protocolos están pensados para utilizar un proxy. Y en esos casos puede ser necesario seleccionar las aplicaciones para Internet según su compatibilidad un protocolo proxy habitual, por ejemplo, SOCKS. Como contrapartida a todos los posibles inconvenientes, el software de proxy se puede combinar con la utilización de antivirus para detectar, dentro de los contenidos que se intercambian las aplicaciones a través del proxy. Las huellas de virus en los mensajes de correo, documentos, applets embebidos en páginas HTML (Java, ActiveX...), ejecutables, etc. y eliminarlos o advertir del riesgo al usuario.

2.6.4 Topologías de cortafuegos.

Aunque el propósito de todos los cortafuegos es el mismo, existen diferencias en sus topologías y prestaciones. Los siguientes son algunos ejemplos de las múltiples posibilidades existentes:

- Bastión Host
- Router con filtro (Screemng Router)
- Host con doble conexión (Duai-Komed Host)
- Cortafuegos mediante filtrado de host (Screened Host)
- Cortafuegos mediante filtrado de subred Screened Subnet)

2.6.4.1 Bastión Host.

Son sistemas identificados por el administrado: de la red como puntos clave en la segundad de la red Son auditados regularmente y pueden tener software modificado para filtrar y bloquear determinados intentos de conexión, trazar las comunicaciones y reparar fallos de seguridad del sistema.

En la figura 31 se observa un ejemplo simple es el caso de la instalación de un software de cortafuegos personal en el equipo del usuario. Mediante este tipo de software el usuario puede controlar, bloquear y filtrar el tráfico de datos que entra y sale por cada uno de los puertos de comunicación de su ordenador personal, tanto si utiliza aplicaciones Cliente, como si ofrece servicios a equipos remotos.

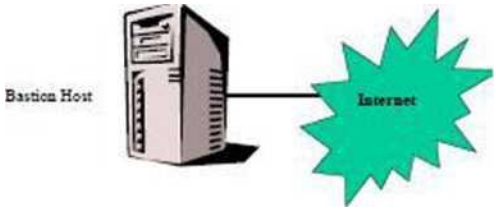


Figura 31: Topología de un cortafuego Bastión Host

2.6.4.2 Enrutador con filtrado (Screening Router).

Son un componente básico de la mayor parte de los cortafuegos. Pueden ser un router comercial o basado en un ordenador convencional, con capacidad para filtrar paquetes. Tienen la capacidad para bloquear el tráfico entre redes o nodos específicos basándose en direcciones y puertos TCP IP (trabajan a nivel de red). Algunos cortafuegos sólo consisten en un "screening router' entre la red privada e Internet como se observa en la figura 32.

En general permite la comunicación entre múltiples nodos de la red protegida y de Internet. La zona de riesgo es igual al número de nodos de la red protegida y el número y tipos de servicios para los que se permite el tráfico. Es difícil controlar los daños que pueden producirse dado que el administrador de la red debe examinar regularmente cada host para buscar trazas de ataques

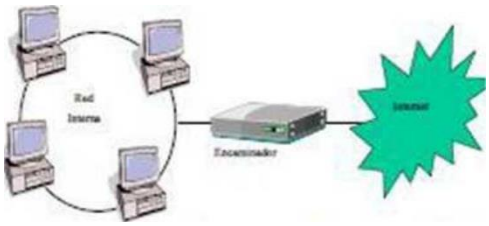


Figura 32: Topología de un corta fuego con enrutador con filtrado (Screemng Router)

Es casi imposible reconstruir un ataque que haya llevado a la destrucción del cortafuego, e incluso puede ser difícil detectar la propia destrucción, aunque algunos poseen capacidades de registro de eventos para paliar esto. En general responden a configuraciones en las que lo que no está expresamente prohibido, está permitido. No son la solución más segura, pero son muy populares dado que permiten un acceso a Internet bastante libre desde cualquier punto de la red privada.

2.6.4.5 Host con doble conexión (Dual-Homed Host)

Algunos cortafuegos son implementados sin necesidad de un screemng router Para ello se conecta un servidor mediante dos tarjetas independientes a la red que se quiere proteger y a Internet, desactivando las funciones de reenvío TCP IP. Este dispositivo puede ser un bastión host y funcionar como servidor (Web. FTF. ...) tanto para la red interna como para la red externa. Los hosts de la red privada pueden comunicarse con el bastión host. Al igual que los nodos de Internet, pero el tráfico directo entre ambos tipos de nodos está bloqueado

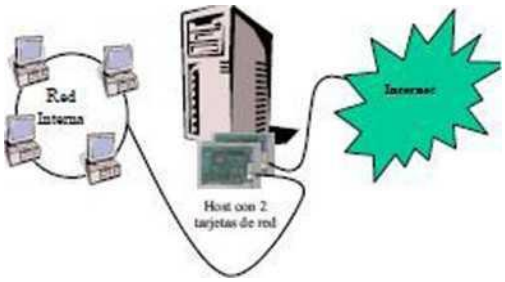


Figura 33: Topología dl cortafuego de host con doble conexión.

En la figura 33 se muestra la estructura de cortafuegos del cortafuego host con doble conexión, el cual es empleada habitualmente debido a que es fácil de implementar. Al no reenviar el tráfico TCP IP, bloquea completamente la comunicación entre ambas redes Su facilidad de uso depende de la forma en la que el administrador proporciona el acceso a los usuarios.

- Proporcionando pasarelas para las aplicaciones
- Proporcionando cuentas a los usuarios en el bastión host.

En el primer caso se está en una situación en la que lo que no está explícitamente permitido, está prohibido. El permiso para el uso de cada aplicación se suele habilitar instalando el software de proxy adecuado para cada una de ellas.

En el segundo caso, el acceso de los usuarios a Internet es más sencillo, pero la seguridad

puede verse comprometida Si un hacker gana acceso a una cuenta de usuario. Tendrá acceso a toda la red protegida. La cuenta de un usuario puede verse comprometida por elegir una contraseña sencilla de adivinar, o por algún descuido. El principal inconveniente es que un hacker mínimamente preparado puede borrar sus huellas fácilmente, lo que hace muy difícil descubrir el ataque. Si el único usuario es el administrador, la detección del intruso es mucho más fácil, ya que el simple hecho de que alguien entrado en el sistema es un indicativo de que sucede algo raro

El aspecto más débil de esta estructura es su modo de fallo. Si el cortafuego es destruido, es posible que un hacker preparado reactive el reenvío TCP IP teniendo libre acceso a toda la red protegida. Para detectar esta situación debe de tener al día las revisiones del software con el fin de eliminar los errores de seguridad. Además, no contiene hacer público el upo y versión del sistema operativo instalado en la máquina para no facilitar el trabajo de los posibles atacantes.

2.6.4.4 Cortafuegos mediante filtrado de Host (Screened Host).

Es la configuración de cortafuegos más común Está implementada usando un bastión host y un screening router. Habitualmente el bastión host está en la red privada, y el screening router está configurado de modo que el bastión host es el único nodo de dicha red que es accesible desde Internet para un pequeño número de servicios con se observa en la figura 34

Figura 34: Topología de cortafuego mediante filtrado de Host.

Como el bastión host está en la red privada, la conectividad para los usuarios es muy buena, eliminando los problemas que suelen aparecer al tener definidas rutas extrañas. Si la red privada es una red local virtual extensa, el esquema funciona sin necesidad de cambios en las direcciones de la red local siempre que ésta esté usando direcciones IP válidas. La zona de nesgo se circunscribe al bastión host y el screening router. La seguridad de este último depende del software que ejecute. Para el bastión host. Las consideraciones sobre segundad y protección son similares a las hechas para un sistema del tipo host de doble conexión.

2.6.4.5 Cortafuegos mediante filtrado de subred (Screened Subnet).

En algunas configuraciones de cortafuegos se crea una subred aislada, situada entre la red privada e Internet. Las formas habituales de usar esa red consisten en emplear screening routers configurados de forma que los nodos dicha subred son alcanzables desde Internet y desde la red privada. Sin embargo, el tráfico desde Internet hacia la red privada es bloqueado.

Figura 35: Topología de cortafuego mediante filtrado de subred

En la subred suele haber un bastión host como único punto de acceso a La misma. En la figura 35 presenta el caso, la zona de riesgo es pequeña y está formada por el propio bastión host, los screening routers que filtran el tráfico y proporcionan las conexiones entre Internet, la subred y la red privada. La facilidad de uso y las prestaciones de la subred varían, pero en general sus servicios se basan en un bastión host que ofrece los servicios a través de gateways para las aplicaciones, haciendo hincapié en que lo que no está explícitamente permitido, está prohibido.

Si este tipo de cortafuegos es atacado en un intento de destruirlo. El hacker debe reconfigurar el tráfico en tres redes, sin desconectarlas, sin dejarse encerrado a sí mismo. Y sin que los cambios sean detectados por máquinas y usuarios. Aunque esto puede ser posible, todavía puede dificultarse más si los routers sólo son accesibles para su reconfiguración desde máquinas simadas en la red privada.

Otra ventaja de este tipo de cortafuegos es que pueden ser instalados de forma que oculten la estructura de la red privada. La subred expuesta es muy dependiente del conjunto de software que se ejecute en el bastión host. La funcionalidad es similar a la obtenida en los casos anteriores, sin embargo, la complejidad de configuración y encaminamiento es mucho mayor.

La subred que incluye el cortafuego y los enrutadores se denomina Zona Neutra o Zona Desmilitarizada *(Demilitarized Zonc - DSIZ).* En esta zona desmilitarizada pueden encontrarse más servidores, bien orientados a dar servicios a usuarios que acceden desde la red externa (red abierta), o bien para facilitar los servicios de proxy y el acceso a internet a

los usuarios de la red interna. Estos servicios pueden residir en una misma máquina, el propio bastión host en las redes como se observa en la figura 36.

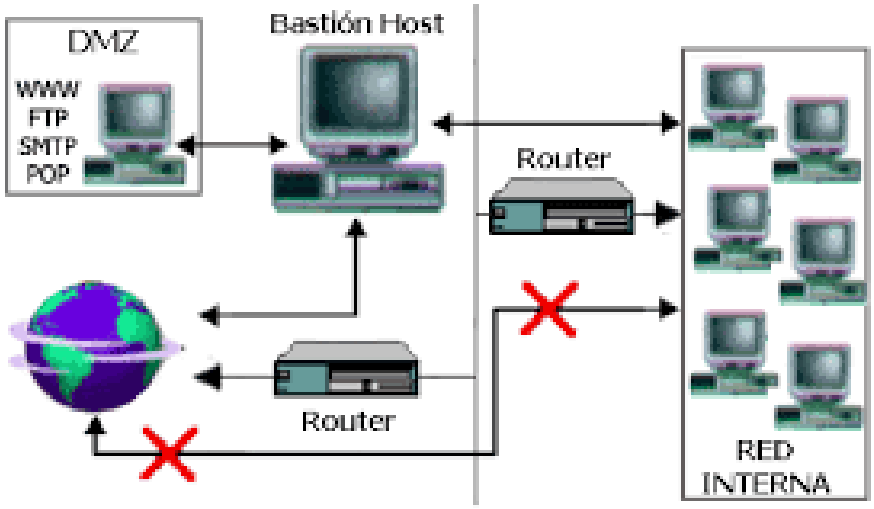


Figura 36: Subred con Zona Desmilitarizada

2.7 Añadir la infraestructura de comunicaciones entre el Maestro, copia de seguridad y Subestaciones

Históricamente, los sistemas de protección y medición se han basado en la comunicación cableada: directa y con conexiones punto-a-punto entre dispositivos electrónicos inteligentes (IEDs). El problema de este enfoque radica en la dificultad de corregir, modificar y actualizar la lógica de control.

Afortunadamente, ETHERNET se ha convertido en el medio preferido de comunicación para cualquier red de comunicación y área local (LAN). La mensajería estándar GOOSE (Generic Object-Oriented Substation Event) es uno de los servicios del IEC61850 que ha contribuido a ir eliminando este cableado punto a punto, simplificando en gran medida los cambios de ingeniería.

Como el diseño de la subestación comienza uniendo, los servicios públicos deben pensar en cómo todas las piezas se comunicarán con otros. ¿Cómo podemos pasar los datos de la subestación a otros lugares? Después de todo esto es lo que se necesita para hacer realidad la promesa de la red inteligente. Clasificación los métodos de redundancia:

- **Dinámica (en espera, en serie)**

La redundancia no participa activamente en el control. Una lógica de conmutación decide insertar redundancia y ponerlo a trabajar
Esto permite:

+ Compartir redundancia y carga
+ Implementar redundancia parcial

+ Reducir la tasa de fallos de redundancia
+ Reducir el modo común de errores
- pero la conmutación lleva tiempo

- **Estática (paralela, de trabajo)**

La redundancia está participando en el control, la Planta elige la unidad de trabajo en la que confía. Esto permite:

+ Proporcionar una transición sin fisuras
+ Ejercer continuamente redundancia y Aumentar la cobertura de detección de fallos
+ Proporcionar un comportamiento a prueba de fallos
- pero la duplicación total es costosa

Subestaciones pueden comunicarse con la estación de control principal y la copia de seguridad estación de control usando una variedad de redes tecnologías. Estos incluyen Ethernet WAN, Celular 3G o WAN MPLS-PPP. Cualquiera tecnología que se elija, debe tener en cuenta lo que es redundante, tales como la adición de otro backup celular. La comunicación sólida mantiene pequeños problemas pequeños y asegura una alta disponibilidad de los sistemas.

Si bien ha habido numerosos esquemas de redundancias desarrollados a lo largo de los años, tres son los que son particularmente útiles para reloj maestro de la subestación de redundancia. Ellos son Protocolo Rapid Spanning Tree (RSTP), Redundancia celular y la redundancia en paralelo Protocolo (PRP).

2.7.1 Protocolo RSTP.

Protocolo de Rapid Spanning Tree (RSTP), definido en el estándar IEEE 802.1w, Este protocolo gestiona enlaces redundantes, reduciendo significativamente el tiempo de convergencia de la topología de la red cuando hay algún cambio o después de un fallo o durante la recuperación de un switch, el puerto o el enlace. En otras palabras, lo detecta y utiliza topologías de red que proporcionan una convergencia más rápida del árbol extensible sin crear bucles de reenvío. RSTP activa puede confirmar que un puerto puede someterse a una transición segura para el envío de estado sin depender de ninguna configuración del temporizador.

RSTP utiliza un anillo físico, pero lógicamente desactiva un enlace a evitar que los mensajes se reenvíen en y el mensaje causando bucle como se observa en la figura 37. Si se detecta una rotura en la red, el enlace desactivado, se vuelve a activar y mensajes luego fluyen a través de la red el uso de la nueva ruta. La ventaja principal de RSTP técnica es que se puede utilizar en cualquier topología de red. Su principal inconveniente, sin embargo, es que los tiempos de recuperación pueden ser tan siempre y cuando 5-20ms por mechón.

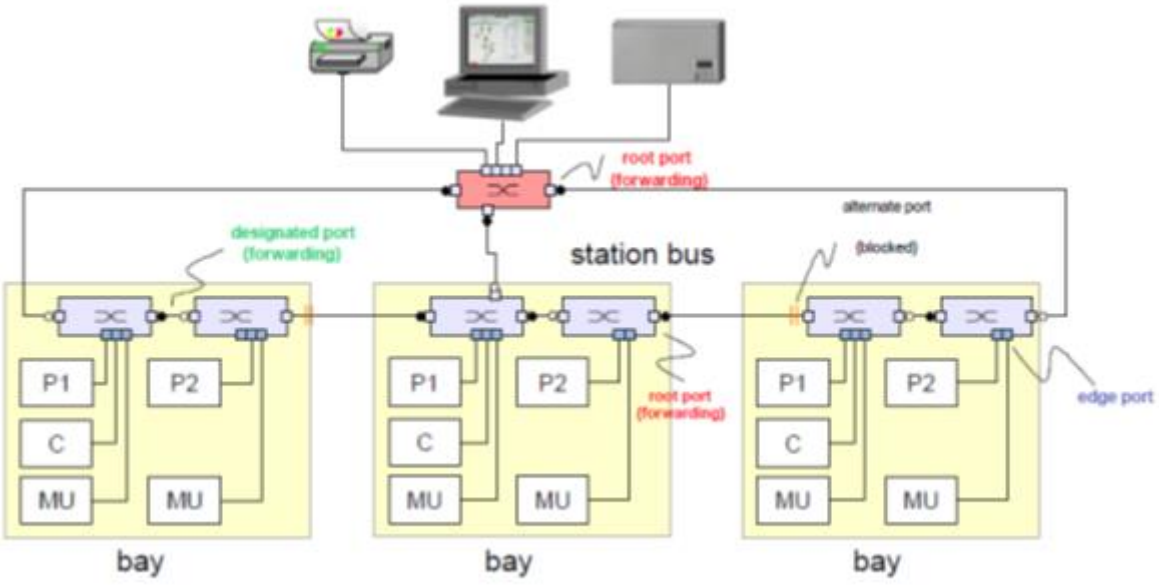


Figura 37: Diagrama del protocolo RSTP.

Rendimiento del RSTP

+ IEEE estándar, probado en el campo, gran mercado, barato
+ Sin impacto en los nodos finales (todos los nodos finales están conectados individualmente
+ Se puede implementar en los nodos si los nodos contienen un elemento puente
- RSTP es en la fama de ser bastante lento (algunos segundos de tiempo de conmutación).

Sin embargo, si su topología es fija, los puentes RSTP pueden aprender la topografía y calcular rutas alternativas en caso de que uno deba fallar. Algunos fabricantes reclaman la recuperación Retrasos <100 ms para configuraciones seleccionadas.

2.7.2 Protocolo de redundancia paralela.

El protocolo de redundancia PRP de acuerdo con la norma IEC 62439-3 se basa en la transmisión doble de cuadros de mensajes en dos redes separadas. Los puntos de acceso pueden conectan hasta dos segmentos de red o dispositivos terminales sin funcionalidad PRP, sin demora, a través de dos redes paralelas.
La fuente o el punto de acceso de red duplican el mensaje que llega del cliente (por ejemplo, un PC); Se envía un cuadro de mensaje a cada una de las dos redes como se muestra en la figura 38. El cuadro de mensaje siempre se transmitirá sin demora, incluso en caso de un fallo, porque no hay necesidad de reconfiguración de la red. El protocolo es transparente para la aplicación en el PC. También pueden utilizarse en condiciones adversas de EMC.

El protocolo PRP ofrecen: tiempo cero de recuperación en caso de fallo en uno de los equipos de la red, cero tramas pérdidas y un robusto mecanismo de monitorización y control de la red gestionada de forma automática por todos los nodos.

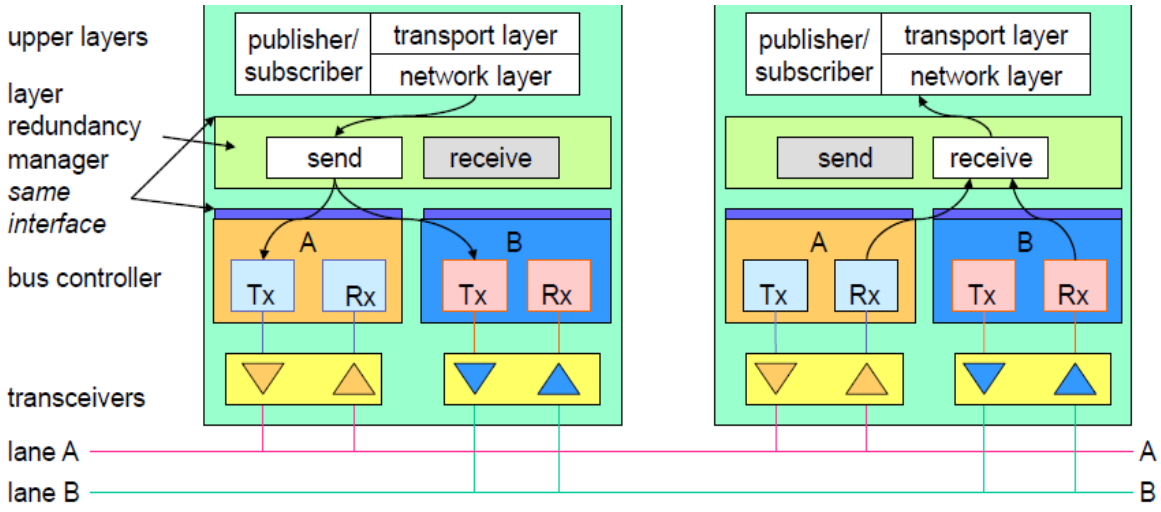


Figura 38: Diagrama del Protocolo de redundancia paralela

En la figura 39 se muestra el funcionamiento del PRP donde: un nodo de origen (DANP) envía simultáneamente dos copias de un marco, una sobre cada puerto. Las dos tramas viajan a través de sus respectivas redes de área local hasta que llegan a un nodo de destino (DANP) con una cierta inclinación tiempo. El nodo de destino acepta la primera trama de un par y descarta el segundo (si es que llega). Por lo tanto, siempre y cuando una LAN está en funcionamiento, la aplicación de destino siempre recibe un cuadro. PRP proporciona la recuperación a tiempo cero y permite comprobar la redundancia continuamente para detectar los fallos que están al acecho.

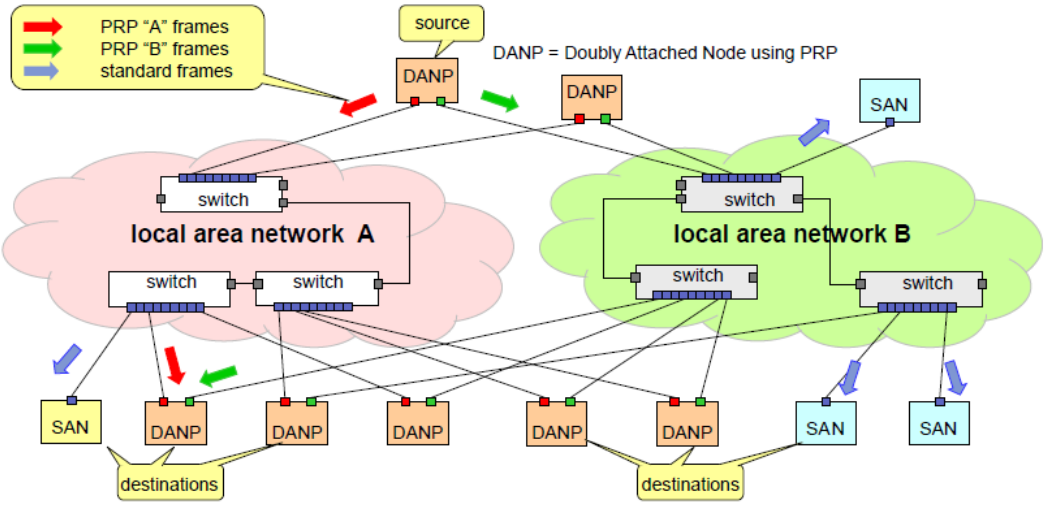


Figura 39: Funcionamiento del protocolo PRP

Para facilitar el rechazo duplicado, los nodos PRP añaden un número de secuencia a los marcos Junto con un campo de tamaño que permite determinar que el marco pertenece al PRP protocolo como se muestra en la figura 40. Este remolque es invisible para las capas superiores (considerado como relleno)
Los receptores descartan duplicados usando una variedad de métodos

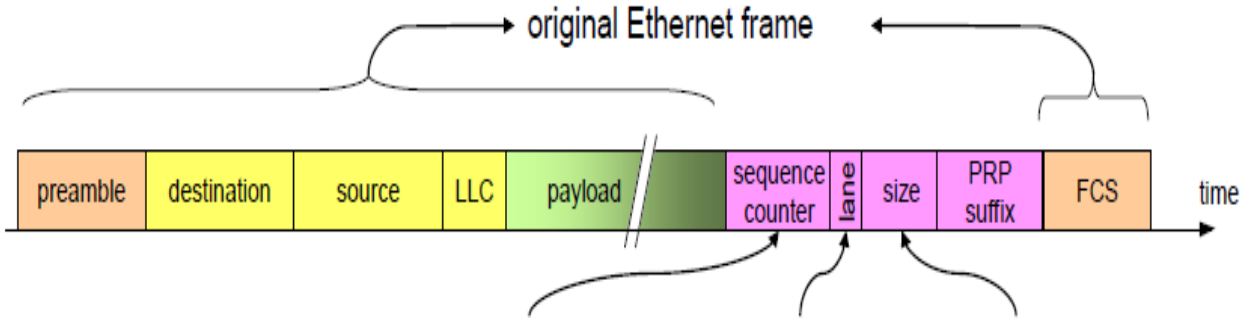


Figura 40: Supresión de duplicados PRP.

Dónde:

- cada trama se prolonga por un contador de secuencia, un indicador de carril, un campo de tamaño y un sufijo * insertada después de la carga útil de permanecer invisible para el tráfico normal.
- El remitente inserta el mismo contador de secuencia en ambos cuadros de un par, y La incrementa en una para cada fotograma enviado.
- El receptor realiza un seguimiento del contador de secuencia para cada uno de cada MAC de origen Dirección desde la que recibe los fotogramas. Marcos con la misma fuente y valor de contador Procedentes de diferentes carriles son ignorados.

Rendimiento PRP

+ PRP permite la conmutación sin problemas, no se pierden marcos
+ Durante el funcionamiento normal, el PRP reduce la tasa de pérdida
+ Los nodos doblemente unidos (DANP) son fáciles de construir
+ SANs pueden comunicarse fácilmente con DANPs
+ PRP comprueba la presencia de nodos por marcos de supervisión periódicos que también indicar qué nodos participan en el protocolo y cuáles no

- Doble coste de red
- SAN de una LAN no puede comunicarse directamente con SANs de la otra LAN
- El tamaño del marco debe ser limitado para evitar que las tramas se vuelvan más largas que el IEEE 802.3. Tamaño máximo (pero la mayoría de los puentes y controladores Ethernet aceptan fotogramas de hasta 1536 octetos)

2.8 Elección de los cables correctos, chaquetas y conectores.

A menudo se pasa por alto en el diseño completo de la infraestructura de comunicaciones los propios cables físicos. Más problemas de comunicación han sido causados por cables o instalación inadecuada de mala calidad que uno puede imaginar.
Se estima que la inversión para cables en una instalación es del 6% del coste total y sin embargo, está comprobado que el 70% de los fallos producidos en una red se deben a defectos en el cableado, por eso es de vital importancia para determinar el cableado apropiado infraestructura que es totalmente compatible con el sistema de requisitos.

2.8.1 Determinar los requisitos de Cobre y Fibra Óptica.

La planificación de las disposiciones físicas a considerar cuidadosamente las distancias y los requisitos de velocidad de datos para determinar la necesidad de cobre y los medios de comunicación de fibra. Se necesita fibra para distancias de más de 100 metros y la señal las tasas de transmisión de 10 Gbps o superior como se observa en la tabla 9.

PROPIEDAD DEL CABLE	PAR TRENZADO			COAXIAL	FIBRA ÓPTICA
	CAT. 5	CAT. 6	CAT. 7		
Ancho de banda	100 MHz	250 MHz	600 MHz	250 MHz	≥10 GHz
Velocidad de transferencia	100 Mbps	1 Gbps	50 Gbps	150 Mbps	≥100 Gbps
Perdida de retorno	25 dB/100 m	25 dB/100 m	25 dB/100 m	25 dB/100 m	3.2 dB/100 m
Resistencia del conductor	19Ω/100 m	19 Ω/100m	19 Ω/100 m	(50, 75, 90) Ω	
Atenuación de acoplamiento	50 dB	75 dB	90 dB	1 a cientos	1.9 dB
Temperatura de funcionamiento	(-20 a 75)° C	(-20 a 75)° C	(-20 a 75)° C	(-50 a 155)° C	(-40 a 70)° C

Tabla 9: Requisitos de operación para los diferentes cables para la comunicación.

2.8.2 El uso del cableado Grado Industrial.

Después de todo de su planificación, se requiere asegúrese de que su infraestructura subestación rendimiento prometido en su entorno hostil. El cable de calidad comercial no está diseñado ni destinado a ser utilizado en ambientes industriales. De acorde a IEC 60529, describe los niveles de protección están indicados por un código compuesto por dos letras constantes “IP”y dos números que indican el grado de protección como se muestra en la tabla 10.

CATEGORÍA	ELEMENTOS	PROTECCIÓN	DESCRIPCIÓN
CAT. 5	**Cable**	**IP20**	Protección contra el contacto entre los dedos y las partes interiores móviles. Protección contra el ingreso de objetos sólidos con un diámetro mayor a 12,5mm.
	Conector	**IP67**	
CAT. 6	**Cable**	**IP55**	Protección contra el contacto entre las piezas móviles interiores y el ingreso de polvo donde no se previene el ingreso completamente, pero el polvo no puede penetrar en tales cantidades que puedan afectar al funcionamiento correcto del mismo y evitar los chorros de agua producidos con manguera y desde cualquier dirección, no deben de causar daño al interior
	Conector	**IP67**	
CAT. 7	**Cable**	**IP55**	Protección contra el contacto entre las piezas móviles interiores y el ingreso de polvo, pero no puede penetrar en tales cantidades que puedan afectar al funcionamiento correcto del mismo y evitando los chorros de agua producidos con manguera y desde cualquier dirección, no deben de causar daño al interior
	Conector	**IP67**	
Coaxial	**cable**	**IP67**	Protección contra cualquier ingreso de polvo y contra chorros de agua producidos con manguera y desde cualquier dirección, no deben de causar daño al interior
	Conector	**IP65**	
Fibra Óptica	**Cable**	**IP66**	Protección contra cualquier ingreso de polvo y contra la cantidad de agua que se introduzca, en casos de inundación esporádica o temporal, no debe dañar el interior
	Conector	**IP67**	

Tabla 10: Grado de protección para los cables y conectores.

2.8.3 El Aislamiento correcto para la Localización

El estándar TIA-1005 (Telecommunications Infrastructure Standard for Industrial Premises) está diseñado para el uso de Ethernet en ambientes complejos, como los que se encuentran en una planta industrial. Si bien ya existía el grupo de tarea conocido como TIA-568 (Commercial Building Telecommunications Cabling Standard), existen diferencias fundamentales entre ambas normativas; en general, la TIA-1005 toma muchos de los aspectos de esta última y los adapta a la complejidad de un ambiente de planta,

donde la polución, vibración y humedad requieren soluciones más robustas de conectividad. Hay tres áreas principales que contribuyen al objetivo de la norma.

La norma permite la planificación y hace recomendaciones sobre las instalaciones de infraestructura para servicios de telecomunicaciones en edificios industriales.

- La potencial exposición de los componentes a ambientes hostiles es el concepto central de esta norma, a diferencia de la TIA-568 que aborda los edificios comerciales, donde el ambiente es más controlado.
- Los requisitos especiales del cableado para las operaciones industriales son el principio fundamental del diseño del documento.

Este término se descompone de la siguiente manera:

1. **M:** Protección Mecánica como impacto, vibración, tensión, torsión.
2. **I:** Ingreso de partículas sólidas y líquidas.
3. **C:** Climático y químico, calor, humedad, radiación solar, químicos.
4. **E:** Interferencias electromagnéticas, descargas en contacto, radiofrecuencia, inducción.

Este parámetro está regulado por el estándar TIA-1005, el que agrega un sub-índice de acuerdo con el área donde será instalado, con la siguiente recomendación en la tabla 11:

Cable	Ambiente	Aplicación
CAT. 5	**M2 I2 C2 E2**	En ambientes intermedios para evitar el ingreso de objetos sólidos con un diámetro mayor a 12,5mm y caída de gotas de agua con hasta un ángulo de 15° de la vertical desde cualquier dirección, no debe causar daño.
CAT. 6	**M2 I2 C2 E2**	
CAT. 7	**M3 I3 C3 E3**	Para aquellos ambientes más severos, como lo son generalmente los de planta evitando contra cualquier ingreso de polvo y en caso de sumergir el equipamiento en específicas condiciones de presión entre 1 y 30 minutos, no debe dañar las piezas internas del mismo.
Coaxial	**M3 I3 C3 E3**	
Fibra Óptica	**M3 I3 C3 E3**	

Tabla 11: Protección de los cables para ambientes industriales.

2.8.4 Elige diseños de cable de alto rendimiento

Con el fin de que la infraestructura pueda funcionar de manera eficiente en el sector industrial, se han tenido que hacer algunas definiciones, desde el punto de vista de la instalación, así como de los requisitos de cableado, y manteniendo el mismo rendimiento requerido por el estándar IEEE para Ethernet sobre par trenzado de cobre. En este sentido, uno de los principales cambios dentro de la normativa TIA-1005, hace referencia a la

posibilidad de utilización de cables de 2 pares. Esta condición limita las tasas de transmisión a solo 10 o 100 Mbps para protocolos IEEE 10 Base-T y 100 Base-T. Otro factor importante dentro de estos ambientes tiene que ver con los rangos de temperatura a los que están sometidos los cables, así como los grados de protección contra el fuego aceptables dentro del proyecto. Respecto de los rangos de temperatura, es conocido el efecto de incremento de la atenuación sobre los 20ºC, por lo que, en muchos casos, no pueden garantizarse los links definidos por la norma TIA-568 de 90 mts.

2.9 Selección de proveedores

La empresa debe evaluar y seleccionar a los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización. Sobre un mercado de proveedores, aquellos que disponen del producto que necesitamos, la empresa evalúa preliminarmente y selecciona aquellos que, en principio, más se ajustan a nuestros requisitos (calidad, precio, etc.) Aquellos que superan el filtro inicial pasan a formar parte de nuestro panel de proveedores. Este panel lo conforman el conjunto de proveedores a los que compramos. Estos proveedores son evaluados continuamente para garantizar que continúan cumpliendo nuestros requisitos y que mejoran de acuerdo con nuestras expectativas.

La norma solicita crear algún sistema de evaluación de los proveedores que nos permita saber en qué medida cumplen nuestros requisitos. Normalmente se suele estructurar la evaluación (en lo que respecta a la calidad) en 2 ámbitos:

- Evaluación del plazo de entrega (el servicio).
- Evaluación de la "calidad" del producto (el producto en sí).

En automoción y otros sectores de producción en serie, se asimilan estas categorías, que son los famosos MPM (Miss Delivery per Million, número de piezas enviadas por el proveedor fuera de plazo por cada millón de piezas enviadas) y PPM (Part per Million, número de piezas defectuosas enviadas por el proveedor por cada millón de piezas enviadas).

Se suelen calcular estos 2 indicadores con todos los proveedores, hasta el punto de que podemos ver en la recepción de muchas grandes empresas listados con los peores proveedores expresados en PPM. El mantenimiento y la utilización de estos 2 indicadores pueden ser los elementos principales de un sistema de evaluación y selección de proveedores. Estos indicadores pueden ser sustituidos, como es normal, por otros que se ajusten mejor a las necesidades de la organización, incluso asignar indicadores distintos en función del proveedor o el producto. Otra forma de evaluar a un proveedor puede hacerse por medio de encuestas, en este caso no es lo más recomendable a menos que se quiera obtener información sobre su capacidad, su gama de productos, etc.

Es válido para muchos auditores de certificación aceptar a todo proveedor que esté certificado ISO 9001 sin más limitación, sin embargo, se recomienda para la imagen de las

entidades de certificación que sus certificados fueran garantía absoluta de satisfacción con el cliente.

Aquí hay algunos factores a considerar cuando se selecciona de un proveedor de equipos de redes subestación

- Utilizar un proveedor que ofrece todo, desde cables, conectores a los conmutadores, enrutadores, y dispositivos de seguridad elimina la necesidad para múltiples gestores de proyectos de diferentes organizaciones.
- Los ingenieros de aplicaciones con experiencia en la organización proveedor debe revisar su solicitud. La mayor parte de control de procesos utilidad y aplicaciones industriales no incluyen datos suficientes para venir en cualquier lugar cerca de La capacidad de Ethernet. Sin embargo, desea estar seguro de que va a tener la capacidad de sobra y que las áreas de riesgo se han tratado en el diseño de la red.
- Trabajar con una organización que tiene la capacidad de proporcionar capacitación a los empleados. También, busque una empresa que utiliza herramientas de diseño para operar los controles vías ingenieros y trabajadores de mantenimiento tanto trabajar y pensar.
- Un proveedor con experiencia específica que fijan las subestaciones y los protocolos industriales
- proporcionarán la mejor recuperación de la inversión en las inversiones en tecnologías de seguridad.
- Un proveedor que ofrece la certificación de red con garantías extendidas será de gran contribuir a la subestación de mejoras futuras.

2.10 Buena Gestión de Proyectos

La gestión de proyectos es la clave para la implementación exitosa de la subestación diseño y automatización. Si no se administran el proyecto adecuadamente, podrían pasos importantes pasarse por alto causando problemas mucho más grandes en el futuro.

Desde la ingeniería básica hasta la puesta en marcha del sistema de control llave en mano. La empresa contratista debe ofrecer servicios integrales que incluyen la construcción de armarios de medición, protección y comunicaciones, la puesta en marcha de sistemas o la formación a ingenieros de medición y protección.

El contratista debe tener Conocimiento, flexibilidad, capacidad para gestionar proyectos de forma integral desde la ingeniería básica hasta la validación, puesta en marcha del sistema y un profundo conocimiento de aplicación. Son las claves que diferencian la oferta del contratista, permitirá ofrecer respuestas ajustadas a las necesidades de cada instalación y aseguran la escalabilidad futura del sistema. Para ellos debe implementar siguientes fases en dicho proyecto.

1) **Ingeniería Básica**
   - Análisis información recibida del cliente.
   - Elaboración de la lista preliminar de documentación.
   - Requisitos preliminares de las protecciones.
   - Esquemas preliminares de equipos. Esquemas dimensionales.
   - Arquitectura del sistema. Comunicaciones.
   - Reuniones o contactos frecuentes o incluso la visita a la instalación caso de tratarse una remodelación
2) **Ingeniería de Detalle**
   - Lista detallada de documentos.
   - Diagrama funcional unifilar de Protección y Medición.
   - Diagramas funcionales.
   - Documentación de fabricación de los paneles.
   - Esquema de Arquitectura de Comunicaciones.
   - Lista de cables.
   - Base de Datos.
   - Diagramas Lógicos.
   - Protocolo de Pruebas. FAT y SAT.
   - Manual de Operación.
   - Manual de Mantenimiento.
   - informe de Documentación técnica de los equipos.
   - informe de Calidad.
   - Estudio de Selectividad y Coordinación.
   - Diagramas de Interconexión entre los paneles de Control y Protección y el resto de los equipos de la Subestación (medida, protecciones, control y telecomunicaciones).
3) **Programación de equipos**
   a) Ensamblaje de armarios
   b) Sistemas de Protección y Control:
      - Configuración de la lógica de control y protección siguiendo los diagramas lógicos aprobados.
      - Configuración de los protocolos de comunicaciones con el sistema de supervisión.
      - Configuración de los protocolos de comunicaciones con los IED´s y entre ellos.
      - Configuración de los parámetros y funciones de protección de acuerdo con el Estudio de Coordinación.

   c) SCADA / HMI
      - Configuración de la adquisición de datos de los equipamientos siguientes:
      - Desde los IEDs.
      - Comunicaciones con otros equipamientos como UPS´s, SSAA, etc.

- Configuración de los protocolos de comunicaciones con los sistemas de supervisión remotos (Despachos Centrales de Operación) (DNP3/IEC101/IEC104/IEC61850).
- Configuración de la Base de Datos.
- Configuración de la interface de Operación.

4) Integración y Pruebas en Fábrica

- Comprobación del cableado, interconexiones y modo de operación siguiendo lo definido en la ingeniería de detalle del proyecto.
- Comprobación de las fuentes de alimentación tanto en AC como en DC.
- Comprobaciones de las tensiones e intensidades en los puntos de test definidos en la ingeniería.
- Pruebas individuales de los equipos de protección y control con maletas de pruebas.
- Pruebas individuales de los equipos de control (cuando existen separados de las protecciones).
- Comprobación de los trasformadores de alimentación.
- Comprobación de la red de comunicaciones y de la red de sincronización.
- Comprobación de todas y cada una de las señales incluidas en la Base de Datos del Sistema. Se comprueban en las bases de datos locales en los HMI y en el SCADA.
- Comprobación de las comunicaciones con el Despacho Central (en las FAT se usa un simulador).

5) SAT, Puesta en Operación & Formación

a) Pruebas en la Instalación y puesta en marcha
   - Ejecución de las pruebas definidas en el Protocolo de Pruebas SAT y que prácticamente son una repetición de las realizadas en fábrica.
   - Puesta en marcha de la instalación.

b) Formación
   - Procesos de formación de los profesionales encargados de la operación de la instalación.
   - Cursos enfocados al uso del hardware, software y prestaciones y funcionalidades presentes en el sistema que se acaba de poner en marcha.

CAPÍTULO III

Propuesta de Laboratorio de interoperabilidad según el Estándar IEC – 61850

3.0 Laboratorio de Pruebas IEC-61850.

En el presente capítulo se presentan los requerimientos que se aplican a las Pruebas de los equipos según IEC – 61850, sean estos IEDs, Switchs , basando estos procedimientos en normas internacionales que nos permitan una normalización en el país para realizar ensayos en lo equipos de protección y medición, tanto de interoperabilidad, sincronismo, etc. Las pruebas deben dar como resultado parámetros que permitan determinar el estado funcional y corroborar las características de rendimiento de los equipos que ya estén operación, así como equipo nuevo que entre en el país para poder verificar sus datos de placa y certificarlos.

3.1 Criterios para la creación de un laboratorio.

Con el propósito de dar vida a un laboratorio basada en la norma IEC 61850 se deben tomar en cuenta no solo los requisitos de software y hardware con los que debe contar sino también el sitio o el ambiente en donde estará instalado dicho laboratorio esto debido a que puede afectar los resultados obtenidos en la pruebas realizadas, los factores a tomar en cuenta son:

- Criterios Ambientales
- Fuentes de Ruido
- Consideraciones Climáticas
- Nivel de Humedad
- Iluminación del área de trabajo
- Temperatura
- Presión
- Seguridad industrial para las personas operarias

En este apartado se definirán cada uno de los factores que puedan influir en los resultados a obtener en un laboratorio de pruebas.

3.1.1 Criterio Ambiental.

Para la localización del laboratorio de pruebas se debe considerando que, la construcción o la obra civil de esta no afecten las condiciones ambientales del lugar; a la vez, un terreno que no sea muy perjudicial para las instalaciones del laboratorio, como, por ejemplo, evitar lugares con altos índices de sal en la atmosfera, a la vez la construcción no debe afectar a los recursos ambientales importantes como la fauna o flora.

3.1.2 Fuentes de Ruido Audible.

Este factor se debe tomas muy en cuenta ya que en una subestación real los ruidos pueden ser muy viniendo de diferentes fuentes, a diferencia de los ruidos que se puedan generar en un laboratorio de prueba. El ruido audible de las subestaciones es causado principalmente por los interruptores y transformadores. De acuerdo con SIGET que según el artículo 69 se

establecen las consideraciones generales, a fin de limitar la contribución de las subestaciones transformadoras a la contaminación por ruido al medio ambiente, se debe procurar que los equipos que se adquieran por parte de las empresas de distribución sean construidos de tal forma que los naturales niveles de ruido que estas máquinas provocan sean limitados y que las subestaciones sean construidas de tal forma que la propagación del ruido sea limitado al ambiente circundante, SIGET da como referencia la siguiente tabla para delimitar los niveles de ruido según el área donde será instalo

ZONA DE UBICACIÓN DE LA SUBESTACIÓN	NIVEL MEDIO DE RUIDO EN (DB)
Hospitales, escuelas y bibliotecas	Menores de 30
Viviendas	30 a 40
Comercial	45 a 55
Oficinas (con máquinas)	45 a 70
Oficinas (sin máquinas)	50 a 75
Industrial	Industrial 76 a 95

Tabla 12: Niveles permisible de ruido

3.1.3 Nivel de Humedad.

Las condiciones de humedad pueden ser un factor clave en los ensayos que se realizan en los laboratorios, ya que pueden afectar algunos parámetros del funcionamiento de los equipos. En casos muy específicos, cuando un equipo electrónico posee humedad pueden generarse daños irreparables al equipo, o generar datos erróneos.
Como consideraciones sobre límites de porcentaje de humedad, en base a lo establecido dentro de las normas que regulan las buenas prácticas de los laboratorios, establecen una relación entre la temperatura ambiente y la humedad relativa, ya que estas van ligadas estrechamente una con la otra. A continuación, se presentan los límites de humedad en base a norma que deben cumplir en un entorno de laboratorio de pruebas.
La norma ISA RP52.1, establece que como buena práctica para los porcentajes de humedad relativa ésta se debe encontrar entre el 20-55% HR cuando la temperatura ambiente sea de 23° C.

3.1.4 Temperatura.

Para obtener buenos resultados en un laboratorio de pruebas, es necesario el control de las condiciones ambientales y su estabilidad temporal dentro de estrechos rangos de tolerancia, siendo esto además requisitos técnicos que establecen normas internacionales como la ISO/IEC 17025 "Requisitos Generales para la competencia de los laboratorios de ensayo y calibración" para el fiel funcionamiento y acreditación del laboratorio de ensayos. La calidad del servicio de medición, entendida como la exactitud, veracidad o precisión de los resultados está fuertemente influenciada por las magnitudes de las variables externas, que en la mayoría de los casos la fuente de mayor incidencia es la temperatura en la sala o entorno de medición.

Algunos instrumentos de medición realizan compensaciones térmicas en base a sus sensores, sin embargo, por más que los sensores y los efectos de la compensación sean de alta calidad no están exentos de errores e incertidumbre en los resultados. Aunque se debe tener en cuenta que la condición de compensación de los instrumentos antes mencionada ayuda a solucionar una parte del problema sobre la inexactitud de los resultados, ocasionados por límites fuera de los rangos de temperatura permisibles según recomendaciones y estándares internacionales en cada procedimiento de prueba. Para establecer las restricciones se deberá considerar las siguientes observaciones recopiladas de diversas normas que regulan de manera importante el ambiente de los laboratorios.

Una restricción de temperatura se toma de la norma IEEE-119 -1974, ya que esta define que se determinara en base a los estándares que el apartado 8.1 establece, pero si en algún caso este no aplica, deberán tomarse como temperatura ambiente lo que establece dicha norma a continuación: "podrá tomarse como temperatura ambiente de referencia el promedio de la temperatura ambiente observada durante los últimos 15 minutos de la prueba y no deberá exceder una variación de ± 5°C. Para esta medición deberán usarse alguno de los equipos especificados en la norma. La norma ISA RP52.1 establece como temperatura para los laboratorios recomendada de 23°C ±1.5°C

3.1.5 Presión.

La presión atmosférica es otra condición ambiental que se debe tomar en cuenta en los laboratorios, esta variable es sumamente importante en los laboratorios donde se dan procesos meteorológicos ya que la variación de presión es un dato clave en dichos procesos. Así como en laboratorios donde se realizan procesos meteorológicos la variable presión se debe monitorear constantemente hay laboratorios de pruebas que no necesitan ese monitoreo, pero si se debe realizar la medición de dichas variables y ser agregado este valor en un apartado de la hoja de resultado de las pruebas.

Se debe considerar que la presión varía según la altitud, cuando se conoce la presión típica en un lugar determinado, es decir, la presión que se tiene por la altitud en que se encuentra ese lugar; analizar los cambios de presión en la mayoría de los casos es relativamente fácil. Para obtener o determinar la presión básica de un lugar basta con tomar una serie de medidas y obtener un promedio.

Se debe tener mucho cuidado de no confundir la presión atmosférica con la presión barométrica a continuación se dan unos conceptos breves;

Presión atmosférica: presión que ejerce la atmosfera que rodea la tierra sobre todos los objetos que se hallan en contacto con ella. La presión atmosférica cambia con la altitud, a mayor altitud menor presión, un amento en altitud de 1000m representa una disminución de presión atmosférica de aproximadamente 100 ha.
Presión atmosférica normalizada: presión ejercida por la atmosfera bajo condiciones normalizadas, igual a 1013.25hPa (760mmHg). La cual idealmente se presenta a una altitud de 0 m.s.n.m, temperatura ambiente de 20 °C, humedad de 65 %HR y densidad de aire de 1.2kg/m^3.
Presión barométrica: presión atmosférica local más una corrección por la altitud geopotencial local. La presión barométrica oscila alrededor de la presión atmosférica normalizada (1013.25 ha).

3.1.6 Partículas de polvo.

Este parámetro es importante tomar en cuenta en el ambiente de desarrollo del laboratorio es las partículas de polvo. Las recomendaciones sobre las partículas de polvo están básicamente fundamentadas en mantenimiento higiénico y sus consideraciones, esta es la mejor práctica para evitar los efectos adversos causados por ambientes con polvo. En medidas de baja frecuencia, la acumulación de polvo en superficies aisladas o conductivas puede influir en las mediciones. Muchos estándares de laboratorio utilizan construcciones de contacto expuesto, haciendo que la limpieza repetida sea necesaria en el área. El polvo puede promover corrosión y desgaste, así como contaminar muestras y mediciones erróneas en los laboratorios. La norma **ISA-RP52.1-1975** "Condiciones ambientales para laboratorio (recomendaciones prácticas)" establece recomendaciones sobre estos parámetros que se muestran a continuación.
Requerimientos:

- Menos de 7 x 10^6 partículas/m^3 de más de 1 μm.
- Menos de 4 x 10^7 partículas/ m^3 de más 0.5 μm.
- Inexistencia de partículas más grandes de 50 μm.

Para el cumplimiento de los requisitos antes mencionados una alternativa es la utilización de un filtro HEPA "High Efficiency Particle Arresting", los filtros HEPA quitan al menos un 99.97 % de partículas de 0.3 micrómetros y son generalmente más eficaces para partículas que son más grandes o ligeramente más pequeños.
Estos filtros estas compuestas por fibra de vidrio y con diámetros entre 0.20 y 0.50 micrones, entrelazadas de forma aleatoria y espaciadas entre si más de 0.3μm.

3.1.7 Aterrizaje para cargas estáticas.

La acumulación de cargas estáticas en exposiciones de campos electromagnéticos en el equipo o materiales y sobre el personal de operación produce un potencial serio en los lugares en los que se encuentran líquidos o gases inflamables, fibras o desperdicios.
La generación de electricidad estática no se puede prevenir, pero se puede mitigar y controla. Los métodos que se usan son:
Aterrizaje y conexión. Muchos problemas de estática se pueden resolver uniendo las diferentes partes del equipo y aterrizando el sistema completo.

La humedad o humedad relativa controla la conductividad de la superficie de estos materiales aislantes. A mayor humedad, mayos conductividad. Cuando la humedad relativa es de 30% o menos, los mismos materiales se secan y se convierten en buenos aisladores; se comienzan a notar las manifestaciones estáticas y se pueden generar chispas estáticas.
Ionización. En el proceso de ionización, las moléculas de aire están sobre-tensionadas, los electrones se separan de sus moléculas. Los electrones son negativos y las moléculas quedan con cargas positivas.

Calzado y rodos conductivos. Se usan en combinación con el piso conductivo. El equipo móvil debe tomar contacto directamente con el piso o a través de los rodos conductivos de hule. Se debe verificar su resistencia siempre, antes de entrar a las áreas de trabajo.
Precauciones especiales. Además de los pisos y calzado conductivos, se pueden considerar otros controles como: usar ropa que produzcan estática baja, establecer procedimientos rígidos de operación.

Si bien en la práctica de la toma de tierra eléctrica Los sistemas están bien establecidos, todas las implicaciones de protección de la electricidad estática no siempre se entienden. El objeto de la protección de la electricidad estática es Proporcionar un medio por el cual cargas de electricidad estática, separados por la causa que sea, puede recombinarse sin causar daños. En orden Para una carga de electricidad estática para convertirse en una fuente de problemas, debe tenerse en cuenta las siguientes condiciones:

- Debe haber un medio de generación de electricidad estática.
- Debe haber un medio de acumulación de una carga estática capaz de producir la ignición.
- Debe haber un medio de descarga de chispa de la carga acumulada.
- Debe haber una mezcla inflamable o la atmósfera en la ubicación de la chispa de descarga para constituir un riesgo de explosión o incendio.
- El potencial estático se debe controlar para no constituir un peligro para el personal.
- La carga estática debe llevarse a cabo de forma continua para constituir un compromiso de las comunicaciones clasificadas.

3.1.8 Iluminación

Una adecuada iluminación es primordial en cualquier ambiente de trabajo, ya que ésta permite un mejor registro de los datos, pero también debe de tenerse el cuidado de elegirse una que sea cómoda para trabajar. Ya que si la iluminación es muy cálida podría producir un ambiente propicio para el descanso mientras que si es muy fría podrá volverse un ambiente incómodo para trabajar. Para evitar esto se establecen las recopilaciones en base a normas para lograr el ambiente idóneo dentro del cual se podrán realizar las pruebas de laboratorio.
La norma ISA 52.1 establece en la sección 5.5.1 sección de iluminación podemos ver: “La especificación "general" de 1000 lux (lúmenes por metro cuadrado). Probablemente la consideración más importante que debe tenerse en cuenta son las otras condiciones de laboratorio o equipos y configuraciones que pueden causar degradación en el rendimiento total de medición. “

Es de considerar que debemos combinar luz natural y artificial para poder lograr los niveles establecidos ya que tener tanta iluminación puede producir cambios en la temperatura ambiente.
Otra sugerencia que se permite considerar dentro de esta norma es la siguiente: la iluminación de intensidad variable. En algunos laboratorios a número de mediciones diferentes deba realizarse bajo una fuente de luz. En el cual podría variar intensidad de esta fuente de luz. Por ejemplo, el requisito de la iluminación para leer un medidor puede ser 125 lúmenes por pie cuadrado mientras que en otro tiempo en el mismo banco un osciloscopio requeriría sólo 30 pie-candela de iluminación.
De los cientos de situaciones de iluminación, ninguno se refiere específicamente a la de un laboratorio de medición. Sin embargo, varios son similares a las condiciones de un laboratorio de medidas físicas, el diseño y la instalación deben proveer no sólo una cantidad suficiente de luz, sino también la dirección correcta de la luz, difusión y protección de los ojos. Es conveniente y práctico limitar proporciones de brillo entre las áreas de tamaño considerable a continuación se muestra estas consideraciones.

Niveles	Condiciones
3 a 1	Entre tarea y alrededores adyacentes
10 a 1	En la tarea y superficies oscuras más remotas
1 a 10	Entre la tarea y superficies más remotas
20 a 1	En las fuentes de luz o ventanas y superficies junto a ellos
40 a 1	En cualquier lugar dentro del campo de visión normal

Tabla 13 Proporciones de brillo.

3.2 Sistema de puesta a tierra o red de tierra.

El cuerpo humano es un buen conductor eléctrico, razón por la cual al verse sometido a una diferencia de tensión se originarían corrientes circulantes a través de él, así mismo la actividad biológica del mismo se encuentra estrechamente relacionada a variaciones de tensión, puesto que cada célula del cuerpo humano se caracteriza por una diferencia de potencial entre la parte externa y la parte interna de su estructura. Por lo mencionado anteriormente podemos concluir que el paso de una corriente de origen externo a través de los órganos del cuerpo humano, pueden alterar las funciones vitales y dañarlos irreparablemente.
Si una persona está en contacto con elementos energizados estará sujeta a sufrir un choque, que no es más que una sensación desagradable ocasionada por el paso de corriente eléctrica en el cuerpo, un paso de corriente menor a 1 amperios por el cuerpo humano puede ocasionar graves daños al organismo. Este riesgo está presente hoy en día bajo múltiple circunstancia, esto debido al uso casi vital de la electricidad en las sociedades humanas para su desarrollo y mejoras en la calidad de la vida. Por lo dicho anteriormente y al no poderse desligar de la fuente de energía eléctrica es necesario crear medios para su generación, transmisión, distribución y consumo de forma segura, para ello surge la necesidad de realizar un buen sistema de puesta a tierra.

3.3 Consideraciones a tomar en cuenta en el diseño de un sistema de puesta a tierra.

3.3.1 Conductor neutro y conductor de tierra.

En el diseño de sistemas de puesta a tierra se tiene que tener cuidado de no confundir o pensar que es lo mismo decir conductor neutro y conductor de puesta a tierra. El conductor neutro es para transportar corrientes de desbalance en los sistemas trifásicos, así como las corrientes de retorno en los sistemas monofásicos, el conductor de tierra su objetivo es proporcionar la conexión a tierra para operación y protección del sistema.

En muchos sistemas eléctricos el neutro se aterriza, Según **NEC** el único punto en donde el neutro debe ser aterrizado es en la barra de neutro del tablero principal de distribución.

3.3.2 Factores que afectan la resistencia de toma de tierra.

Depende de los siguientes aspectos: Material del terreno, Granulometría del material, Humedad, Temperatura, Salinidad.
Cuando se realiza un diseño de Sistema de puesta a tierra se supone que el diseño es seguro cuando la resistencia de conexión a Tierra es inferior a un valor recomendado.

3.3.3 Resistividad del terreno.

La resistividad del terreno es la resistencia que presenta al paso de la corriente un cubo de terreno de 1 metro de arista. Se mide en Ω-m.
Según los cálculos físicos el valor de la Resistencia del material circundante es:
ρ = R * A / L (Ωm2/m) (Ω-m)
ρ = Resistividad del material
L = Longitud del material
A = Área perpendicular al flujo de corriente.

3.3.4 Elementos que influyen la resistividad del terreno.

Los elementos que influyen en la resistividad del terreno son los siguientes: Naturaleza del terreno, Humedad, Temperatura, Salinidad, Estratigrafía (Capas del terreno), Variaciones estaciónales y Compactación.

3.3.5 Resistividad vs temperatura.

A medida que disminuye la temperatura aumenta la resistividad. Esto se debe a que el agua en estado sólido se comporta como un conductor de resistividad muy alta. A medida de que la temperatura aumenta el agua pasa de estado sólido a líquido, disminuyendo así su valor de resistividad.

Es importante observar que un aumento de la temperatura no implica que el suelo tenga un valor de resistividad bajo puesto que, para ello, se requiere que este posea agua en los poros de las rocas que la conforman.

3.3.6 Resistividad vs presión.

El efecto de la presión sobre la resistividad del suelo es opuesto al producto por la temperatura ya que, al aumentar la presión, los poros de las rocas contenidas en el suelo se cierran disminuyendo así su humedad produciendo que la resistividad aumente. La relación resistividad vs presión se muestra en la Figura

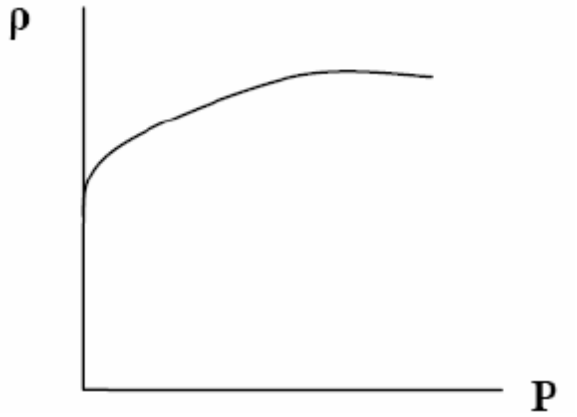


Figura 41: Relación de resistividad vs presión.

3.4 Resistencia de la red de tierra según el NEC y según acuerdo N°29-E-200 de la SIGET.

La conexión a tierra debe tener una baja resistencia o impedancia, la cual debe ser al menos, menor a (según NEC):

- 10 Ω para sistemas de potencia.
- 5 Ω para sistemas de bajo voltaje
- 1 Ω para sistemas electrónicos

Con esto nos aseguramos de que la función básica de la puesta a tierra se cumpla.
En la tabla se presentan los valores máximos permitidos de resistencia de tierra de una subestación en función de su capacidad tomadas de la tabla 22 del acuerdo N°29-E-2000 " Norma técnica de diseño seguridad y operación de las instalaciones de distribución".

Capacidad de subestación (MVA)	Resistencia de la red a tierra(Ω)
menor de 0.05	12
0.05-0.1	6
0.1-0.50	2
0.50-1	1.5
1 a 50	1
50-100	0.5
mayor de 100	0.2

Tabla 14: Niveles de resistividad en subestaciones

3.4.1 Método para calcular la resistividad del terreno

3.4.1.1 Método de los 3 puntos.

Este es el método más empleado para la medición de la resistencia de sistemas de tierra. Este método también es conocido por algunos autores como método de caída de potencial.
El medidor de uso común para la prueba de resistencia de tierra es el óhmetro de tierras que debe tener una calibración vigente.

El método consiste en hacer circular una corriente entre dos electrodos: uno llamado **E** que corresponde a la red de puesta a tierra y un segundo electrodo denominado de corriente (**C**) y medir la caída de potencial mediante otro electrodo denominado de potencial (**P**).
La resistencia de los electrodos se desprecia, porque la resistencia del electrodo **C** no tiene determinación de la caída de potencial V. La corriente I se comporta como constante. La resistencia del electrodo **P**, hace parte de un circuito de alta impedancia y su efecto se puede despreciar. La figura 42 muestra las distancias correctas que deben estar los electrodos.

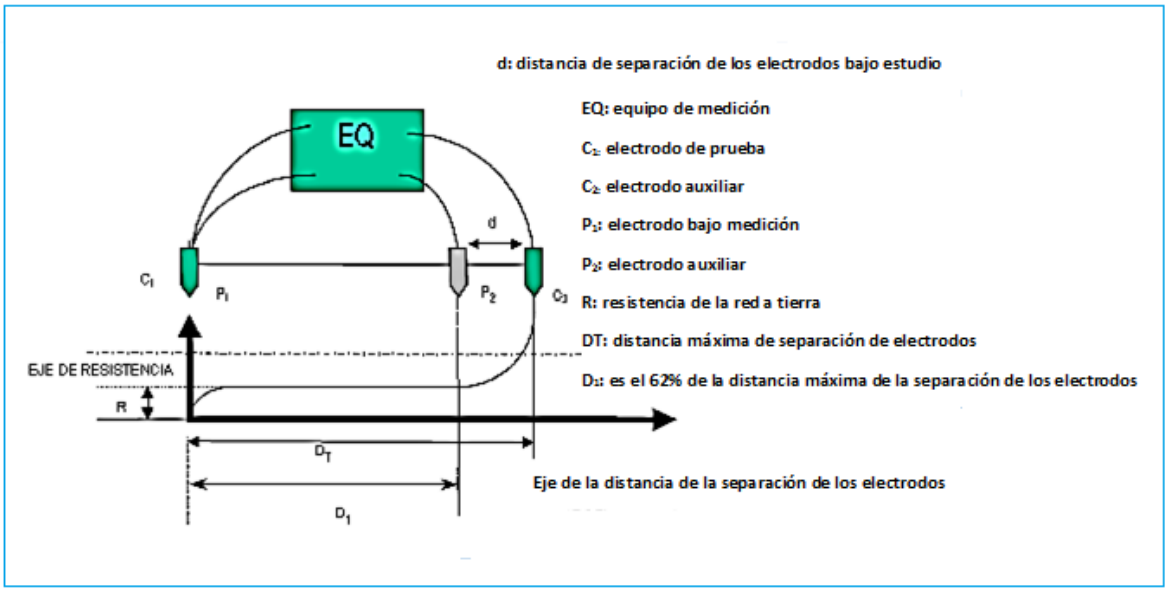


Figura 42: Método de los 3 puntos para medir la resistencia de un sistema de puesta a tierra.

3.4.1.2 Pasos realizar el método de los 3 puntos

Los electrodos de potencial y corriente (**C** y **P**) deben clavarse a una profundidad de 20 a 60 cm aproximadamente, y deben estar firmemente clavados en el suelo y tener un buen contacto con tierra.

Con el fin de obtener una medida correcta, los tres electrodos deben estar bien alineados y la distancia entre **E** y **P** debe ser un 62% de la distancia entre **E** y **C** (Distancia Total, **DT**). Esta distancia está basada en la posición teóricamente correcta para medir la resistencia exacta del electrodo para un suelo de resistividad homogéneo.
La localización del electrodo **P (figura 43)** es muy importante para medir la resistencia del sistema de puesta a tierra. La localización debe ser libre de cualquier influencia del sistema de puesta a tierra bajo medida y del electrodo auxiliar de corriente. La distancia aconsejable entre el electrodo de puesta a tierra **E** y el de corriente **C** es no menos a 20 metros. Para comprobar la exactitud de los resultados y asegurar que el electrodo bajo prueba está fuera del área de influencia del de corriente, se deberá cambiar de posición el electrodo de potencial **P**. La primera medición se hace con el electrodo **P** a la distancia 62% de DT. La medición se debe repetir a las distancias de 62% $de\ DT$ + 10 % del 62% $de\ DT$ y 62% $de\ DT$ − 10 % del 62% $de\ DT$. Si los dos resultados obtenidos no difieren en más de un 10 % con respecto a 0.62 x DT, entonces el primer resultado será el correcto. En caso de una diferencia superior al 10 % se debe incrementar la distancia (DT) entre el electrodo de corriente **C** y el electrodo de puesta a tierra bajo prueba **E**, repitiendo el procedimiento anterior hasta que el valor de resistencia medido se mantenga casi invariable

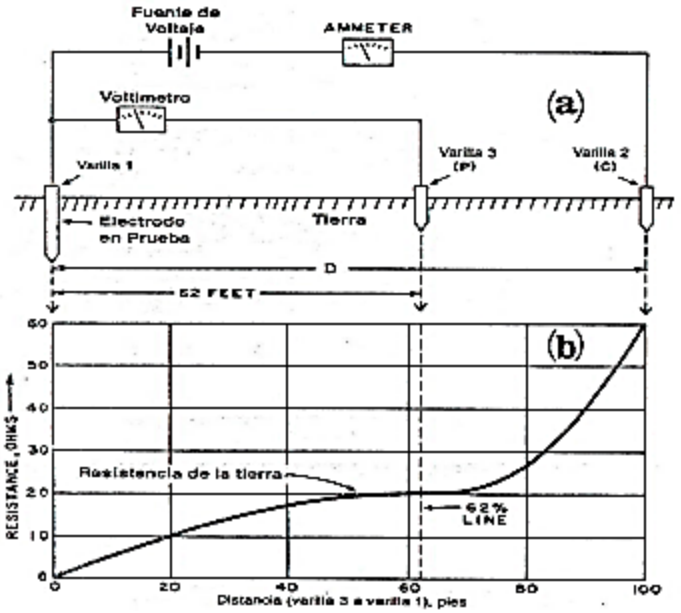


Figura 43: Principio de una prueba de resistencia de tierra

Una excesiva resistencia de los electrodos auxiliares puede impedir que la corriente que debe pasar por el electrodo de corriente **C** pase por el mismo o que no se pueda medir el potencial a través del electrodo potencial **P**. Muchos equipos de medición cuentan con indicadores que parpadean si la medida no es válida.

Esto puede deberse a un mal contacto con el suelo o por elevada resistividad del mismo. En estos casos, se recomienda compactar la tierra que rodea a los electrodos de modo que se eliminen capas de aire entre los mismos y la tierra. Si el problema es la resistividad, se puede mojar el área alrededor del electrodo, con lo que está disminuirá.

3.5 Condiciones de seguridad humana.

Otro aspecto a tomar en cuenta es lo relativo a condiciones de Seguridad e Higiene en que deben mantenerse en un entorno de un laboratorio, a fin de eliminar o controlar los factores de riesgos en los puestos de trabajo, sean estos de naturaleza mecánica o estructural, física o química. Todo con el propósito de proteger la vida, salud, integridad física, mental y moral del personal que realice las pruebas.
Por otro lado, también debemos prevenir condiciones de incendios, para lo cual deberán especificarse la ubicación de un sistema anti-incendio el cual nos permita prevenir daños en las personas y el equipo.

3.6 Señalización e instalaciones con las que debe contar el laboratorio según ley general de prevención de riesgo.

3.6.1 Las puertas de emergencia.

Ley General de Prevención de Riesgos Art.13.- Las puertas y salidas de emergencias deberán cumplir los siguientes requisitos mínimos:

1. Las salidas y puertas de emergencias de los lugares de trabajo tendrán acceso visible o debidamente señalizado.
2. En los accesos a las puertas y salidas de emergencia no se permitirán obstáculos que interfieran la salida normal de los trabajadores.
3. El ancho mínimo de las puertas de emergencia será de uno con veinte (1.20) metros.
4. Las puertas de las salidas de emergencia se abrirán hacia el exterior.
5. Ninguna puerta de emergencia permanecerá con llave de manera que pudiese impedir la evacuación.
6. Las puertas de emergencias que comuniquen a las gradas no se abrirán directamente sobre sus escalones, sino sobre descansos de ancho al menos igual a la de aquéllas.
7. En caso de fallo en el suministro de energía, las vías y salidas de evacuación deberán estar equipadas con iluminación de emergencia.

3.6.2 Equipos de Seguridad y Señalizaciones

Extintores

El laboratorio debe estar dotado de extintores portátiles, debiendo el personal del laboratorio conocer su funcionamiento a base de entrenamiento. Los extintores deben estar señalizados y colocados a una distancia de los puestos de trabajo que los hagan rápidamente accesibles. Deben ser del tipo de fuego ABCD.

Se muestran las siguientes señalizaciones, que se necesita para mantener debidamente el laboratorio, en la figura 44 se muestran las señales para los extintores, en la figura 45 las señales de prohibición, en la figura 46 se observan las señales de advertencia. Posteriormente presentamos en la figura 47 las de obligación y finalmente en la figura 48 es la de terremotos.

Figura 44: Señales de extintores

Figura 45: Señales de Prohibición.

Figura 46: Señales de advertencia.

Figura 47: Señales de obligación

Figura 48: Señales de emergencia.

3.7 Propuesta de equipo hardware y software para un laboratorio basado en la norma IEC – 61850.

Un laboratorio de Pruebas IEC –61850 ofrece pruebas de alcance total para la automatización de subestaciones, EMS, DMS. Pero para poder llevar a cabo las pruebas del laboratorio, es necesario poder adquirir diversas herramientas de software y de hardware en este capítulo se hace una propuesta en particular.

Para la ejecución de un laboratorio de pruebas IEC-61850 en la tabla 15 se detallan las herramientas de hardware y equipo consecutivamente en la tabla 16 se muestra una lista de software utilizados.

Cantidad	Equipos	Fabricantes	Referencia
4	Gateway	Kalkitech	SVNC 3000 S12R6
4	Switch	CISCO	CGS2S20 16S8PC
1	IED	ABB	REF615
1	IED	SEL	351ª
1	IED	ABB	REM620
1	IED	SIEMENS	6MD85
1	Automation controller RTAC	SEL	3505
1	Unidad de prueba universal de relés	Omicron	CMC-356 con opción completa Net-1
2	Computadora	HP	HP 15-AS002LA ENVY i5-6200U/ 2,3 GHz/ RAM 12GB/ DISCO
2	Mesas		1.80 ms X 1.10 ms.
4	Sillas industriales		

Tabla 15: Equipos de Hardware y equipo del Laboratorio

Herramienta	Licencia
Hammer (Test Client)	Hammer (Test Client) to 61850 Test Suite License
Anvil (Test Server)	Add Anvil (Test Server) to 61850 Test Suite License
NPM Solar Winds	1 licencia
Wireshark	Licencia bajo la cual se emite Wireshark es la Licencia Pública General GNU versión 2
Test Universe	1 licencia
Módulo Goose Configuration	1 licencia
Módulo Sampled Values Configuration	1 licencia
IEDScout	1 licencia

Tabla 16: Software del laboratorio

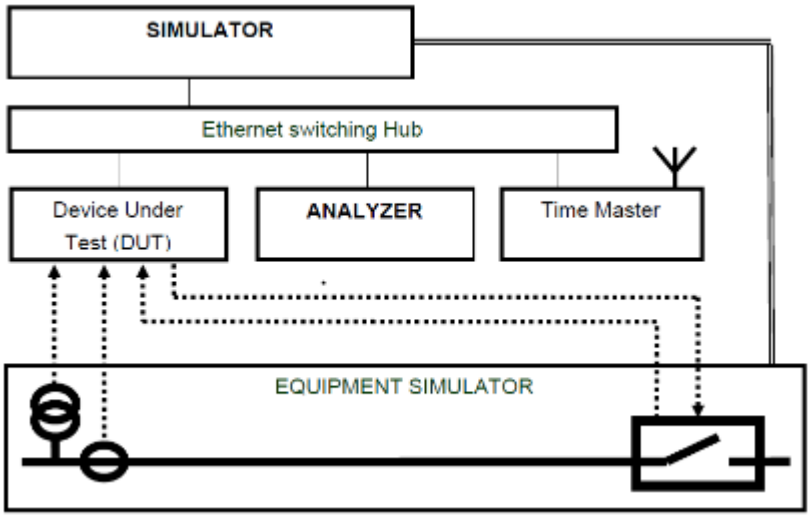


Figura 49: Equipos del laboratorio.

3.8 Especificaciones de Hardware.

3.8.1 Swiches.

Estos equipos garantizan la conformación del anillo de fibra óptica redundante entre los tableros de control y protección, además de ordenar el tráfico de datos en la red de comunicaciones. Los cuales deben cumplir con los requisitos del apartado 2.5

3.8.2 Gateway

El Gateway o puerta de enlace es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes entre varios niveles de comunicaciones.
El propósito del empleo de este equipo es traducir la información del protocolo utilizado en la red de nivel 1 de la subestación al protocolo usado en la red. El equipo propuesto es el modelo Kalkitech SVNC 3000 S12R6 el cual recolecta la información de los controladores y relés de protección mediante el protocolo IEC 61850 y envía esta información bajo el protocolo IEC 60870-5-101, cumpliendo las característica del apartado 2.5

3.8.3 IED’s

Para la integración de las protecciones se utiliza el protocolo IEC – 61850. La información específica de la cantidad de datos disponibles puede ser encontrada en el manual de cada IED. Se Propone los equipos de protección marca SEL, ABB y SIEMENS. Como requisitos para la selección de IED’s que se puedan utilizar en una subestación o en un laboratorio basado en el estándar IEC-61850 deben ser:

- Deben de contar con protocolo de comunicación IEC-61850
- Doble tarjeta de Red

- Puertos Ethernet
- Equipos de protección de tipo multifuncional

3.8.4 Unidad de prueba universal de relés.

La unidad de prueba a utilizar en un laboratorio debe de ser una opción para aplicaciones que necesiten de una gran versatilidad, potencia y amplitud. Con esta unidad deben de realizar una amplia gama de pruebas e incluso comprobaciones de cableado y plausibilidad de los transformadores de corriente, mediante la inyección primaria de altas corrientes desde la unidad de prueba.

Características para la adquisición de una unidad de pruebas universal de relés es:

- Fuentes de corriente muy potentes para prueba incluso de relés electromecánicos de alta carga
- Altas amplitudes de corriente para prueba de relés de 5 A
- Alta precisión y versatilidad para pruebas de relés estáticos y numéricos de todos los tipos
- Red integrada para prueba de dispositivos IED IEC 61850
- Funcionalidad de medida analógica de 10 canales y registro de transitorios (opción)
- Control de ángulo de fase independiente para cada fuente
- 8 entradas binarias, 8 salidas binarias
- Entradas binarias con umbral ajustable (0-350V)

Algunas maletas de prueba que existen y que cumplen con estas características en particular se encuentran: PW636i, POM2-6143, L336i, CMC356, SVERKER 650, etc.

3.8.5 Computadoras Personales

Las computadoras personales a utilizar son necesarias para poder ejecutar el software necesario para la verificación de la red, poder realizar las pruebas de conformidad y de interoperabilidad para dichas actividades los softwares exigen ciertas características de software y de hardware a las computadoras las cuales es necesarias suplir para dichas actividades.

Características necesarias para las computadoras personales:

- Procesador Intel core i7
- Disco duro de 500 GB
- Memoria RAM de 8 GB.
- Windows 7, 8, 10 (64 bytes)

3.8.6 Mesas.

Las mesas forman un papel muy importante dentro de la instalación del laboratorio porque es más que todo donde se pretende localizar el equipo para poder realizar las pruebas a los equipos además que deben de ser lo suficientemente livianas para poder desplazarlas y de esa manera poder tener mejor movilidad dentro de la instalación del laboratorio .

3.8.7 Sillas

Deben de ser de preferencia movibles con rodos para lograr la máxima flexibilidad dentro del laboratorio.

Figura 50: Silla industrial

3.9 Especificaciones de Software.

3.9.1 Hammer (Test Client).

Es un cliente de prueba para probar IED con MMS (informes, registros, etc.), GOOSE y valores muestreados. Además, posee la capacidad de probar y optimizar rápidamente la calidad de aplicaciones de voz, aplicaciones móviles y sistemas de centros de contacto de una manera robusta y completa.
La plataforma mejora la experiencia del cliente al identificar y corregir los problemas relacionados con la experiencia antes y durante las operaciones de producción. Las organizaciones pueden aprovechar el sistema de prueba de martillo para detectar y medir los problemas de rendimiento en toda su red de comunicaciones.
El Hammer Test System emula todos los aspectos de un flujo de llamadas**,** incluyendo la entrada de información dinámica, utilizando tonos de tacto, y puede reproducir un número ilimitado de archivos de voz para probar sistemas basados en reconocimiento de voz. La capacidad patentada de reconocimiento de Hammer permite la comprobación de que se están reproduciendo las indicaciones correctas en la aplicación.

3.9.2 Anvil (Test Server).

Es una aplicación de Windows que crea un servidor IEC 61850 compatible con cualquier archivo SCL válido. Anvil es una herramienta altamente configurable que puede utilizarse para probar a los Clientes IEC 61850 con múltiples opciones de simulación para cambiar los valores del Modelo de Datos y generar tráfico de mensajes válido. Soporte para lectura, escritura, GOOSE, valores muestreados, informes, descubrimiento, registro, controles, conjuntos de datos dinámicos, seguimiento y servicios de archivos están incorporados en la herramienta

3.9.3 NPM Solar Winds.

SolarWinds NPM permite detectar, diagnosticar y resolver rápidamente problemas e interrupciones del rendimiento de red, antes de comenzar a recibir llamadas para preguntar si la red se cayó. Y SolarWinds NPM es fácil de implementar, usar y mantener de su tipo. Esto significa que puede utilizar el tiempo para realmente administrar su red y no para brindar soporte para su software de administración de red.

3.9.4 Wireshark.

Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.
Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.
Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android, y Mac OS X, así como en Microsoft Windows.

3.9.5 Simulador De Tiempo Real (Test Universe).

Es la herramienta de software más potente y conveniente para la prueba relacionada con parámetros básicos de dispositivos de protección y medición en sistemas de potencia. Ofrece una amplia gama de opciones de software que se tiene varios paquetes.
Permite una variedad de enfoques de prueba, desde pruebas manuales hasta pruebas totalmente automatizadas y estandarizadas, que se ejecutan en un PC o portátiles

3.9.6 Paquete de software para la generación y el mensaje GOOSE

- Módulo Goose Configuration: permite la realización de pruebas de dispositivos de protección con mensajes GOOSE IEC 61850. Se utiliza para configurar las

asignaciones y para configurar la unidad de prueba para la comunicación con la red de la subestación.

- Módulo Sampled Values Configuration: permite configurar la unidad de prueba CMC para la generación de Sampled Values IEC 61850. Dependiendo del modelo de unidad de prueba, pueden generarse simultáneamente hasta tres flujos de Sampled Values.
- IEDScout: es un cliente universal de servidores IEC 61850 (como los IED de subestación) y editor/suscriptor de mensajes GOOSE. Proporciona numerosas funciones útiles que son necesarias en la subestación o el laboratorio.

3.10 Tipos de pruebas.

Las pruebas que se pueden ejecutan en el laboratorio son:

- Pruebas de interoperabilidad
- Funcionalidad pruebas
- Evaluación de Rendimiento
- Estudios de Impacto
- Sitio Puesta en marcha
- Evaluación STP/RSTP en los Switch.
- Pruebas de estrés en la red LAN.
- Verificación de conversión IEC 61850 a IEC 60870-5-101.
- Pruebas GOOSE.
- Pruebas de fallos de red.

3.10.1 Pruebas Interoperabilidad.

Realizar las pruebas solo dispositivo, las pruebas de interoperabilidad de dispositivos múltiples y pruebas de integración del sistema:

- Solo dispositivo IEC 61850 pruebas que cubren tanto, estación de buses y bus de proceso
- IEC 61970 IEC 61968 pruebas / CIM
- Las pruebas de interoperabilidad
- La integración de sistemas y pruebas.

3.10.2 Pruebas de Funcionalidad.

Evaluar las funciones del DUT (Device Under Test) como se especifica y su respuesta en las siguientes condiciones:

- Ajuste de protección solo dispositivo, el tiempo, las pruebas de alcance de zona
- Múltiples dispositivos de pruebas esquema de protección que implica la comunicación
- Múltiples dispositivos individuales / esquema de control local / remoto, pruebas de enclavamiento

3.10.3 Evaluación de Rendimiento.

La coordinación con los servicios públicos para definir los criterios de evaluación de desempeño, y para llevar a cabo la evaluación del desempeño en términos de retardo de latencia, un tratamiento prioritario y caída sobre el manejo. Esto se aplica a los sistemas de comunicación, como la evaluación del desempeño bien en:

- arquitecturas de comunicación de la subestación
- Los sistemas de automatización de subestaciones
- Sistemas de gestión energética
- Sistemas de gestión de la distribución
- Los esquemas de protección y control

3.10.4 Estudios de Impacto.

Mediante el uso de modelos detallados de componentes del sistema de energía basado en transitorios en el RTDS para los estudios de impacto, las señales de corriente y tensión de la RTDS se amplifican y se inyectan en el DUT(Device Under Test), junto con las señales generadas digitalmente corriente / tensión / binarios.

Respuesta del DUT se alimenta de nuevo en el RTDS, donde continúa la simulación en tiempo real para evaluar el impacto del DUT) en todo el sistema de alimentación. El alcance de estos estudios de impacto incluye:

- Solo dispositivo y su impacto en el sistema de energía
- Coordinadas de múltiples dispositivos y su impacto en el sistema de energía
- Esquemas de interoperabilidad y su impacto en la parrilla

3.10.5 Sitio puesta en marcha.

El sitio de ventanilla única puesta en marcha que cubre todos los aspectos de:

- Prueba de integración para asegurar la totalidad de las funciones del sistema de automatización de subestaciones de forma interactiva
- Prueba de interoperabilidad para asegurar la inter-relé de esquemas de protección / de control funcionan como se ha diseñado
- Prueba de funcionalidad para asegurar las funciones del dispositivo / sistema con eficacia. Esto incluye la comprobación de todos los valores establecidos, verificando zona alcance y la confirmación de los retrasos de tiempo asociados con el esquema.

3.10.6 Evaluación STP/RSTP en los Switch.

Las arquitecturas de comunicaciones implementadas para la automatización de las subestaciones por lo general son arquitecturas con equipos de respaldo y rutas redundantes (ver figura 5). Dichas arquitecturas pueden conllevar a que los paquetes de información se queden en la red de Switches sin llegar a su destino.

Por los motivos expuestos anteriormente, es necesario realizar pruebas STP/RSTP para evitar bucles de capa 2 en la red de la subestación.
En las pruebas STP/RSTP del Laboratorio se aplican métodos determinísticos para:

- Medir tiempos de conexión.
- Medir tiempos de cálculo del protocolo STP/RSTP.
- Medir tiempos de restablecimiento.

3.10.7 Pruebas De Estrés En La Red LAN.

En las subestaciones se genera gran cantidad de información que debe ser transmitida al centro de control, por lo cual se hace necesario verificar que la arquitectura de comunicaciones implementada soporte la cantidad de datos generados por los equipos de bahía.
Las pruebas de estrés realizadas en el laboratorio generan sobrecarga de datos en una arquitectura de comunicación simulada con dispositivos físicos y se evalúan:

- Consumo de recursos de los equipos.
- Ocupación de los canales.
- Pérdida do paquetes.

3.10.8 Verificación De Conversión IEC 61850 a IEC 60870-5-101.

Actualmente el protocolo de comunicaciones en subestación es diferente al protocolo de comunicación del centro de control, por lo cual a la salida de la red de la subestación se instalan Gateways con el fin de realizar la conversión de los protocolos.
Debido a que estos equipos cumplen una función muy importante en el proceso de automatización de las subestaciones. Surge la necesidad de verificar su configuración y los tiempos de conversión de datos.
En el proceso de verificación de conversión de protocolos se realizan las siguientes actividades:

- Evaluar la coherencia de los datos a la entrada y a la salida del Gateway.
- Medir tiempos de conversión de datos.
- Verificar que las estampas de tiempo de un evento coincidan en ambos canales.

3.10.9 Pruebas GOOSE.

La principal característica del protocolo IEC 61850 es permitir la interoperabilidad entre los equipos instalados en la subestación, la cual se puede realizar a través de mensajes tipo GOOSE. Adicionalmente los mensajes GOOSE son también llamados mensajes rápidos de subestación, por lo cual son usados para transmitir información de eventos de alta prioridad.
Actualmente los mensajes GOOSE son subutilizados, pero a futuro dichos mensajes serán aplicados para explotar las características de interoperabilidad y para mejorar los tiempos de respuesta en las subestaciones. La prueba GOOSE se realiza actualmente en el labora-

torio para verificar que las arquitecturas de comunicaciones que se están implementando hoy en día puedan soportar el paso de mensajes GOOSE.
Esta prueba consiste en:

- Configurar un IED para que publique un mensaje GOOSE.
- Excitar el equipo para que publique el mensaje GOOSE.
- Medir el tiempo de recepción.

3.10.10 Pruebas De Fallos De Red

Las pruebas de fallos de red consisten en replicar las fallas que se están presentando actualmente en una subestación, para identificar su causa raíz.
Algunas pruebas de fallos de red aplicadas en el Laboratorio son:

- Apagar el Gateway que se encuentra con el rol de hot y evaluar el tiempo de respuesta del Gateway que se encuentra en Stand-by, para tomar el rol de hot.
- Apagar el switch correspondiente al Gateway que tenga el rol de hot y evaluar el comportamiento del sistema (con IED conectados).
- Desconexión de conector Ethernet correspondientes a un IED (error de conmutación modo y Switch) que se encuentra en el bus de estación, conectado al Switch que esta con el Gateway en rol de hot.
- Apagar el switch del Bus de estación del anillo activo y verificar el comportamiento de los IED que se encuentran conectados en el Proceso bus, teniendo a los IED en Failover o Switch en su tarjeta de red.

3.11 Implementación de una prueba a protección basada en la norma IEC – 61850.

3.11.1 Prueba de bajo Voltaje (27)

Paso 1. Se abre el software Test Universe y se da clic en Abrir un documento de prueba existente y se selecciona.

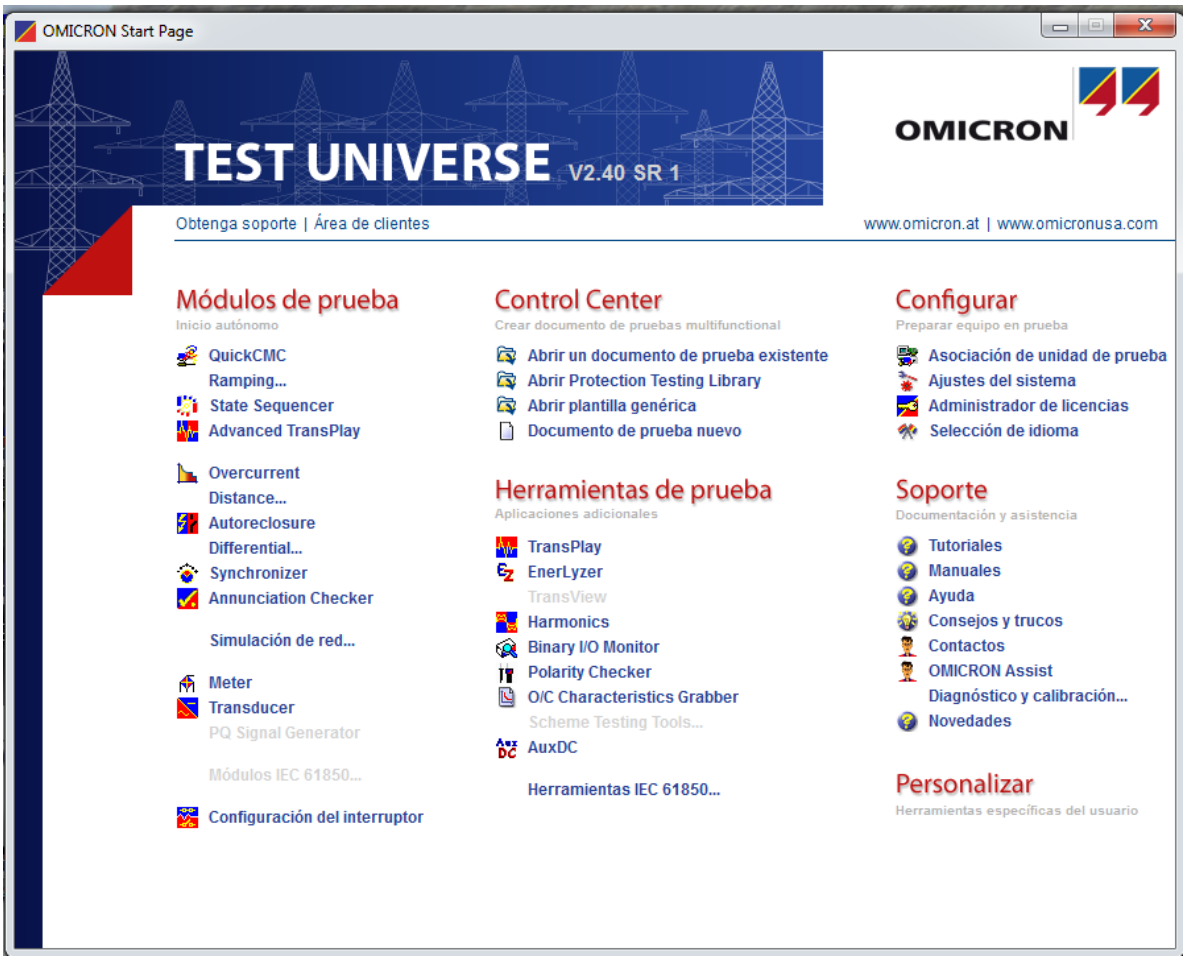


Figura 51: Ventana de inicio de test universo.

Paso 2. Se da clic en la opción de "Prueba de Operación de Pickup 27 Fase AB" que es un nombre ya dado a esta prueba por el usuario.
Paso 3. Después se define el estado de la rampa para este caso la rampa debe ser una rampa decreciente para simular una caída de voltaje.

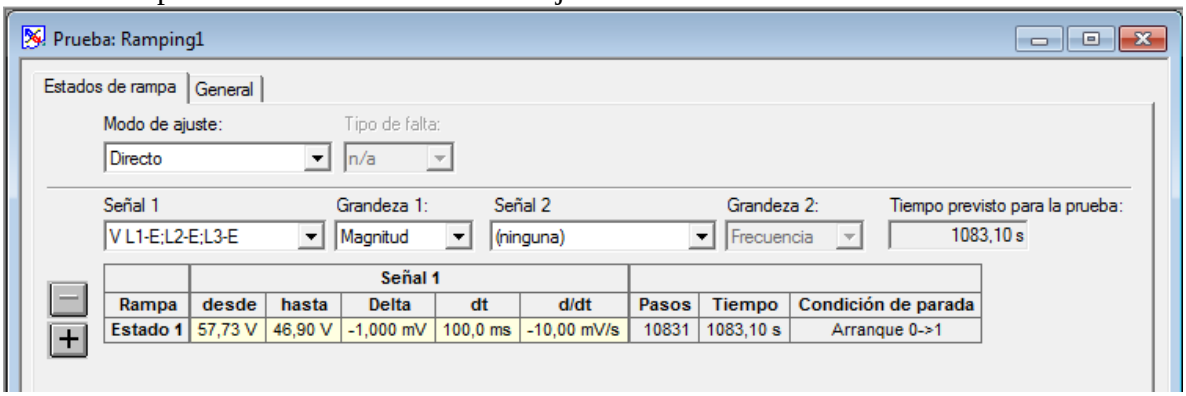


Figura 52: Definiendo el estado de la rampa

Paso 4. Los estados de rampa definidos se representan automáticamente en la Oscilógrafo

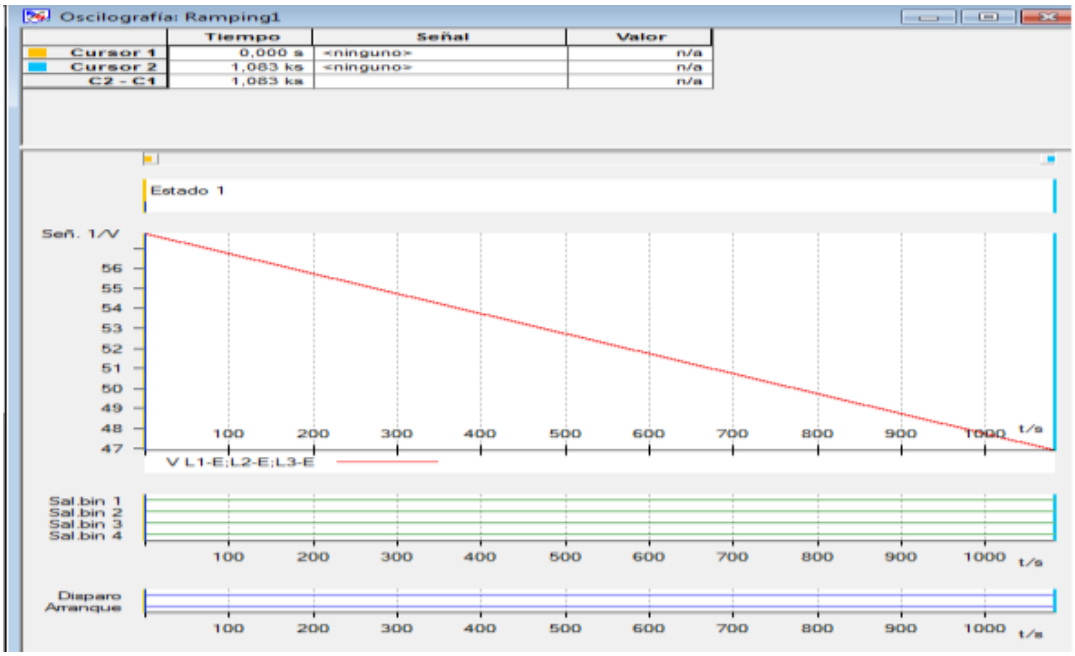


Figura 53: Estado de la rampa

Todos los valores que son estáticos, durante la emisión del estado de rampa, se definen en la ficha Salidas analógicas en la vista Detalle del módulo de prueba Ramping.

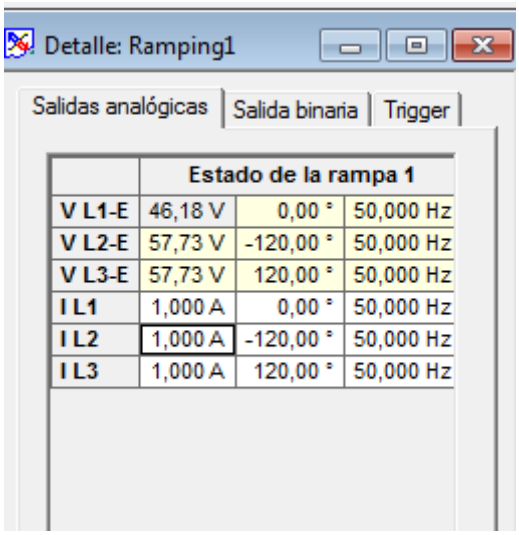


Figura 54: Detalles de la rampa

Paso 5. Para iniciar la prueba, haga clic en el icono COMENZAR de la barra de herramientas del módulo de prueba Ramping.

3.11.2 Pruebas de Sobre corriente

Paso 1. Se conecta la maleta omicrom CMC 356 para dichas pruebas.

- Se conecta en las salidas de voltaje del CMC 356 a las entradas de voltaje de la protección y las salidas de corriente a las entradas de corriente de dicha protección.

Figura 55: Unidad de pruebas de reles universal CMC 356

Paso 2. La señal de disparo de la protección se conecta a la entrada la entrada binaria 1.

Paso 3. Definir los ajustes del relé sometido a prueba. Para hacerlo, se tiene que abrir los parámetros del Equipo en prueba que están ubicados en la barra de ayuda del programa.

Paso 4. Luego le damos doble clic sobre el módulo sobre corriente que está en la sub-carpeta RIO.

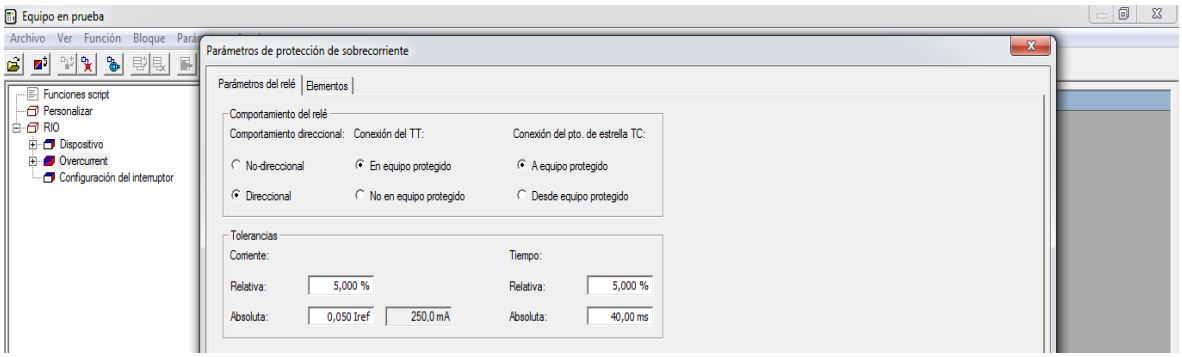


Figura 56: Ventana de parámetros de la prueba de protección de sobrecorriente.

Paso 5. Dar clic en la pestaña elementos.

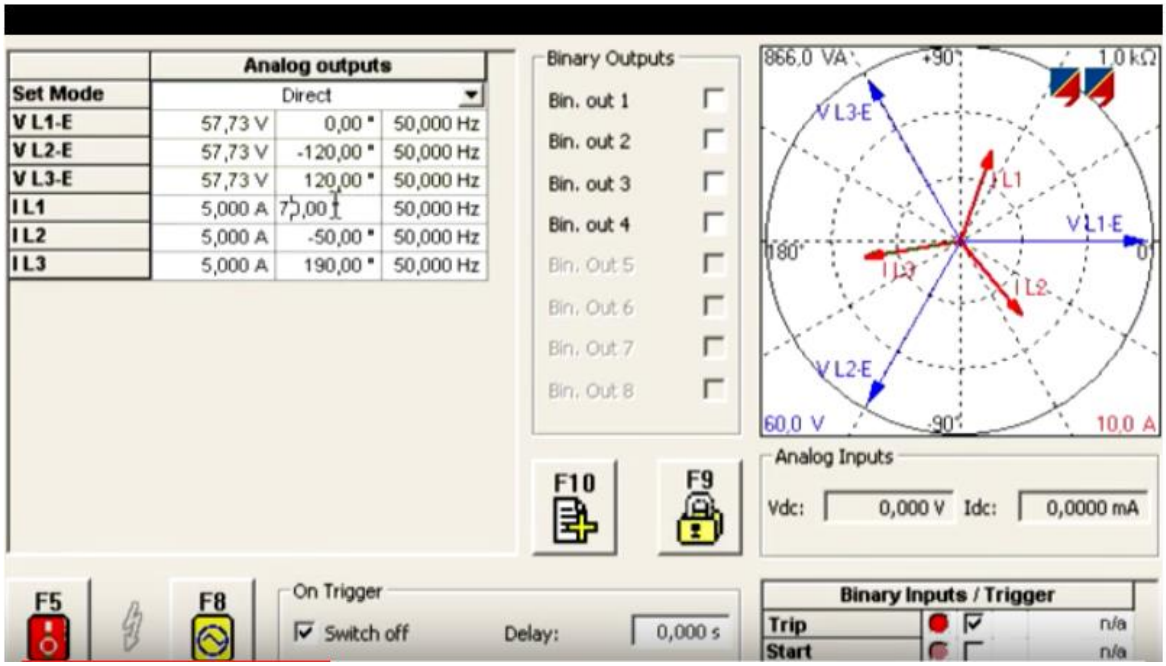


Figura 57: Descripción de los elementos de protección

En esta tabla se indican los elementos que definen la característica de disparo del tipo de elemento seleccionado. También hay que ajustar I arranque y el Tiempo de disparo.

Paso 6. El tipo de característica del primer elemento se tiene que cambiar a inversa, después hay que ajustar I arranque y el Índice de tiempo.

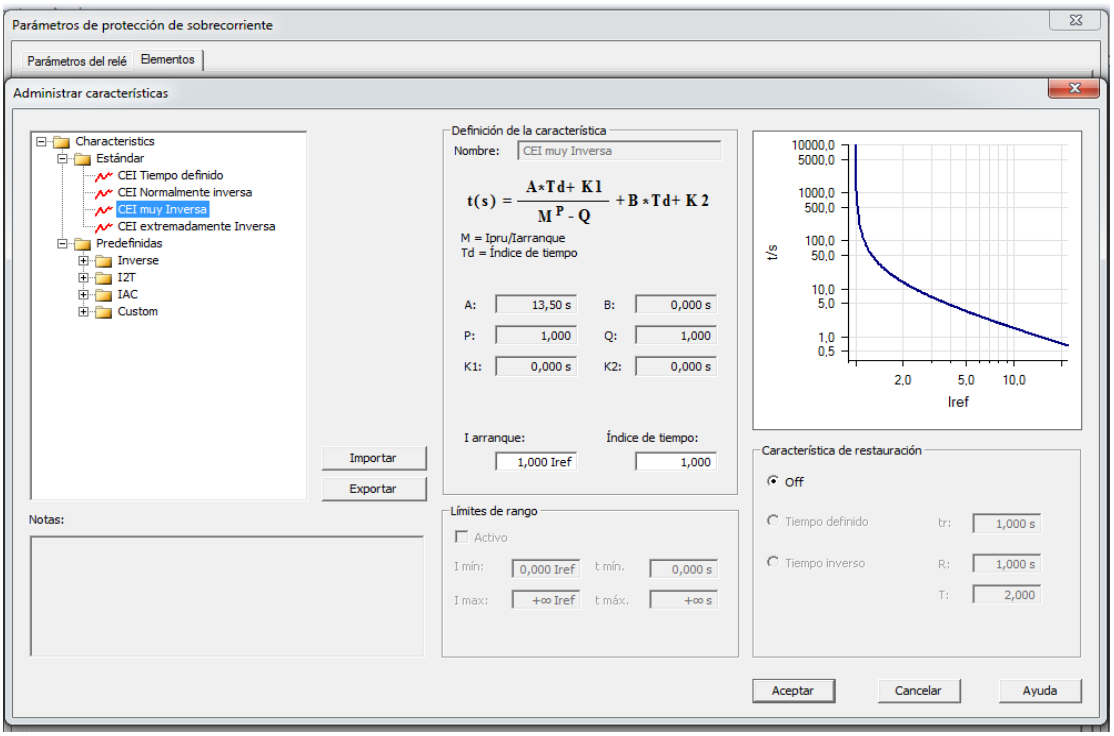


Figura 58: Cambio de características de protección a muy inversa.

Paso 7. Ahora para realizar la prueba de disparo se ingresan varios puntos comprobando la curva de la protección.

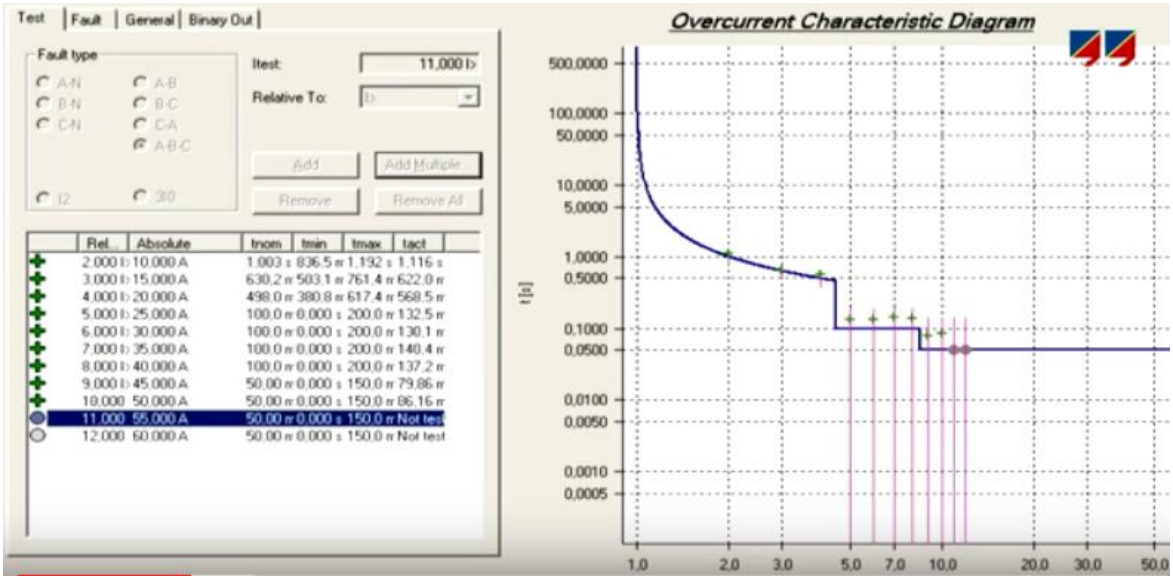


Figura 59: Modificando los diferentes putos de disparo de la curva.

CAPÍTULO IV

Estimación del costo de la Implementación del Laboratorio IEC – 61850.

4.1 Mediciones

En este capítulo se recogen los costes de las diferentes partes necesarias para el desarrollo del proyecto, agrupados en distintas partidas, definiendo tanto los presupuestos de cada una de ellas como el presupuesto total.

A la hora de detallar los conceptos que serán incluidos en el presupuesto final correspondiente al presente proyecto, se han seguido las premisas que se exponen a continuación:

- Los precios de los componentes detallados corresponden al importe pagado en su fecha de compra, y pueden no coincidir con el importe de compra en caso de requerirse una reproducción del proyecto, en cuyo caso el presente presupuesto podrá ser revisado y actualizado.
- Se incluyen los costes correspondientes al equipo informático y al software utilizado en el desarrollo del proyecto.
- El presupuesto final incluye la totalidad de los componentes empleados en el proyecto que constituye el concepto global desarrollado, pero la mano de obra incluida se corresponde únicamente con la empleada por el proyectista encargado de la parte del concepto global desarrollada en el presente proyecto. El primer paso para realizar el presupuesto del proyecto es detallar las cantidades empleadas de los diferentes medios necesarios.

Las partidas correspondientes a Recursos Humanos se recogen a continuación, en la Tabla 17.

CONCEPTOS	NÚMEROS DE HORAS
Estudio y auditoría	40
Ingeniería	100
Elaboración de documentación	20

Tabla 17: Mediciones de los Recursos Humanos.

En la Tabla 18 se hace referencia a los elementos y materiales empleados en la composición del proyecto, indicando las unidades necesarias de cada uno de ellos.

CONCEPTOS	CANTIDAD
2 LAPTOP HP 2,3 GHz/ RAM 12GB	2 unidades
Anvil	1 licencia
Hammer	11 licencia
Wireshark	1 licencia
NPM Solar Winds	1 licencia

Módulo Goose Configuration	1 licencia
Unidad de prueba universal de relés	1 unidad
CPC 1000 +Test Universe	1 licencia
IEDScout	1 licencia
Gateway	4 unidades
Automation controller RTAC	1 unidad
Switch	4 unidades
Cable Ethernet cruzado	1 unidad
IEDs	4 unidades
Mesas	2 unidades
Sillas	4 unidades

Tabla 18: Mediciones de los medios materiales.

4.2 Precios unitarios

Una vez conocidos cuáles son los recursos que se han empleado en el desarrollo del proyecto, es necesario determinar qué coste económico supone cada uno de ellos de manera unitaria. La información se presenta en forma de tablas siguiendo la estructura anterior.

En primer lugar, se detallarán los precios unitarios de las partidas correspondientes a los Recursos Humanos. La Tabla 19 muestra dichos valores.

Conceptos	**Precios en $/hora**
Estudio y auditoría	45
Ingeniería	30
Elaboración de documentación	20

Tabla 19: Precio unitario de los Recursos Humanos.

Respecto a los Recursos Materiales empleados, los costes unitarios de cada elemento se recogen en la siguiente Tabla:

Conceptos	Precios/unidad
LAPTOP HP 2,3 GHz/ RAM 12GB (El Salvador)	1,200
Anvil (Norte América)	5,000
Hammer (Norte América)	2,500
Wireshark (Norte América)	0
NPM Solar Winds (Norte América)	2,895
Módulo Goose Configuration (Norte América)	2,500
Unidad de prueba universal de relés (México)	7,500
CPC 100 +Test Universe (OMICRON, México)	17,710
IEDScout	0
Gateway (Norte América)	1,100
Controlador Automático RTAC (SEL, Norte América)	8,945
Switch (CISCO)	300
Cable Ethernet Trenzado (El Salvador)	185
IED ABB REF615	950
IED ABB REM620	2,500
IED SEL	1,540
IED SIEMENS	6,930
Mesas	75
Sillas	80

Tabla 20: Precio unitario de los Recursos Materiales.

4.3 Sumas parciales

Una vez conocidas las cantidades de cada recurso, y sus precios unitarios, quedan por establecer los costes correspondientes a cada una de las partidas.

Las sumas parciales de los Recursos Humanos empleados se muestran en la Tabla 21.

Conceptos	Número de horas	Precios en $/hora	Precios en $/hora Total
Estudio y auditoría	40	45	1,800
Ingeniería	250	35	8,750
Elaboración de documentación	25	25	625
		Total en RH	**11,175**

Tabla 21: Sumas parciales de los Recursos Humanos.

La partida de los Recursos Materiales presenta los siguientes valores:

Conceptos	Cantidad	Precios/unidad	Total ($)
LAPTOP HP 2,3 GHz/ RAM 12GB	2	1,200	2,400
Anvil	1	5,000	5,000
Hammer	1	2,500	2,500
Wireshark	1	0	0
NPM Solar Winds	1	2,895	2,895
Módulo Configuración GOOSE	1	2,500	2,500
Unidad de prueba universal de relés	1	7,500	7,500
CPC 100 + Test Universe	1	17,710	17,710
IEDScout	1	0	0
Gateway	4	1,100	4,400
Automation controller RTAC	1	8,945	8,945
Switch	4	300	1,200
Cable Ethernet Trenzado	1	185	185
IED ABB REF615	1	950	950
IED ABB REM620	1	2,500	2,500
IED SEL	1	1,540	1,540
IED SIEMENS	1	6,930	6,930
Mesas	2	75	150
Sillas	4	80	320
		Total de M&E	**67,625**

Tabla 22: Sumas parciales de los Recursos Materiales.

Una última partida no indicada anteriormente, pero necesaria para el desarrollo del proyecto es la que refleja los gastos indirectos ocasionados. La Tabla 23 muestra el coste correspondiente.

Conceptos	Total ($)
Modificaciones del edificio	1500
Conexiones telefónicas (El Salvador)	54
Línea ADSL (El Salvador)	50
Papelería	20
Certificación de la norma IEC 61850 (KEMA Europa)	60,640
Estimación de Gastos Indirectos ($)	**62,264**

Tabla 23: Estimación de los Gastos Indirectos.

4.4 Estimación general.

El último paso para completar el presupuesto del proyecto es realizar el monto de todas las partidas descritas en los Capítulos anteriores de este documento.

En la Tabla 24 se recogen los valores totales de cada tipo de recurso y el Presupuesto General resultado de la suma de todos ellos.

PARTIDA	IMPORTE ($)
Recursos Humanos	11,175
Materiales	67,625
Gastos Indirectos	62,264
Subtotal	141,064
I.V.A (13%)	18,338.32
PRESUPUESTO GENERAL	**159,402.32**

Tabla 24: Importe total del presupuesto

CONCLUSIONES

De acuerdo con la investigación realizada se puede concluir lo siguiente.

- El fundamento principal de la norma IEC61850 es establecer la interoperabilidad dentro de la subestación existiendo equipo de diferentes fabricantes, y ser aplicado en los 3 niveles en la que divide una subestación como lo es nivel de proceso, nivel de bahía, nivel de estación.

- El uso de equipos de diferentes fabricantes no estandarizado pueden conducir a errores de comunicación o incompatibilidad al momento de implementar un sistema SAS.

- La información dentro del entorno de la subestación se intercambia entre los equipos que forman el sistema SAS, donde los datos fluyen entre funciones y sub funciones de los equipos para ello el estándar IEC – 61850 propone representar todas las funciones y equipos utilizado en el sistema por medio de nodos lógicos. De esta forma toda la información de la subestación se estructura en forma atómica, permitiendo la posibilidad de poder incorporar nuevos nodos lógicos, siempre y cuando se sigan las reglas definidas en dicho estándar.

- La Sincronización independiente de una subestación por medio de un servidor GPS reduce la cantidad de fallas en la sincronización de los dispositivos de protección, proporciona independencia de niveles de jerarquía en la subestación, comunicación por medio de varias interfaces y no depende de otras subestaciones.

- La norma IEC 61850 se refiere a lo correspondiente a modelos abstractos de datos de la subestación y de los servicios de comunicación, aun así no define el diseño de una red para su puesta en servicio por tal motivo para una implementación adecuada de la norma en una red se hace necesario el poder configurar correctamente la red según los requerimientos de mensajes publicados por las IEDs y que tenga una buena operación esperada para el sistema.

RECOMENDACIONES

Se recomienda:

- Iniciar un plan de concientización de parte de la planta docente de la EIE-UES para su alumnado en la que se exponga que en los sistemas de potencia no solo son importantes los transformadores o generadores sino también el monitoreo y protección.

- Capacitarse en temas sobre la norma IEC61850 para la implementación de nuevas prácticas en los laboratorios, y no quedarse con los estándares antiguos ya que estos en cualquier momento deberán ser sustituidos por otros más recientes.

- Investigar con la intención de comprender el concepto de las nuevas redes de energía, las Redes Inteligentes, y el estado actual en el que se encuentra su implantación e investigación, describiendo qué es una Red Inteligente, detallando sus características, componentes, ventajas e inconvenientes.

- Realizar una investigación sobre las ITIL (Information Technology Infrastructure Library), tomando en cuenta el modelo para la administración de servicios de tecnología de información (TI) e incluyendo información sobre las metas, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar en el área TI.

- Capacitar al personal del área de potencia en la aplicación de la norma IEC – 61850 dentro de la subestación, acerca de los aspectos importantes para las evaluaciones del sistema, en el contexto tecnológico y que conozcan su importancia en la implementación.

- Diseñar e implementar un sistema de comunicación para la mejora de los procesos de servicio, sustentado y validado por algún modelo de trabajo basado en algún estándar de calidad como el ISO/IEC 2000.

- Implementar subestaciones inteligentes en la UES, es decir, que consten con dispositivos IEDs, dispositivos de comunicación certificados bajo la norma IEC61850, para ser monitoreados desde un centro de control ya sea vía redes inalámbricas o enlace microondas, esto permitiría a los docentes realizar actividades de campo (mantenimientos, pruebas de conformidad, etc..) en conjunto con los alumnos, permitiendo un primer contacto con las subestaciones inteligentes.

- Proponer una nueva asignatura para que el alumnado estudie la implementación de la norman IEC61850, ya que ese es el futuro en el que se enmarcan las subestaciones de nuestro país de migrar a esta norma para un mejor rendimiento y eficiencia en respuesta a protección y medición de los equipos de potencia.

REFERENCIAS

1. Belden.com. (2016). *Belden - Sending All the Right Signals*. [online] Available at: http://www.belden.com [Accessed 2 Sep. 2016].

2. Cisco. (2017). *Cisco - Global Home Page*. [online] Available at: http://www.cisco.com [Accessed 5 Nov. 2016].

3. Energy.siemens.com. (2017). *Energy Products & Services*. [online] Available at: http://www.energy.siemens.com [Accessed 13 Sep. 2017].

4. Furukawa.co.jp. (2017). [online] Available at: http://www.furukawa.co.jp [Accessed 15 Jun. 2017].

5. Ghosh, K. (1997). Distribution automation: SCADA integration is key. *IEEE Computer Applications in Power*, [Accessed 24 Sep. 2016].

6. Haffar, M., Thiriet, J. and Savary, E. (2007). Modeling of substation architecture implementing IEC 61850 protocols and solving interlocking problems. *IFAC Proceedings Volumes*, [Accessed 29 Sep. 2017].

7. IEC 61850- 7 Configuration description language for communication in electrical substations related to IEDs. (2002), (CDV2R8DRAFT).

8. IEC 61850 Communication Networks and Systems in Substations. (2002). 1st ed. IEC, INTERNATIONAL STANDARD.

9. IEC 61850-10 Conformance testing. (2004). 2nd ed. INTERNATIONAL STANDARD: CDV R07.

10. IEC 61850-5 Communication requirements for functions and device models. (2004). 1st ed. INTERNATIONAL STANDARD.

11. IEC 61850-6 Configuration description language for communication in electrical substations related to IEDs. (2002). 1st ed. IEC.

12. IEC 61850-7-1 Basic communication structure for substation and feeder equipment – Principles and models. (2003). 1st ed. INTERNATIONAL STANDARD.

13. IEC 61850-7-2 Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI). (2017). 1st ed. INTERNATIONAL STANDARD.

14. IEC 61850-7-3 Basic comunication structure for substation and feeder equipment common data classes. (2017). 1st ed. INTERNATIONAL STANDARD.

15. IEC 61850-7-4 Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes. (2003). 1st ed. INTERNATIONAL STANDARD.

16. IEC 61850-8-1 Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. (2003). 1st ed. INTERNATIONAL STANDARD.

17. IEC 61850-9-2 Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3. (2004). 1st ed. INTERNATIONAL STANDARD.

18. IEEE 1316 Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations. (2002). 1st ed. IEEE.

19. Ieeexplore.ieee.org. (2017). *IEEE Xplore Digital Library*. [online] Available at: http://ieeexplore.ieee.org [Accessed 8 Ene. 2017].

20. Infoplc.net. (2017). *Automatización Industrial - Robotica - Industria 4.0 - infoPLC*. [online] Available at: http://www.infoplc.net [Accessed 1 Feb. 2017].

21. Infostore.saiglobal.com. (2017). *SAI Global*. [online] Available at: http://infostore.saiglobal.com [Accessed 1 Mar. 2017].

22. Innovave.com. (2017). *Low Voltage Systems Design and Consulting – Innovate | A/V- IT-SECURITY CONSULTING AND DESIGN*. [online] Available at: http://innovave.com [Accessed 15 May. 2017].

23. ISO 9001:2015. (2017). *ISO 9001:2015*. [libro] Available at: http://www.nueva-iso-9001-2015.com [Accessed 21 May. 2017].

24. Keat Khoo, T. (2007). IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799 3rd ed.20071Alan Calder and Steve Watkins. IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799 3rd Ed. London and Sterling, VA: Kogan Page 2005. , ISBN: 0-7494-4394-4 (pbk). *Corporate Governance: The international journal of business in society*, 7(1), pp.79-104.

25. Kinectrics.com. (2017). *Case Studies for Testing, Inspection & Certification | Life Cycle Management | Electricity Industry*. [online] Available at: http://www.kinectrics.com/Pages/Case-Studies.aspx [Accessed 14 Aug. 2016].

26. Kumpulainen, L., Jäntti, A., Rintala, J. and Kauhaniemi, K. (2017). Benefits and performance of IEC 61850 Generic Object Oriented Substation Event-based communication in arc protection. *IET Generation, Transmission & Distribution*, 11(2), pp.456-463.

27. Lee, N. and Jang, B. (2010). Development of IEC 61850 Client Testing System for Verifying the Communication Conformance of Substation Automation. *Journal of the Korean Institute of Illuminating and Electrical Installation Engineers*, 24(6), pp.169-176.

28. Nema.org. (2017). *NEMA - The Association of Electrical Equipment and Medical Imaging Manufacturers*. [online] Available at: http://www.nema.org [Accessed 23 May. 2017].

29. Nerc.com. (2017). *NERC*. [online] Available at: http://www.nerc.com [Accessed 20 Feb. 2017].

30. New.abb.com. (2017). *ABB Group - Leading digital technologies for industry*. [online] Available at: http://new.abb.com [Accessed 20 Feb. 2017].

31. Ozansoy, C. (2010). *Modelling and object oriented implementation of IEC 61850*. Saarbrücken: LAP Lambert Academic Pub.

32. Perlesystems.es. (2017). *Perle | Serial a Ethernet, Fibra a Ethernet y Dispositivos de Red*. [online] Available at: http://www.perlesystems.es [Accessed 15 Jun. 2017].

33. Perlesystems.es. (2017). *Perle | Serial a Ethernet, Fibra a Ethernet y Dispositivos de Red*. [online] Available at: http://www.perlesystems.es [Accessed 5 Jul. 2017].

34. Raj. T, S. (2017). Substation Automation System for Energy Monitoring and Control using SCADA. *International Journal for Research in Applied Science and Engineering Technology*, V (III), pp.1232-1257.

35. Redeweb.com. (2017). *Revista Española de electrónica*. [online] Available at: http://www.redeweb.com [Accessed 15 Abr. 2017].

36. S.L.U., U. (2017). *Entel | Cableado Estructurado, CPD y Soluciones Informáticas*. [online] Unitel - Soluciones e infraestructuras Tecnológicas. Available at: https://unitel-tc.com [Accessed 10 May. 2017].

37. Schwarz, K. (2017). *How to Model Thousands of Measurement Signals?* [online] Blog.iec61850.com. Available at: http://blog.iec61850.com/2017/06/how-to-model-thousands-of-measurement.html [Accessed 6 May. 2017].

38. Techstreet.com. (2017). *Techstreet -Technical Information Superstore*. [online] Available at: http://www.techstreet.com [Accessed 14 Abril. 2017].

39. Thefoa.org. (2017). *The Fiber Optic Association*. [online] Available at: http://www.thefoa.org [Accessed 1 Abr. 2017].

40. Trianglemicroworks.com. (2017). *IEC 61850 Test Suite*. [online] Available at: http://www.trianglemicroworks.com/products/testing-and-configuration-tools/61850-test-suite-pages/test-suite [Accessed 3 mar. 2017].

41. Trianglemicroworks.com. (2017). *Triangle Micro Works Home*. [online] Available at: http://www.trianglemicroworks.com/ [Accessed 26 May. 2017].

42. Trilliant Inc. (2017). *Trilliant | Energy Industry Communications Platform: Complete Smart Grid Solutions and Services*. [online] Available at: http://trilliantinc.com [Accessed 8 Feb. 2017].

43. User, S. (2017). *Universidad Nacional de Colombia: Infraestructura*. [online] Grupotyt.medellin.unal.edu.coma: http://grupotyt.medellin.unal.edu.co/laboratorio-iec61850/infraestructura [Accessed 5 mar. 2017].

44. vistos, L.,!!!, M., Troncal., T. and IPv4, C. (2017). *Sea CCNA - Informaciones indispensables para quien conoce o está estudiando redes de computadoras*. [online] Sea CCNA. Available at: http://www.seaccna.com [Accessed 27 Abr. 2017].

45. Workshop, D. (2017). *World Leader in Innovative Power System Testing Solutions - OMICRON*. [online] Omicronenergy.com. Available at: http://www.omicronenergy.com [Accessed 4 Mar Jul. 2017].

46. www.gesio.com, D. (2017). *Presentación - RTDS - INDIELEC - Software CAD y CAE para ingeniería*. [online] Indielec.com. Available at: http://www.indielec.com/presentacion-cms-4-50-73/ [Accessed 12 Feb. 2016