

UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**IMPLEMENTACIÓN DE SISTEMAS DE COMUNICACIONES PARA
LA AUTOMATIZACIÓN DE SUBESTACIONES ELÉCTRICAS**

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

CARLOS ALBERTO CONGA CARRASCO

**PROMOCIÓN
1999 - II**

**LIMA – PERÚ
2009**

**IMPLEMENTACIÓN DE SISTEMAS DE COMUNICACIONES PARA LA
AUTOMATIZACIÓN DE SUBESTACIONES ELÉCTRICAS**

A mis padres por todo el apoyo que me
brindaron.

SUMARIO

La necesidad de intercambiar datos en tiempo real en las subestaciones eléctricas a velocidades muy altas, se ha incrementado en los últimos tiempos. El presente informe revisa los requerimientos de infraestructura de comunicaciones en las subestaciones eléctricas y analiza las opciones actuales y futuras de implementación. Revisa las tecnologías que se pueden utilizar para satisfacer estos requerimientos y la modernización que la subestación eléctrica requiere desde el punto de vista de las comunicaciones. Adicionalmente se analiza las tendencias industriales para el intercambio de datos en tiempo real.

ÍNDICE

PRÓLOGO	1
CAPÍTULO I	
MARCO TEÓRICO	3
1.1 Definiciones y Terminología	3
1.2 Transferencia de Información de la Subestación a la Empresa Eléctrica	5
1.3 Arquitectura del Sistema de Automatización de Subestaciones	6
1.4 Estándares y Protocolos de Comunicaciones	8
1.4.1 Normas de Hardware Orientadas al Entorno de Subestaciones	9
1.4.2 Protocolos de Comunicaciones	11
1.4.3 Tendencias de la Industria	21
1.5 Sincronización de Tiempo en Subestaciones	25
CAPÍTULO II	
CRITERIOS DE DISEÑO	27
2.1 Diseño de una red de comunicaciones para automatización	27
2.2 Requerimientos Funcionales	27
2.2.1 Características de los Sistemas de Comunicaciones en Subestaciones	28
2.2.2 Seguridad Informática	32
2.3 Evaluación de Infraestructuras de Comunicación Existentes	35
2.3.1 Redes Privadas y Redes Arrendadas	36
2.3.2 Comunicaciones Telefónicas	38
2.3.3 Comunicaciones de Red IP	38
2.4 Comunicaciones dentro de la Subestación	45
2.4.1 Requerimientos Ambientales de los Equipos del Sistema	45
2.4.2 Cableado de Campo	46
2.4.3 Topologías de Comunicaciones	47
2.4.4 Protocolos de Comunicaciones Soportados por los IEDs	53
2.5 Comunicaciones con la Empresa Eléctrica	54
2.5.1 Acceso de la Subestación a la Red de Transporte	56
2.5.2 Red de Transporte	62
2.6 Consideraciones de Implementación	64

2.6.1	Coexistencia de Redes Nuevas y Existentes	64
2.6.2	Períodos de Tiempo	65
2.6.3	Requerimientos Organizacionales	65
2.6.4	Alternativas de Implementación	65
2.6.5	Plan de Proyecto	67

CAPÍTULO III

APLICACIÓN DE LA IMPLEMENTACIÓN DE SISTEMA DE COMUNICACIONES PARA LA AUTOMATIZACIÓN DE SUBESTACIONES ELÉCTRICAS

3.1	Introducción	68
3.2	Niveles de Automatización	71
3.3	Centro de Control de Antamina	72
3.4	Comunicaciones en Subestación Antamina	73
3.4.1	Entre Niveles IEDs - Subestación	73
3.4.2	Entre Niveles Subestación - Centro de Control	74
3.4.3	Comunicaciones entre Centros de Control	75
3.4.4	Configuración de IEDs	75
3.4.5	Acceso Remoto	75
3.5	Comunicaciones en Subestación Vizcarra	75
3.5.1	Entre Niveles IEDs - Subestación	75
3.5.2	Entre Niveles Subestación - Centro de Control	76
3.6	Hardware del Sistema	77
3.6.1	Subestación Antamina	77
3.6.2	Subestación Vizcarra	78
3.7	Presupuesto y Tiempo de Ejecución	78

CONCLUSIONES Y RECOMENDACIONES

ANEXO A

COMPARACIÓN ENTRE ESTÁNDARES DNP3 E IEC 61850

ANEXO B

DIAGRAMAS UNIFILARES DE SUBESTACIONES DE ANTAMINA

ANEXO C

DISTRIBUCIÓN DE HARDWARE Y SISTEMA DE COMUNICACIONES

BIBLIOGRAFÍA

PRÓLOGO

Los sistemas de comunicaciones en las empresas eléctricas surgieron hace más de 40 años, en respuesta a los cortes de energía que dejaban a las poblaciones sin suministro eléctrico.

Desde entonces, las capacidades de recolección de datos de los dispositivos de subestaciones, tales como los IEDs (dispositivos electrónicos inteligentes) y la capacidad de cómputo de programas como los Sistemas SCADA y Sistemas de Gestión de Energía (EMS) en los centros de control, han crecido enormemente. Sin embargo, los enlaces de comunicaciones conservan gran parte de las características impuestas por la tecnología de esa época: son de baja velocidad y no proporcionan la flexibilidad para adaptarse a las necesidades de cambio. Como resultado de esto es poco el uso operativo que se puede hacer de la gran cantidad de datos disponibles existentes en las subestaciones. Por otra parte, algunas empresas eléctricas implementan tecnologías de redes de mayor velocidad, pero que no ofrecen la flexibilidad y robustez que se requiere.

Estas capacidades limitadas de los sistemas de comunicaciones en las empresas eléctricas, a su vez limitan la implementación y el funcionamiento de los sistemas de automatización de subestaciones.

Este informe trata de los requerimientos de diseño e implementación de una mejor infraestructura de comunicaciones para la automatización de las subestaciones eléctricas, utilizando diferentes tecnologías de redes de computadoras de gran flexibilidad y portabilidad, tales como IP, SCADA, SONET, y otras, con la premisa de conservar un elevado índice en la continuidad del servicio, incrementar la confiabilidad del sistema y mejorar el tiempo de respuesta ante la presencia de situaciones anormales en la operación de subestaciones, que son críticos dentro de los sistemas eléctricos de potencia.

El capítulo I cita el marco teórico referido a los sistemas de comunicaciones para la automatización de subestaciones, su necesidad, sus definiciones, las normas y protocolos normalmente utilizados y las tendencias de la industria.

Los criterios de diseño para la implementación del sistema de comunicaciones para la automatización de subestaciones se describen en el capítulo II. Se determinan los pasos a seguir y requerimientos funcionales para la implementación del sistema en cualquier

subestación en general; se describen las características de los sistemas de comunicaciones a tomar en cuenta, incluyendo la evaluación de infraestructuras existentes, las redes de comunicaciones dentro y fuera de las subestaciones, así como las consideraciones de implementación.

El capítulo III describe una aplicación práctica del proceso de implementación del sistema de comunicaciones para la automatización de dos subestaciones de la Compañía Minera Antamina S.A. Se describen los principios de diseño, las funcionalidades a utilizar, la arquitectura y equipos tomando en cuenta criterios y parámetros, específicos y aplicables a las necesidades de dicha compañía, así como el presupuesto para el proyecto y el tiempo de ejecución.

CAPÍTULO I

MARCO TEÓRICO

1.1 Definiciones y Terminología

Una Subestación Eléctrica es una parte de la red eléctrica, concentrada en un lugar dado, que incluye principalmente los terminales de los dispositivos de control y maniobra y las celdas de las líneas de transmisión o distribución y que también podría incluir transformadores. Generalmente incluye las instalaciones necesarias para los sistemas de seguridad y control (por ejemplo, dispositivos de protección). [1]

La figura 1.1 muestra el diagrama de bloques de la red eléctrica y diferentes tipos de subestaciones, según su aplicación (generación, transmisión y distribución).

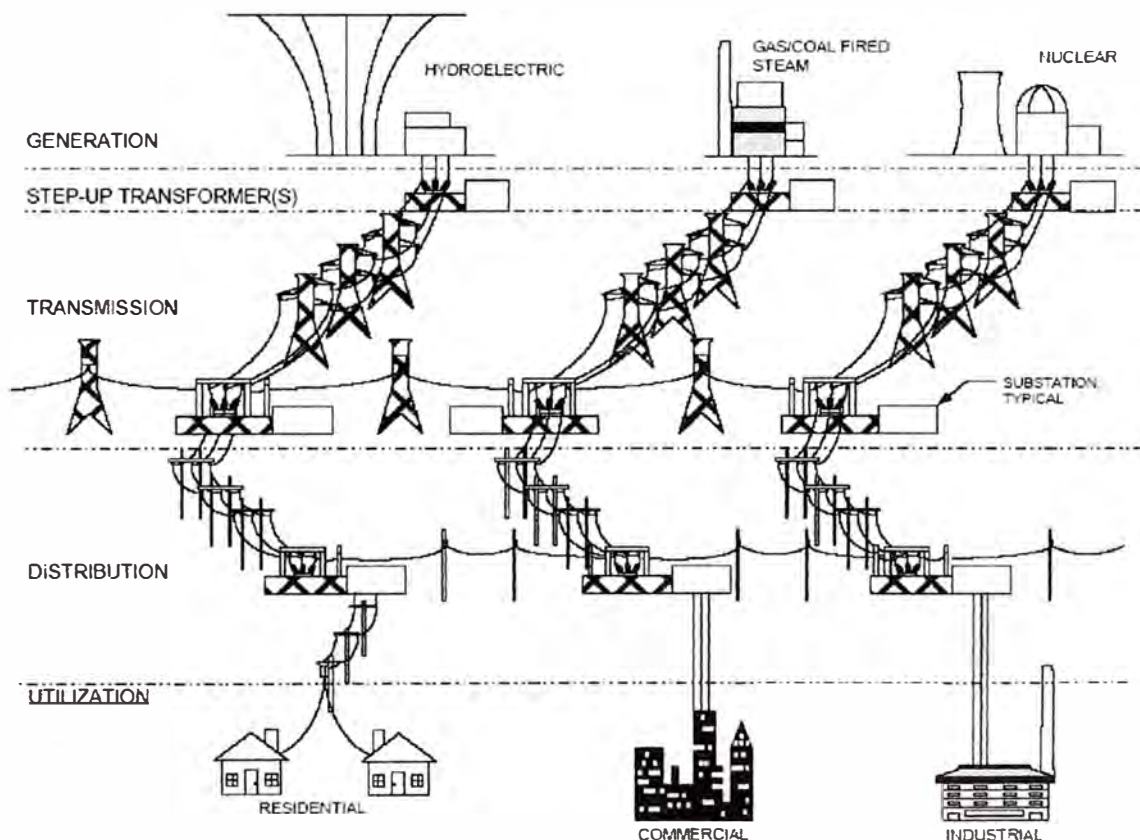


Fig. 1.1 Diagrama de Bloques de la Red Eléctrica

La figura 1.2 muestra una subestación eléctrica de transmisión típica.



Fig. 1.2 Subestación Eléctrica

Los equipos de protección y control de una subestación eléctrica se encuentran en tableros dentro de las edificaciones de la subestación o en el patio de llaves. La figura 1.3 muestra estos equipos dentro de una subestación.



Fig. 1.3 Equipos de Protección y Control de una Subestación de Distribución

La integración de subestaciones eléctricas es la integración de las funciones de protección, control y adquisición de datos, en un número mínimo de plataformas para

reducir los costos de capital y operación, reducir gabinetes y espacio en las salas de control, y eliminar la redundancia de equipos y bases de datos.

La automatización de subestaciones eléctricas es la implementación de funciones de operación, de subestaciones y alimentadores, y aplicaciones que van desde un sistema SCADA (Supervisión, Control y Adquisición de Datos) y de procesamiento de alarmas hasta el control integrado de tensión y potencia reactiva, a fin de optimizar la gestión de activos fijos y mejorar las eficiencias de operación y mantenimiento de la subestación, con mínima intervención humana. [2]

La integración y automatización de las subestaciones eléctricas puede dividirse en cinco niveles, como se muestra en la tabla 1.1.

TABLA 1.1 Niveles de Integración y Automatización de Subestaciones Eléctricas

Conexión con la Empresa Eléctrica
Aplicaciones de Automatización de Subestaciones
Integración de IEDs
Implementación de IEDs
Equipos del Sistema Eléctrico

El nivel más bajo está compuesto por los equipos del sistema eléctrico, tales como los transformadores e interruptores de potencia. Los niveles intermedios comprenden la implementación e integración de IEDs (dispositivos electrónicos inteligentes), y las aplicaciones de automatización de subestaciones. El nivel más alto es la conexión de la subestación con la empresa eléctrica.

Un IED es cualquier dispositivo que incorpora uno o más procesadores, con la capacidad de recibir datos de una fuente externa o enviar mandos de control a una fuente externa. Ejemplos de IEDs son los medidores electrónicos multifuncionales, relés digitales de protección, controladores, etc., y se muestran en la figura 1.4.



Fig. 1.4 Dispositivos Electrónicos Inteligentes (IEDs)

1.2 Transferencia de Información de la Subestación a la Empresa Eléctrica

Existen tres rutas funcionales de transferencia de información de la subestación a la empresa eléctrica, que se muestran en la tabla 1.2. La ruta más común es la que

transmite datos operacionales (por ejemplo voltios, amperios, etc.) al sistema SCADA de la empresa eléctrica. Esta información es crítica para los operadores de la empresa eléctrica que monitorean y controlan el sistema eléctrico. La ruta de datos que demanda más desafíos es la que transporta datos no operacionales al almacén de datos corporativos (Data Warehouse) de la empresa eléctrica, por las características de sus datos (que no necesariamente son puntos, sino archivos y formas de onda), la frecuencia de la transferencia de estos (no continua, sino bajo demanda), los protocolos utilizados para obtener los datos de los IEDs (no estándares, sino propietarios), y la forma de envío o extracción. La tercera ruta es el acceso remoto a un IED que atraviesa la arquitectura de integración de la subestación y aísla a un IED particular en la subestación.

TABLA 1.2 Rutas de Transferencia de Información de la Subestación a la Empresa Eléctrica

Empresa Eléctrica		
Datos Operacionales al Sistema SCADA	Datos no Operacionales al Almacén de Datos Corporativos	Acceso Remoto a IED
Aplicaciones de Automatización de la Subestación Eléctrica		
Integración de IEDs		
Implementación de IEDs		
Equipos del Sistema Eléctrico		

1.3 Arquitectura del Sistema de Automatización de Subestaciones

El diagrama de arquitectura de la figura 1.5 muestra las tres rutas funcionales de transferencia de información de la subestación a la empresa eléctrica, así como el sistema SCADA y el almacén de datos corporativos.

La ruta de datos operacionales utiliza los protocolos de comunicaciones soportados por el sistema SCADA. La ruta de datos no operacionales, transporta los datos no operacionales de los IEDs del sistema de automatización al almacén de datos corporativos, extrayéndolos mediante una aplicación del almacén de datos corporativos o enviándolos del sistema de automatización al almacén de datos corporativos en base a un disparador de evento o tiempo. Esta comunicación se suele hacer a través de un router. La ruta de acceso remoto a la subestación puede utilizar una conexión telefónica dial-up o VPN. El reloj GPS (Sistema de Posicionamiento Global por satélite), proporciona la referencia de tiempo al sistema de automatización y a los IEDs de la subestación. La computadora de usuario (Host Processor), por lo general es un servidor y proporciona la interfaz gráfica de usuario y el sistema de información histórica para archivar los datos operacionales y no operacionales. La interfaz SCADA maneja los puntos del sistema de

automatización que son enviados al sistema SCADA y el protocolo utilizado. Los IEDs con interfaces Ethernet (LAN IED en el diagrama) pueden conectarse directamente a la red de área local (LAN) del sistema de automatización. Los IEDs sin interfaces Ethernet requieren un módulo de interfaz de red (NIM) para la conversión de protocolo e interfaz física. Los IEDs pueden tener varias aplicaciones, tales como monitoreo de condiciones de equipos, protección e integración de entradas y salidas (I/Os) cableadas directamente. Entre estos últimos tenemos a los controladores, tales como los PLCs o equipos de interfaz, tales como una Unidad Terminal Remota (RTU) convencional.

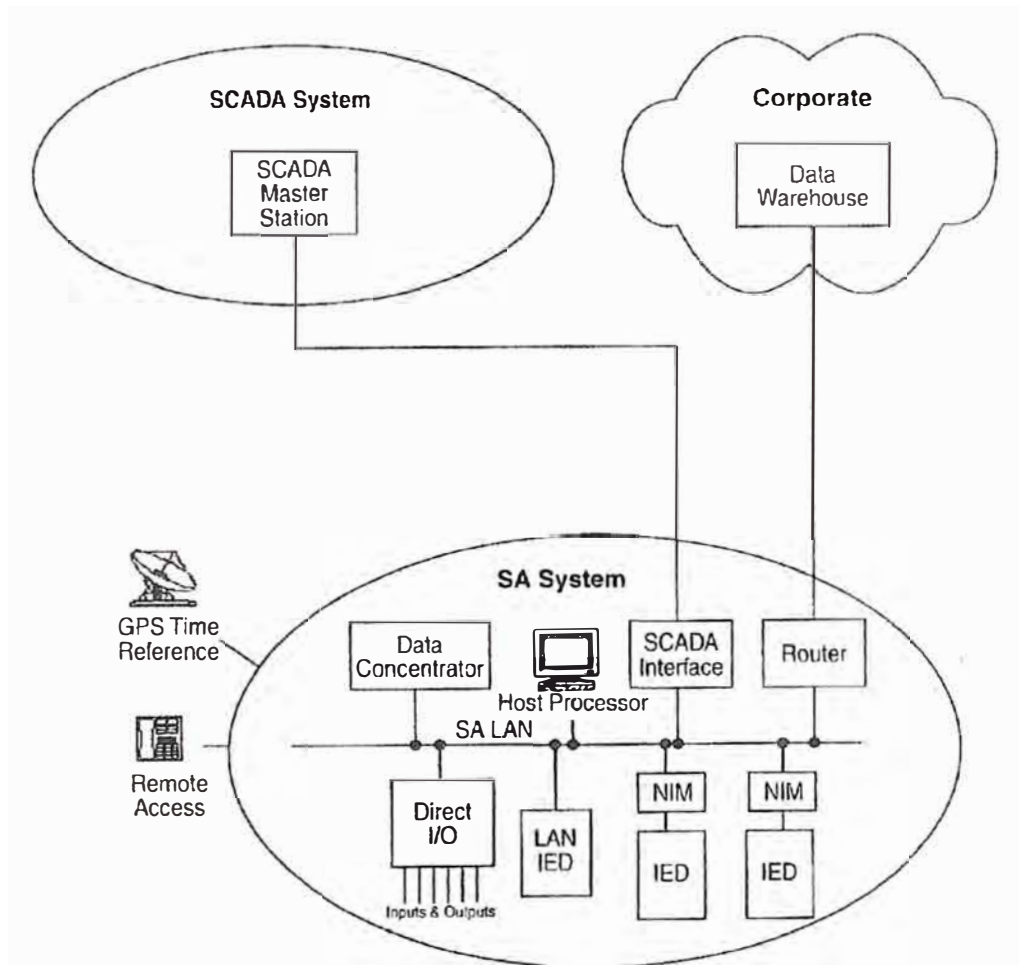


Fig. 1.5 Arquitectura Funcional del Sistema de Automatización de Subestaciones

Desde el punto de vista de integración, existen subestaciones pequeñas, denominadas secundarias, que tienen IEDs pero puede que no tengan una computadora de usuario. Utilizan un concentrador de datos para la integración de estos IEDs para enviarlos a una subestación más grande, denominada principal, que contiene un sistema completo de integración y automatización de subestaciones. Las figuras 1.6 y 1.7 muestran los sistemas de integración y automatización principal y secundaria, respectivamente.



Fig. 1.6 Sistema de Automatización de Subestación Principal



Fig. 1.7 Sistema de Automatización de Subestación Secundaria

1.4 Estándares y Protocolos de Comunicaciones

Esta sección proporciona un resumen de los principales estándares y protocolos, que prevalecen en la industria, para aplicaciones en subestaciones eléctricas.

1.4.1 Normas de Hardware Orientadas al Entorno de Subestaciones

El entorno de una subestación eléctrica es severo. La operación de equipos de potencia, tales como interruptores, seccionadores, bancos de capacitores, cambiadores de posición de taps de transformadores, etc., generan altos niveles de ruido eléctrico y transitorios. La aplicación exitosa de esquemas de control basados en comunicaciones sólo es posible, si los equipos de comunicaciones, utilizados por la red LAN de la subestación o que interactúan con la red de área extensa (WAN) de la empresa, satisfacen los mismos o superiores requisitos ambientales y de desempeño que los dispositivos de control que están siendo integrados al sistema de control distribuido. Esto se debe al hecho de que la falla de un elemento de la red LAN de la subestación, tal como un switch, producirá una pérdida de comunicaciones entre los IEDs conectados a el y, por tanto, la falla de cualquier esquema de control distribuido basado en el intercambio de mensajes de comunicación. [3]

En marzo del 2003 se aprobó la norma IEEE 1613 Requerimientos Ambientales y de Prueba para Dispositivos de Redes de Comunicaciones en Subestaciones Eléctricas. Integra las normas para sistemas de relés de protección instalados en el severo entorno de las subestaciones eléctricas, elaboradas por el Comité sobre Relés de Protección de Sistemas Eléctricos del IEEE:

- C37.90: define las condiciones de servicio, rangos de tensión, rangos de temperatura de operación, humedad, dieléctrico requerido y la capacidad para soportar impulsos
- C37.90.1: define la capacidad necesaria para soportar los transitorios generados en las subestaciones, sin daño o falsa operación.
- C37.90.2: define la inmunidad necesaria a la operación de transceptores portátiles, en las proximidades.
- C37.90.3: define la inmunidad a los transitorios debido a cargas estáticas.

IEEE 1613 adapta estas normas y las aplica ya no a nivel de sistema sino a nivel de dispositivo. Define las comunicaciones que serán utilizadas, durante las pruebas de los dispositivos de redes de comunicaciones, y desarrolla nuevos criterios de aceptación. La exigencia de que no se produzcan falsas operaciones en los relés, como consecuencia de los transitorios, fue modificada para los dispositivos de redes, permitiendo errores o interrupción de comunicaciones cuando se producen transitorios, pero se exige su recuperación automática, sin la intervención humana.

IEEE 1613 define dos clases de dispositivos de redes de comunicaciones:

- Clase 1: dispositivos en los que la pérdida temporal de comunicaciones y/o errores de comunicaciones pueden ser tolerados cuando se producen transitorios. Este es el requerimiento mínimo de la norma.
- Clase 2: dispositivos en los que se desea tener comunicaciones ininterrumpidas y libres de errores, cuando se producen transitorios. Operan al mismo nivel de los relés de protección. Para cumplir estos requerimientos, los medios de comunicación de estos dispositivos deben utilizar fibra óptica y las fuentes de alimentación deben estar protegidos para que no aparezcan transitorios en su entrada, que podrían afectar a las comunicaciones. Es un requerimiento opcional.

IEEE 1613 considera que los equipos han pasado las pruebas si durante, o como resultado de las pruebas, la totalidad de las siguientes condiciones son cumplidas para cada clase de dispositivo:

- No se produce daño de hardware.
- No se produce pérdida o corrupción de memoria almacenada o datos, incluyendo las configuraciones activas o almacenadas.
- No se produce reinicio del dispositivo y no se requiere reinicio manual.
- No se producen cambios en los estados de las salidas de estado eléctricas, mecánicas, o de comunicación. Esto incluye alarmas, salidas de estado, o señalizaciones.
- No se produce cambios de estado, erróneos y permanentes, de las salidas visuales, de audio o de mensaje. Se permiten cambios momentáneos de estas salidas durante las pruebas.
- No se produce error fuera de las tolerancias normales de las señales de comunicación de datos.

Similar a IEEE 1613, la norma IEC61850-3 Redes de Comunicaciones y Sistemas en las Subestaciones, delinea un marco completo para la automatización de subestaciones, incluyendo la inmunidad a interferencias electromagnéticas (EMI) y los requerimientos ambientales para redes y sistemas de comunicaciones en subestaciones. Los requerimientos de inmunidad a EMI de esta norma se derivan de la norma IEC 61000-6-5 Inmunidad para Entornos de Centrales y Subestaciones Eléctricas, que define un conjunto de ensayos de tipo EMI potencialmente destructivos, diseñados para simular fenómenos EMI continuos y transitorios en las subestaciones.

Ejemplos de pruebas de inmunidad a interferencias electromagnéticas (EMI) de las normas IEEE 1613 e IEC 61850-3, se muestran en las figuras 1.8 y 1.9.

IEEE 1613 EMI Immunity Type Tests			
IEEE C37.90.3	ESD	Enclosure Contact	+/- 8kV
		Enclosure Air	+/- 15kV
IEEE C37.90.2	Radiated RFI	Enclosure ports	35 V/m
IEEE C37.90.1	Fast Transient	Signal ports	+/- 4kV @ 2.5kHz
		D.C. Power ports	+/- 4kV
		A.C. Power ports	+/- 4kV
		Earth ground ports ³	+/- 4kV
IEEE C37.90.1	Oscillatory	Signal ports	2.5kV common mode @ 1MHz
		D.C. Power ports	2.5kV common & differential mode @ 1MHz
		A.C. Power ports	2.5kV common & differential mode @ 1MHz
IEEE C37.90	Dielectric Strength	Signal ports	2kVac
		D.C. Power ports	2kVac
		A.C. Power ports	2kVac

Fig. 1.8 Pruebas de inmunidad EMI, según la norma IEEE 1613

IEC 61850-3 EMI Immunity Type Tests			
TEST	Description	Test Levels	
IEC 61000-4-2	ESD	Enclosure Contact	+/- 6kV
		Enclosure Air	+/- 8kV
IEC 61000-4-3	Radiated RFI	Enclosure ports	10 V/m
IEC 61000-4-4	Burst (Fast Transient)	Signal ports	+/- 4kV @ 2.5kHz
		D.C. Power ports	+/- 4kV
		A.C. Power ports	+/- 4kV
		Earth ground ports ³	+/- 4kV
IEC 61000-4-5	Surge	Signal ports	+/- 4kV line-to-earth, +/- 2kV line-to-line
		D.C. Power ports	+/- 2kV line-to-earth, +/- 1kV line-to-line
		A.C. Power ports	+/- 4kV line-to-earth, +/- 2kV line-to-line
IEC 61000-4-6	Induced (Conducted) RFI	Signal ports	10V
		D.C. Power ports	10V
		A.C. Power ports	10V
		Earth ground ports ³	10V
IEC 61000-4-8	Magnetic Field	Enclosure ports	40 A/m continuous, 1000 A/m for 1 s
IEC 61000-4-29	Voltage Dips & Interrupts	D.C. Power ports	30% for 0.1s, 60% for 0.1s, 100% for 0.05s
		A.C. Power ports	30% for 1 period, 60% for 50 periods
IEC 61000-4-11			100% for 5 periods, 100% for 50 periods ²
IEC 61000-4-12	Damped Oscillatory	Signal ports	2.5kV common, 1kV differential mode @ 1MHz
		D.C. Power ports	2.5kV common, 1kV differential mode @ 1MHz
		A.C. Power ports	2.5kV common, 1kV differential mode @ 1MHz
IEC 61000-4-16	Mains Frequency Voltage	Signal ports	30V Continuous, 300V for 1s
		D.C. Power ports	30V Continuous, 300V for 1s
IEC 61000-4-17	Ripple on D.C. Power Supply	D.C. Power ports	10%

Fig. 1.9 Pruebas de inmunidad EMI, según la norma IEC 61850-3

1.4.2 Protocolos de Comunicaciones

Los principales protocolos de comunicaciones que se utilizan dentro de una subestación eléctrica se tratan en esta sección.

a) MODBUS

Es un protocolo de comunicaciones seriales, desarrollado por Modicon en 1979, para comunicación entre controladores de lógica programable (PLCs). Debido a su simplicidad

y especificación abierta, se ha convertido en un protocolo estándar de comunicaciones de facto en la industria, y actualmente es ampliamente utilizado por diferentes fabricantes y dispositivos electrónicos, tales como PLCs, unidades terminales remotas, relés y medidores, sensores y actuadores remotos.

El medio físico de conexión puede ser un bus semidúplex (half duplex) (RS-485 o fibra óptica) o dúplex (full duplex) (RS-422, BC 0-20mA o fibra óptica). La comunicación es asíncrona y las velocidades de transmisión previstas van desde los 75 baudios a 19.200 baudios. La máxima distancia entre estaciones depende del nivel físico, pudiendo alcanzar hasta 1200 m sin repetidores. [4]

La estructura lógica es del tipo maestro-esclavo, con acceso al medio controlado por el maestro. El número máximo de estaciones previsto es de 63 esclavos más una estación maestra.

La codificación de datos dentro de la trama puede hacerse en modo ASCII o puramente binario, según el estándar RTU (Remote Transmission Unit), cada mensaje obedece a una trama que se muestra en la figura 1.10.

Modo ASCII					
Comienzo de Trama	Dirección	Función	Datos	Control de Errores	Fin de Trama
:	2 bytes	2 bytes	N x 2 bytes	2 bytes	CR + LF

Modo RTU					
Comienzo de Trama	Dirección	Función	Datos	Control de Errores	Fin de Trama
Tiempo de 3 bytes	1 bytes	1 bytes	N x 1 bytes	2 bytes	

Fig. 1.10 Tramas Modbus

Existen versiones del protocolo Modbus para puertos seriales y Ethernet. También existe una versión ampliada, Modbus Plus (Modbus+ o MB+), de propiedad de Modicon, que utiliza par trenzado a 1 Mbit/s y requiere interfaces especiales para conectarse a un puerto serial de ordenador.

b) DNP3.0 Serial y DNP3.0/LAN

El Protocolo para Red Distribuida (DNP) fue creado por Westronic, Inc. (actualmente GE Harris) en 1990 y publicado en 1993. Su versión actual es la 3.0. El Grupo de Usuarios de DNP 3 tiene la responsabilidad de mantener y definir futuras especificaciones del

protocolo. Está compuesto por usuarios y fabricantes, con más de 300 miembros en la actualidad

DNP3 proporciona multiplexación, fragmentación de datos, verificación de errores, control de enlace, priorización, y servicios de direccionamiento de capa 2 para los datos de usuario. Hace uso de sumas de verificación (checksums) integradas en sus paquetes de datos, con la intención de hacer frente a los entornos muy ruidosos en los que es utilizado. Una trama DNP3 consta de una cabecera y sección de datos, que soporta hasta 65,520 direcciones individuales, 2 bytes de verificación de errores (CRC) cada 16 octetos de datos, y provisiones para soportar respuestas no solicitadas, reporte de eventos, representación de datos en diferentes formatos, así como priorización de datos. La trama y cabecera del protocolo DNP3 se muestran en la figura 1.11.

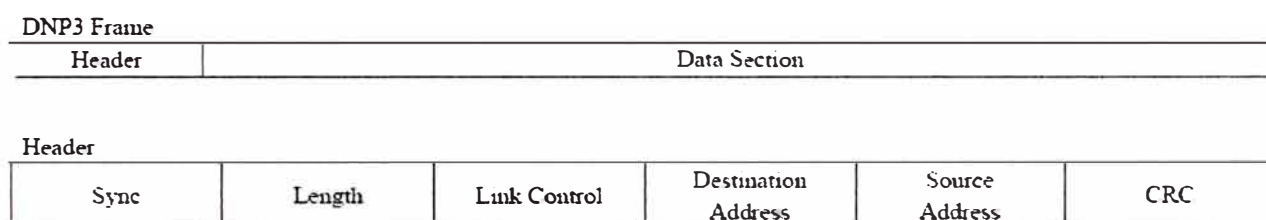


Fig. 1.11 Trama y cabecera del protocolo DNP3

DNP3 ofrece varias características importantes para aplicaciones en empresas eléctricas:

- Opciones de salidas
- Configuración y transferencia de archivos seguros
- Direccionamiento de hasta 65,520 dispositivos en un solo enlace
- Sincronización de tiempo y eventos con estampa de tiempo
- Mensajes de difusión (broadcast)
- Transferencia de archivos
- Confirmación de las capas de enlace de datos y de aplicación

DNP3 originalmente fue diseñado en base a tres capas del modelo OSI: la capa de aplicación, la capa de enlace de datos y la capa física. La capa de aplicación está basada en objetos proporcionados para la mayoría de formatos de datos comunes. La capa de enlace de datos proporciona varios métodos de recuperación de datos, tales como interrogación por clases y variaciones de objetos. La capa física normalmente es una interfaz serial RS-232 o RS-485.

DNP3 es adecuado para aplicaciones de comunicaciones de RTU a IED, comunicaciones maestro a esclavo, comunicaciones peer-to-peer y aplicaciones de redes. DNP3 soporta múltiples modos de operación, tales como respuesta de interrogación, reporte por

excepción, respuestas no solicitadas y peer-to-peer. Permite múltiples maestros y soporta inteligencia distribuida.

En los últimos años, se ha utilizado TCP/IP para el transporte de mensajes DNP3, en lugar de los medios de comunicación seriales estándares. Las tramas de capa de enlace son encapsuladas en los paquetes TCP/IP. Este enfoque ha permitido a DNP3 aprovechar de la tecnología de Internet y la recolección de datos y control entre dispositivos muy distantes a través de las redes Ethernet LAN y WAN.

c) IEC 61850

El estándar IEC 61850 Redes y Sistemas de Comunicaciones en Subestaciones Eléctricas fue desarrollado por los Grupos de Trabajo WG 10, WG 11 y WG-12 del Comité Técnico 57 del IEC (IEC - TC 57) y se estableció como estándar el año 2005. Es un estándar de comunicaciones para la automatización de subestaciones, cuyo objetivo principal es permitir la interoperabilidad de dispositivos IED, especialmente de diferentes fabricantes, dentro de la subestación. Se divide en diez partes, como muestra la figura 1.12.

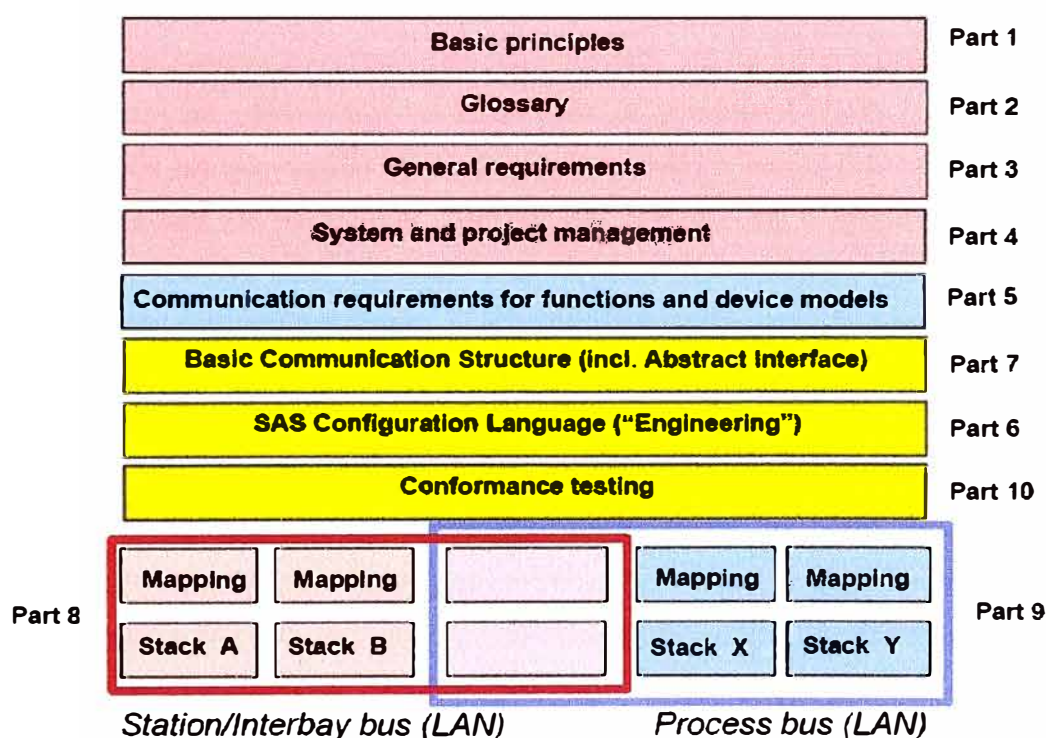


Fig. 1.12 Estructura del estándar IEC 61850

IEC 61850 especifica una arquitectura con dos buses basados en redes LAN Ethernet: un bus de estación, utilizado para la comunicación entre IEDs, y un bus de proceso, utilizado

para enviar información de sensores digitales a los IEDs. Estos buses se muestran en la figura 1.13.

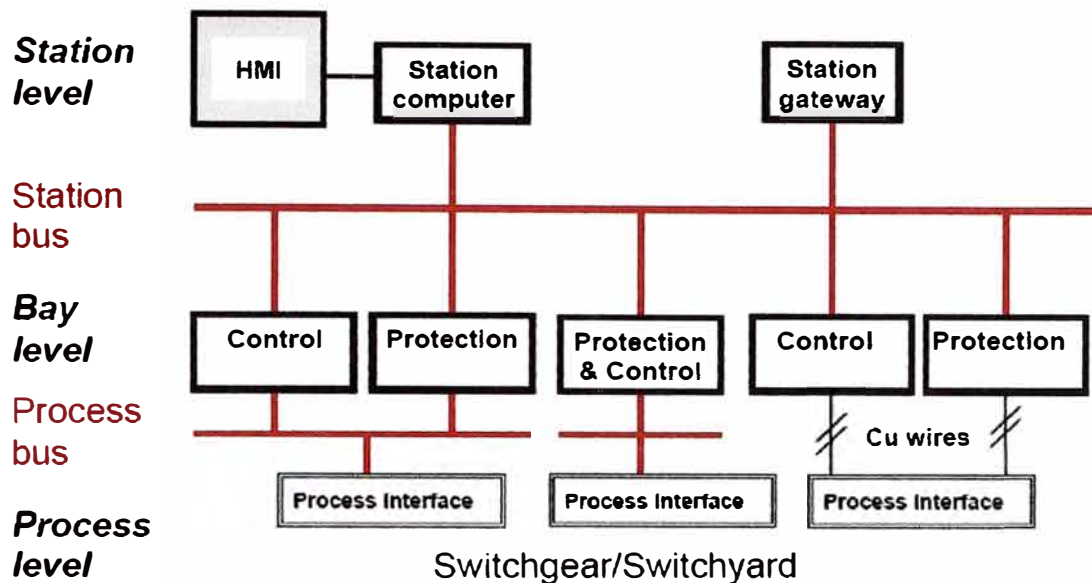


Fig. 1.13 Arquitectura de subestación IEC 61850

Una característica de IEC 61850 es la representación o modelo de datos orientada a objetos, para cada función (por ejemplo, el modelo de los datos de entrada y salida de un transformador), en forma de convenciones estándares de nombre, estructuras y formatos. El modelo de datos es desarrollado en lenguaje UML (Unified Modelling Language).

Otra característica es que define un conjunto de servicios abstractos de comunicaciones (ACSI) que abordan los requisitos básicos del proceso de intercambio de datos de aplicaciones en tiempo de ejecución, a través de servicios de comunicaciones independientes del protocolo y medio. Ejemplos de este tipo de intercambio son la lectura de la posición actual de un interruptor, un comando de operador o el disparo de una función de protección para cambiar la posición de un interruptor.

Proporciona un lenguaje estandarizado de configuración de subestaciones (SCL), utilizado para el intercambio de datos de configuración de todas las aplicaciones y dispositivos de automatización (IEDs). Un archivo SCL utiliza un formato XML.

Soporta mensajería peer-to-peer de alta velocidad, utilizando las definiciones de Evento de Subestación Orientado a Objetos Genérico (GOOSE) y Evento de Estado de Subestación Genérico (GSSE). Esta característica está diseñada para soportar aplicaciones de protección del sistema.

GOOSE, GSSE y los Valores Medidos Muestreados SMV, son datagramas multicast peer-to-peer sobre la red LAN de subestaciones y no son enrutables. Los mensajes deben ser transmitidos dentro de 4 milisegundos y por ello la encriptación, u otras

medidas de seguridad que afectan a las velocidades de transmisión, no son aceptables. Por lo tanto, la autenticación es la única medida de seguridad incluida, por ello la especificación IEC 62351-6 proporciona un mecanismo que involucra requerimientos mínimos de cálculo para que estos perfiles de comunicación firmen digitalmente los mensajes.

Ya que IEC 61850 es un protocolo relativamente nuevo, algunos fabricantes han desarrollado dispositivos de interfaz que sirven como un gateway IEC 61850, que permiten integrar sus relés a redes basadas en IEC 61850. Sin embargo, la experiencia demuestra que los gateways de este tipo pueden introducir latencias significativas, que no son aceptables por las empresas eléctricas.

Dado que los mensajes de IEC 61850 no son enrutables, el transporte fuera de la subestación no ha sido cubierto por el estándar. El año 2005 se formó un grupo de trabajo dentro del IEC para definir una especificación para el uso de IEC61850 para comunicaciones entre subestaciones o con el centro de control, cuya especificación y posterior implementación se prevé estará disponible muy pronto.

Aunque el protocolo DNP fue diseñado y es ideal para aplicaciones SCADA, IEC 61850 es más adecuado para aplicaciones de automatización. Si bien la tendencia por IEC 61850 parece ser superior, DNP continuará siendo utilizado por instalaciones existentes y por muchas aplicaciones SCADA.

d) Ethernet

El término Ethernet se refiere a la familia de productos de red LAN, cubiertos por el estándar IEEE 802.3, que define lo que se conoce comúnmente como el protocolo CSMA/CD. En la actualidad, se definen cuatro velocidades de datos que operan sobre cables de fibra óptica y par trenzado:

- 10 Mbps - Ethernet
- 100 Mbps - Fast Ethernet
- 1000 Mbps - Gigabit Ethernet
- 10 Gigabit Ethernet

Ethernet es utilizado por la mayoría de PCs y estaciones de trabajo del mundo, conectadas a redes LAN, ya que su protocolo es fácil de entender, implementar, administrar y mantener, permite implementaciones de red de bajo costo, proporciona una amplia flexibilidad topológica para la instalación de redes, y garantiza la interconexión y operación exitosa de productos conforme a estándares, independientemente del fabricante.

Los medios de interconexión las redes LAN Ethernet incluyen tres tipos de cables de cobre: par trenzado no apantallado (UTP), par trenzado apantallado (STP) y par trenzado con pantalla global (FTP); además de varios tipos de cables de fibra óptica.

Ethernet define las características de cableado y señalización para la capa física, dos medios de acceso a la red en la Capa de Control de Acceso al Medio (MAC)/Enlace de Datos, y un formato de direccionamiento común. Por encima de la capa física, las estaciones Ethernet se comunican entre sí enviando paquetes de datos. A cada estación Ethernet se le entrega una única dirección MAC de 48 bits, que es utilizada para especificar tanto el destino como la fuente de cada paquete de datos. Las tarjetas de interfaz de red (NICs) de una estación Ethernet, normalmente no aceptan paquetes dirigidos a otras estaciones.

Las sencillas redes Ethernet conmutadas todavía sufren de una serie de problemas:

- Adolecen de puntos únicos de falla. Si un enlace o switch falla, la red puede quedar dividida.
- Es posible engañar a los switches o hosts para enviar datos a una máquina, incluso si esa no es la intención.
- Es posible inundar la red con tráfico de broadcast, formando un ataque de denegación de servicio contra cualquier host, que se ejecuta a la misma o menor velocidad que el dispositivo de ataque.
- Adolecen de puntos de estrangulamiento de ancho de banda, en los cuales el excesivo tráfico hace caer un enlace.

Algunos switches administrables ofrecen una variedad de herramientas para combatir estos problemas, entre ellas:

- Protocolo Spanning-tree para mantener los enlaces activos de la red como un árbol, mientras permite bucles físicos de redundancia.
- Diversas características de protección de puertos, ya que es mucho más probable el ataque sobre un puerto del sistema que sobre un enlace switch-switch.
- VLANs para mantener diferentes clases de usuarios por separado, mientras se utiliza la misma infraestructura física.
- Enrutamiento rápido en los niveles superiores entre VLANs.
- Agrupación de enlaces para agregar ancho de banda a enlaces sobrecargados y proporcionar alguna medida de redundancia.

e) IPv4 e IPv6

El protocolo IPv4 es la cuarta versión del Protocolo IP y es el protocolo de capa de red dominante en Internet. Es un protocolo orientado a datos, utilizado sobre una red Internet

conmutada de paquetes. Se trata de un protocolo de mejor esfuerzo en el sentido de que no garantiza la entrega, pudiendo dar lugar a duplicación de paquetes y/o paquetes fuera de orden. Estos problemas son tratados por un protocolo de capa superior (por ejemplo TCP o UDP).

El propósito general de IP es proporcionar direccionamiento único de computadoras a nivel mundial, para garantizar que dos computadoras puedan identificarse entre sí a través de Internet.

IPv4 utiliza direcciones de 32 bits, limitándose a $2^{32} = 4.294.967.296$ direcciones únicas, muchas de las cuales están dedicadas a redes LAN. Por el crecimiento enorme que ha tenido Internet, mucho más de lo que esperaba cuando se diseñó IPv4, además del desperdicio de direcciones en muchos casos, desde hace varios años se nota la escasez de direcciones IPv4. Esta limitación ayudó a estimular el impulso hacia IPv6, que esta todavía en las primeras fases de implantación y se espera termine reemplazando a IPv4.

Para conectar las redes IP privadas en cada extremo de Internet, se utilizan conexiones de redes privadas virtuales (VPNs) a través de la porción pública de Internet. Las VPNs trabajan insertando un paquete IP (paquete encapsulado) directamente en el campo de datos de otro paquete IP (paquete encapsulante) y utiliza una dirección públicamente enrutable en el paquete encapsulante. Una vez que el paquete VPN es enrutado a través de la red pública y alcanza el punto final, el paquete encapsulado es extraído y luego transmitido a la red privada, como si las dos redes privadas estuvieran directamente conectadas. Opcionalmente, el paquete encapsulado puede ser encriptado, para proteger los datos mientras se encuentren sobre la red pública.

IP tiene la capacidad de proporcionar un parámetro de Calidad de Servicio (QoS). En una cabecera IP, se asignan 8 bits para definir un Tipo de Servicio (TOS) en términos de precedencia, retardo, rendimiento y confiabilidad. La intención original de este campo era que el host de envío especifique una preferencia, en la forma en que el datagrama sería manejado, cuando se desplace a través de la red. Estos bits han sido redefinidos recientemente por la IETF (Fuerza de Trabajo para la Ingeniería de internet) para acomodar los servicios diferenciados (DiffServ). Las nuevas tecnologías emergentes requieren flujos de datos en tiempo real y por tanto harán uso del campo TOS. Ejemplos de estas son Voz sobre IP (VoIP) utilizada para transportar voz a través de las redes de datos, así como aplicaciones SCADA en tiempo real en el entorno de las empresas eléctricas.

El protocolo IPv6 es la nueva versión del protocolo IP. Su principal mejora es el incremento del número de direcciones disponibles para los dispositivos de red, permitiendo, por ejemplo, que cada teléfono celular y dispositivo electrónico móvil tenga

su propia dirección IP. IPv6 soporta 2^{128} direcciones, que es cerca de 670 mil billones de direcciones por mm^2 de superficie de La Tierra.

Para aplicaciones de empresas eléctricas, IPv6 tiene un potencial para proporcionar suficientes direcciones únicas para el medidor de cada cliente, así como dispositivos del hogar que pueden interactuar con un sistema de gestión de carga. Sin embargo, la necesidad para implementar IPV6 a estas aplicaciones todavía está siendo revisada.

IPSec (Seguridad IP) es una parte obligatoria de IPv6 y opcional en IPv4. Es un conjunto de protocolos que protegen las comunicaciones del Protocolo IP mediante la encriptación y/o autenticación de cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves criptográficas.

Existen dos modos de operación de IPsec: modo de transporte y modo de túnel. En el modo de transporte sólo la carga útil (mensaje) del paquete IP es encriptada. Es totalmente enrutable ya que la cabecera IP es enviada como texto sin formato, sin embargo, no puede cruzar interfaces con NAT. Es utilizado para comunicaciones host-to-host. En el modo de túnel, todo el paquete IP es encriptado. Luego, debe ser encapsulado en un nuevo paquete IP para su enrutamiento. Es utilizado para comunicaciones red a red (túneles seguros entre routers), host a red y host-a-host.

IPsec se utiliza principalmente para crear VPNs (redes privadas virtuales) para cualquiera de los dos modos de operación. Sin embargo, las implicaciones de seguridad son diferentes entre estos dos modos.

f) ICCP

Las empresas eléctricas en todo el mundo especifican el Protocolo ICCP (Protocolo de Comunicaciones entre Centros de Control) para proporcionar el intercambio de datos entre centros de control, empresas eléctricas y no eléctricas. ICCP es también una norma internacional: IEC TASE.2 (Telecontrol Application Service Element 2). La arquitectura del protocolo ICCP se muestra en la figura 1.14.

ICCP opera a través de redes LAN y WAN, habilitando el intercambio de datos de monitoreo y control del sistema eléctrico en tiempo real e histórico, incluyendo valores medidos, datos de programación, datos de conteo de energía y mensajes de operador. Permite el intercambio de datos entre múltiples sistemas EMS de centros de control, sistemas EMS y DCS de planta de energía, sistemas EMS y SCADA de distribución, sistemas EMS y otros sistemas, y sistemas EMS/SCADA con subestaciones.

Una aplicación ICCP consta de software cliente y software servidor. El software cliente se conecta, desde programas de operación y aplicación, a otros miembros de la red solicitando datos de puntos y enviando solicitudes de control. El software servidor

responde a las solicitudes del cliente devolviendo los datos solicitados y ejecutando (si es posible) los controles solicitados. Junto con los datos, se transmiten códigos de calidad, tales como ingresos manuales y falla de telemetría. En las operaciones de control de dispositivos, se respetan las etiquetas del sistema servidor. El administrador del sistema define en cada sistema servidor que puntos de su base de datos serán accesibles para interrogación y control de otros sistemas miembros en la red, definiendo con un editor, los grupos de puntos analógicos, de estado, acumuladores y de control, llamados RTUs virtuales.

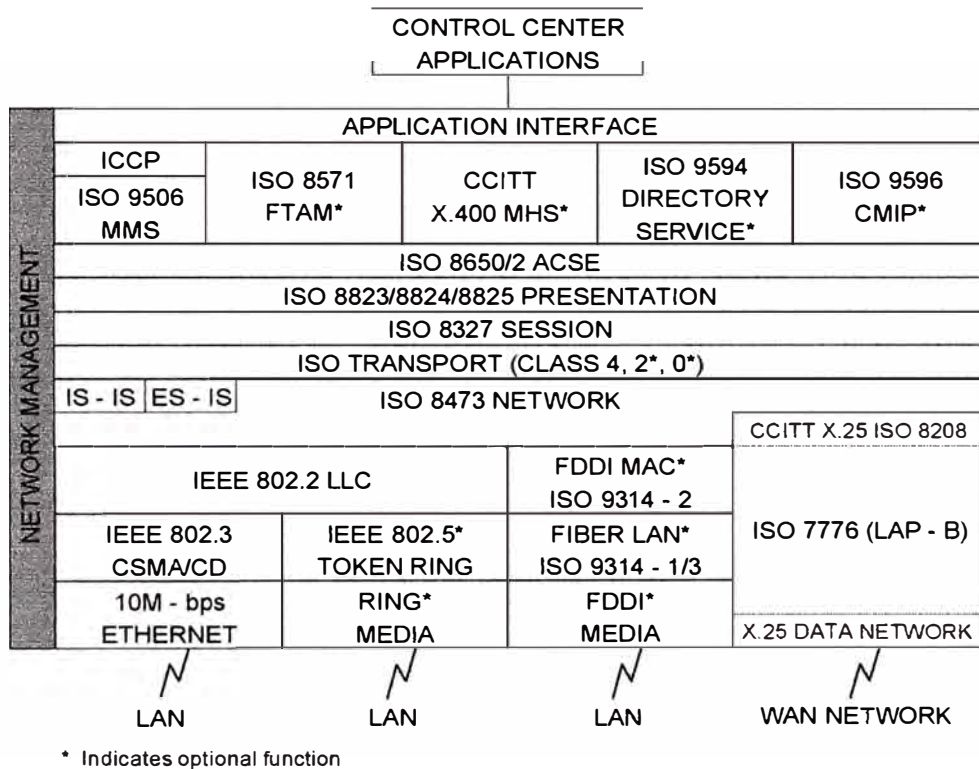


Fig. 1.14 Arquitectura del protocolo ICCP

Cualquier miembro de la red ICCP puede actuar como cliente o servidor o ambos. La relación entre cualquier par de miembros puede ser completamente bidireccional, es decir, ambos miembros pueden actuar como cliente y servidor al mismo tiempo. Es más, cualquier miembro puede actuar como servidor de múltiples clientes y, al mismo tiempo, actuar como cliente de múltiples servidores. El establecimiento de las conexiones es responsabilidad del software cliente. El modelo Cliente/Servidor del protocolo ICCP se muestra en la figura 1.15.

En nuestro país, las empresas eléctricas utilizan el protocolo ICCP para la conexión a centros de control externos, pero principalmente para la conexión al coordinador de la

operación del sistema eléctrico peruano, el COES SINAC (Comité de Operación Económica del Sistema Eléctrico Interconectado Nacional).

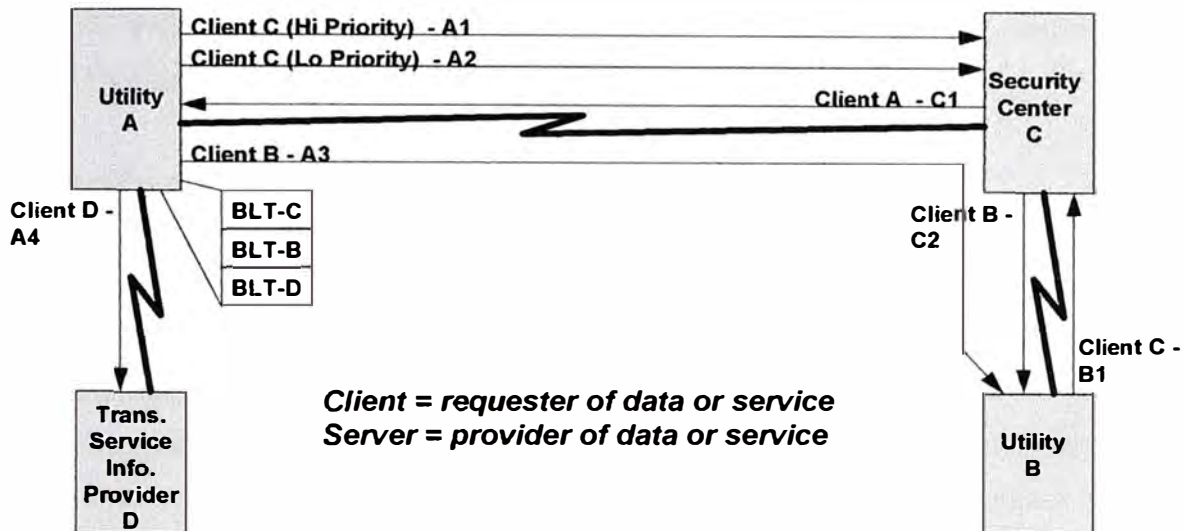


Fig. 1.15 Modelo Cliente/Servidor del protocolo ICCP

g) Uso de Protocolos de Emulación de Terminal

Las empresas eléctricas suelen utilizar programas de emulación de terminal para acceder a los dispositivos de subestaciones. Un programa emulador de terminal emula un terminal de vídeo tonto dentro de otra arquitectura de despliegue y permite al usuario acceder al terminal de texto y todas sus aplicaciones. Se puede ejecutar a través de telnet, Secure Shell (SSH), o dial-up. Ejemplos de programas de emulación de terminal utilizados por empresas eléctricas bajo Microsoft Windows, son el programa integrado HyperTerminal y programas de terceros como Tera Term y SecureCRT. El programa Procomm basado en MS-DOS también es utilizado. En general, las empresas eléctricas no han establecido un programa de emulación de terminal estándar, siendo HyperTerminal la aplicación de facto.

1.4.3 Tendencias de la Industria

a) Uso de Dispositivos Electrónicos Inteligentes

Los IEDs, tales como relés de protección, controladores de reclosers y monitores de condiciones de equipos, se vienen implementando en casi todas las subestaciones nuevas y existentes. La fabricación y modelos de IEDs, así como las interfaces de comunicaciones se han estandarizado, proporcionando un entorno de operación y mantenimiento familiar a ingenieros, operadores y técnicos, y su implementación es más fácil. Del mismo modo, los formatos de datos operacionales y no operacionales se han estandarizado, simplificando el almacenamiento, mantenimiento y los requerimientos de

análisis. La mayoría de empresas eléctricas tienen IEDs en operación con puertos seriales, pero los IEDs modernos cuentan con puertos Ethernet disponibles. El tema por resolver todavía es, si se debe desarrollar una arquitectura con protocolo DNP3 o IEC61850. Varias empresas eléctricas tienen implementado DNP3, pero están pensando en IEC61850 como el estándar futuro.

b) Migración de Comunicaciones Seriales a Ethernet

Las comunicaciones seriales son tradicionales, bien conocidas y han sido ampliamente probadas en subestaciones eléctricas. Se encuentran en IEDs existentes, poseen robusta presentación y velocidades aceptables, y requieren buses continuos para su funcionamiento.

Estos IEDs pueden ser llevados a una red IP mediante convertidores seriales a Ethernet como servidores de dispositivo seriales (terminal servers) y convertidores de medios (media converters), como se muestra en la figura 1.16. Estos dispositivos permiten que una empresa eléctrica, que no está en condiciones de reemplazar sus dispositivos seriales, los conserve y utilice una red IP al mismo tiempo. Estos dispositivos encapsulan los datos RS-232/422/485 y protocolos seriales, como DNP o Modbus, en TCP/IP, para transportarlos sobre redes IP, obteniendo las eficiencias asociadas de un sistema de comunicaciones en red.

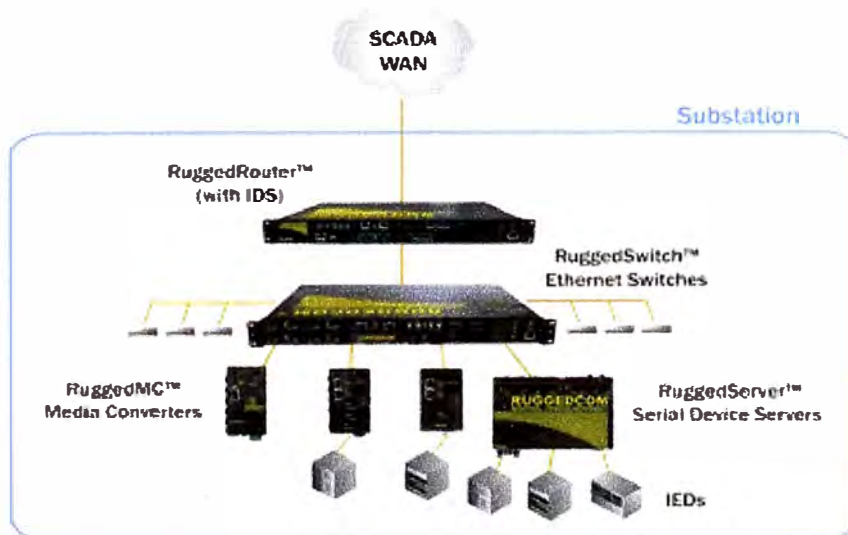


Fig. 1.16 Integración de dispositivos seriales

En el mercado existen dispositivos Terminal Server desde uno hasta 32 puertos seriales de conexión. Un Terminal Server con un puerto puede costar \$180 y de 16 puertos entre \$1300 y \$1600.

c) SONET

El estándar SONET (Red Óptica Síncrona), de la cual deriva SDH (Jerarquía Digital Síncrona), ha sido utilizada en nuestro continente por varias empresas eléctricas desde hace muchos años y, en cierto sentido, es la red de "legado" de fibra óptica. Fue desarrollada por las compañías telefónicas, para redes de alta capacidad y alta confiabilidad. El sistema SONET fue cuidadosamente especificado para permitir la rápida recuperación de fallas de equipos (menos de 50 milisegundos) y para evitar problemas técnicos, como la sincronización de tiempo, que alteran la confiabilidad. Su configuración más utilizada es en anillo, que incorpora diversidad de rutas, lo que significa que si se rompe o corta una ruta, existen rutas físicamente independientes que pueden hacerse cargo del tráfico sin interrupciones. El anillo se establece alrededor de una zona de varios kilómetros de distancia. La figura 1.17 muestra una topología SONET/SDH representativa.

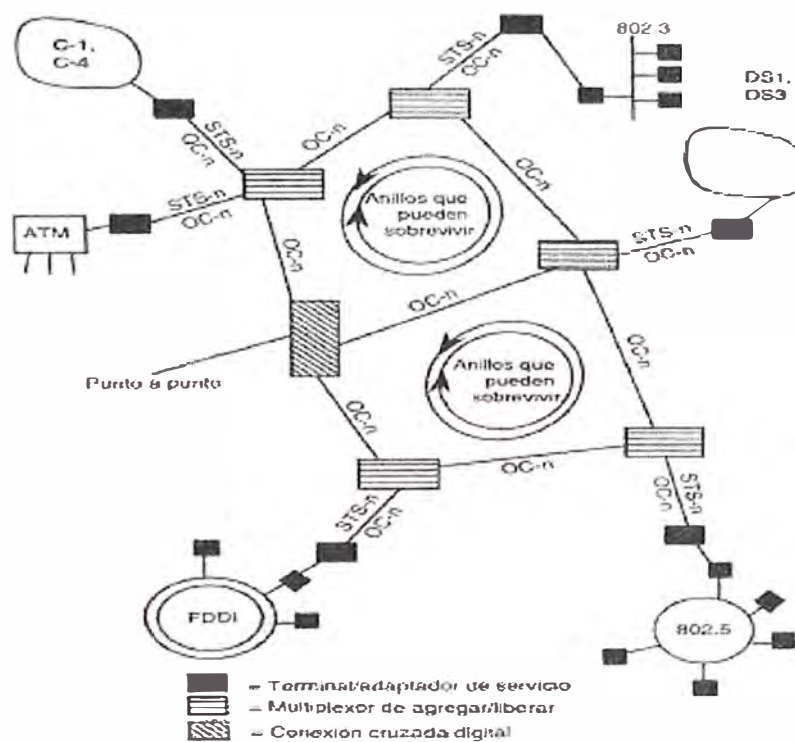


Fig. 1.17 Topología SONET/SDH

Los actuales sistemas SONET se definen por un conjunto de velocidades estándares de transmisión de datos, que se muestran en la tabla 1.3.

La mayoría de empresas eléctricas la utilizan como medio de transporte. Es altamente confiable, basada en esquemas de multiplexación por división de tiempo, pero también puede ser costosa. Ethernet puede segmentarse y colocarse dentro de un determinado ancho de banda SONET, pero no puede extenderse fuera de ese ancho de banda fijo.

TABLA 1.3 Señales y velocidades binarias SONET

Portadora óptica	Señal eléctrica	Velocidad Binaria (Mbps)	Equivalencia SDH
OC-1	STS-1	51.84	STM-0
OC-3	STS-3	155.52	STM-1
OC-9	STS-9	466.56	-
OC-12	STS-12	622.08	STM-4
OC-18	STS-18	933.12	-
OC-24	STS-24	1244.16	-
OC-36	STS-36	1866.24	-
OC-48	STS-48	2488.32	STM-16
OC-96	STS-96	4976.64	-
OC-192	STS-192	9953.28	STM-64

d) Infraestructura Única Consolidada

La tendencia de la industria más significativa tomada en cuenta por las empresas eléctricas es la migración a redes basadas en IP. Esta tendencia facilita la idea de convergencia de red, cuyo objetivo es encontrar una plataforma única que permita que múltiples redes se comuniquen e interactúen. A nivel de una subestación eléctrica, la convergencia de red y la automatización pueden lograrse a través de una red LAN Ethernet, proporcionando enlaces a equipos de comunicaciones ópticas de gran ancho de banda, equipos de gestión de energía y sistemas de seguridad que incluyen video vigilancia, controladores de acceso y monitoreo remoto.

La ventaja de utilizar la arquitectura Ethernet en subestaciones es que esta proporciona estandarización, que también impulsa la tendencia de convergencia de red. Los IEDs modernos con interfaces basadas en IP, permiten la interoperabilidad de múltiples proveedores y con otros equipos de la subestación.

Las comunicaciones recomendadas dentro de las subestaciones también incluyen el uso de concentradores de datos, para acomodar más eficazmente el tráfico para el transporte sobre la red WAN.

Para soportar necesidades de redes locales en una subestación, los proveedores proporcionan equipos robustos, que incluyen routers, switches, relés, dispositivos de interfaz de red y equipos de radio no licenciados.

e) Separación de Rutas de Datos dentro de la Infraestructura Consolidada

Si bien la migración a una infraestructura consolidada es una tendencia de la industria, existe todavía una necesidad de separar los datos operacionales en tiempo real, que requieren entrega a un centro de control en pocos segundos, de los datos no operacionales, que no tienen tales exigencias de entrega. Con las redes Ethernet e IP, el uso de VLANs se está convirtiendo en parte de esta infraestructura. Desde el punto de

vista de la seguridad, la separación de datos críticos de los no críticos también es importante, con medios de protección como firewalls o DMZs. La separación de datos también puede estar dirigida al establecimiento de redes físicamente separadas, para garantizar la seguridad necesaria y los requerimientos de latencia. Esto se está volviendo predominante en las subestaciones, donde una red LAN operacional es separada totalmente de la red LAN corporativa menos crítica, como muestra la figura 1.18.

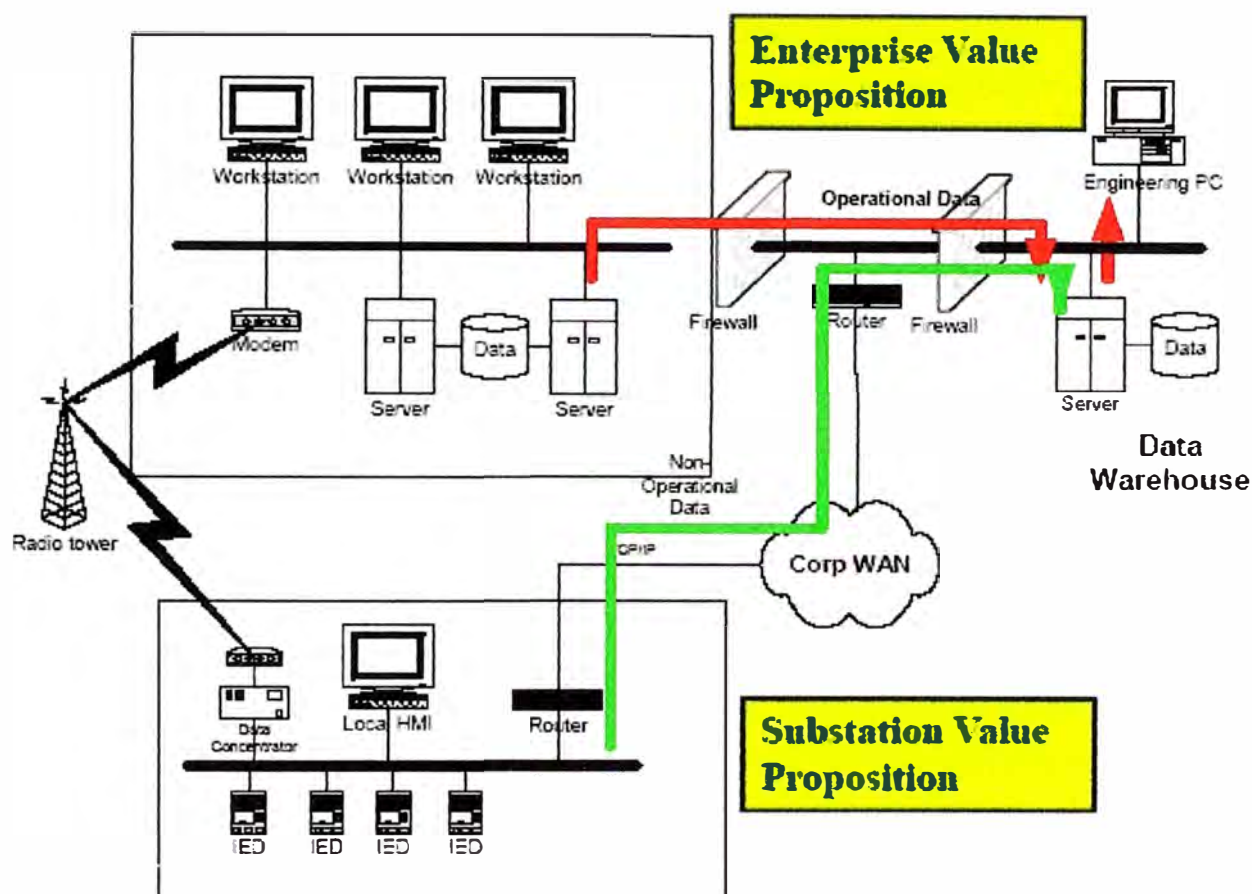


Fig. 1.18 Separación de rutas de datos

1.5 Sincronización de Tiempo en Subestaciones

La respuesta adecuada de las funciones de protección y control a las perturbaciones de la red eléctrica, requiere la coordinación de relés de protección y sistemas de comunicaciones en lugares dispersos. El análisis posterior a la perturbación, de la operación del sistema de protección y control, también requiere el uso de información de secuencia de eventos y datos oscilográficos, proporcionados por equipos de monitoreo en estos lugares dispersos. Algunas empresas eléctricas también relacionan datos de descargas atmosféricas, proporcionados por servicios meteorológicos, a la ocurrencia de fallas en la red de transmisión, como parte de este análisis posterior de falla.

Estos análisis posteriores a las perturbaciones de la red eléctrica, requieren el uso de datos con etiquetas de tiempo, para asegurar que estos eventos sean debidamente secuenciados. Para ello en cada lugar se utiliza relojes sincronizados a una única unidad de referencia de tiempo, para estampar el tiempo a los eventos, con una resolución de estampado de un milisegundo o superior.

La escala de tiempo estándar, utilizada por la mayoría de naciones, es el Tiempo Universal Coordinado (UTC), que puede ser distribuida por diversos medios, pero el más utilizado es el satelital mediante GPS (sistema de posicionamiento global).

El sistema de automatización de subestaciones debe incluir un receptor GPS en cada subestación, con la capacidad de sincronizar los componentes del sistema, conectados directamente a la red LAN de la subestación, mediante protocolo NTP (Protocolo de Tiempo de Red) o SNTP (Protocolo de Tiempo de Red Simple). El receptor GPS también debe incluir una o más salidas IRIG B, para la sincronización de dispositivos del sistema que no están directamente conectados a la red LAN o que requieran sincronización de tiempo por debajo del milisegundo.

Para soportar precisiones superiores a 1 milisegundo, ha sido desarrollada la norma IEEE 1588 Protocolo de Sincronización de Relojes de Precisión para Sistemas de Medición y Control en Red. Esta norma define un protocolo que permite la sincronización precisa de relojes en sistemas de medición y control, implementado con tecnologías como comunicación de red, cómputo local y objetos distribuidos. El protocolo es aplicable a sistemas comunicándose por redes de área local, soportando mensajería multicast, incluyendo, pero no limitado a, Ethernet. Permite sistemas heterogéneos con relojes de sincronización de diferente precisión, resolución y estabilidad. Soporta la precisión de sincronización de todo el sistema por debajo del microsegundo, con mínimos recursos de red y de cómputo de reloj local. El comportamiento predeterminado del protocolo permite sistemas sencillos sean instalados y operados, sin necesidad de atención administrativa de los usuarios. En la actualidad, el soporte para IEEE 1588 no está disponible en todos los receptores GPS del mercado.

CAPÍTULO II

CRITERIOS DE DISEÑO

2.1 Diseño de una red de comunicaciones para automatización

El diseño de un sistema de comunicaciones para la automatización de subestaciones incluye los siguientes pasos: [5]

- a) Definir los nodos del sistema de mensajería
 - b) Desarrollar la topología del sistema de comunicación
 - c) Determinar los requerimientos de interoperabilidad de dispositivos
 - d) Elegir los medios de comunicación
 - e) Definir la arquitectura de comunicaciones
 - f) Determinar los protocolos y las interfaces físicas soportadas por cada IED que será interconectado
 - g) Determinar los protocolos y las interfaces físicas mínimos que deben ser suministrados
 - h) Determinar si es más rentable proporcionar convertidores de protocolos y medios, o establecer redes dedicadas para cada combinación, o una combinación de alternativas.
- Estos pasos se relacionan entre sí. Por ejemplo, algunas topologías pueden ser soportadas por pocos medios de comunicación, o la topología puede restringir la elección de los protocolos de comunicación, o un sistema de comunicaciones basado en red puede requerir el uso de ciertos protocolos. Las siguientes secciones describen las consideraciones para realizar estos pasos y diferentes opciones que pueden utilizarse.

2.2 Requerimientos Funcionales

El requerimiento funcional básico de todo sistema de comunicaciones es soportar los distintos métodos de comunicación que puedan ser requeridos o necesarios. Si se especifica una nueva instalación, debe realizarse un estudio para determinar:

- a) Todas las fuentes y destinos de datos
- b) El enrutamiento previsto incluyendo rutas alternas, si es necesario
- c) El tiempo de entrega y refresco de todos los datos y mensajes de control

- d) El flujo esperado en el corto y largo plazo para condiciones normales y anormales del sistema eléctrico
- e) Los medios y tecnologías de comunicación adecuados
- f) Los requerimientos de aislamiento eléctrico y físico
- g) La estimación de costos preliminares
- h) Los requerimientos de continuidad del servicio
- i) La evaluación de requerimientos de privacidad, seguridad y control de acceso

Si el sistema de comunicaciones debe incorporar una parte de un sistema existente, tal como las interfaces de comunicaciones de instalaciones existentes, los requerimientos funcionales deben incluir descripciones detalladas de las condiciones existentes y definir la forma en que estas instalaciones serán integradas al sistema de comunicaciones.

2.2.1 Características de los Sistemas de Comunicaciones en Subestaciones

Las características típicas de los sistemas de comunicaciones en subestaciones eléctricas son las siguientes:

- Los datos operacionales tienen la máxima prioridad. Estos no deben ser degradados por los datos corporativos o no operacionales.
- Se desea un tiempo de respuesta típico del sistema a una solicitud del centro de control de dos segundos. El sistema SCADA puede reportar por excepción o por interrogación, esta última imponiendo mayores requerimientos de datos en la red. Algunos sistemas SCADA existentes, que fueron diseñados para uso con instalaciones dedicadas, requieren tiempos de respuesta de interrogación por debajo del segundo, creando mayores retos a propuestas de redes basadas en IP compartidas.
- Para el entorno de automatización de subestaciones, diez minutos es una buena estimación del requerimiento para la entrega automática de datos no operacionales, tales como archivos de eventos o registros de fallas, a un repositorio de datos para su inmediata revisión.
- Los tamaños típicos de archivos de eventos pueden variar de 300 KB a 1 MB por evento transitorio y de 2 a 5 MB por evento de mayor duración. El número de archivos es una función del número de registros de fallas generados por evento y el número de veces que ocurren al año.
- Algunas aplicaciones pueden recuperarse con un barrido lento continuo, con capacidad para recuperarlas "bajo demanda", si es necesario.

- Muchos de los datos generados por los registradores de falla estarán basados en disparadores (triggers) y, si el proceso es automático, puede generarse una cantidad adicional de datos para procesamiento, posiblemente innecesarios.

a) Tasa Efectiva de Transmisión de Datos

Es la cantidad de datos de usuario que puede ser transmitida en un período de tiempo. La cantidad real de datos (carga útil) que se puede enviar es una función del empaquetamiento "superior" de los datos con cabeceras, encriptación, etc., así como la congestión y el retardo que se experimenta a través del medio de transmisión. El ancho de banda disponible es una función de la capacidad del medio para soportar una determinada velocidad de transmisión de datos.

La tasa de transferencia de datos de la red LAN de la subestación debe ser lo suficientemente alta para satisfacer los requerimientos de desempeño del sistema de automatización en las peores condiciones, como cuando ocurren múltiples fallas de equipos en la subestación o en sus líneas de alimentación y alimentadores. Estos tipos de eventos pueden producir avalanchas de información analógica y alarmas, que pueden producir excesivo tráfico en la red.

Las simulaciones y pruebas referenciales han demostrado que las redes LAN Ethernet funcionando a 100 Mbps o 1 Gigabit, satisfacen los requerimientos de desempeño de grandes subestaciones (más de 100 IEDs), bajo condiciones de sobrecarga de red por desastre. Estudios similares para pequeñas subestaciones (menos de 100 IEDs) han demostrado que Ethernet de 10 Mbps, con medios compartidos, satisfacen los requerimientos de desempeño, ya que la actividad básica de carga de las comunicaciones es sólo el 5% de la capacidad de la red LAN.

Por un modesto incremento de costos, una empresa eléctrica debería implementar su red LAN con dispositivos Ethernet de 100 Mbps o 1 Gigabit. La mayor velocidad de la red LAN proporcionará un excelente desempeño y rendimiento para las funciones iniciales del sistema de automatización, y permitirá a la empresa eléctrica implementar futuras aplicaciones, sin actualizaciones de la red. Los dispositivos de red deben ser switches, ya que funcionan mejor que un hub compartido, soportan un mayor rendimiento y son una ruta de migración completa, cuando se añadan otras funciones de automatización.

b) Latencia

La latencia o retardo de red, es la cantidad de tiempo que tarda una unidad de datos para viajar de un punto a otro dentro de una red (retardo de extremo a extremo). Puesto que se desea un tiempo de respuesta del sistema a un centro de control de dos segundos,

cuanto menor sea la latencia, más dispositivos podrán comunicarse en esos dos segundos. Las mediciones típicas de latencia son tomadas por el tiempo de retardo de ida y vuelta de un paquete de datos entre dos destinos. Los contribuyentes a la latencia de red son:

- Los medios de transporte de fibra, cobre, inalámbricos u otros, con ciertas características físicas de transmisión.
- El tamaño de los paquetes de información, determinado por la cantidad de datos transmitidos y la carga del protocolo de comunicaciones. Cuanto mas grande sea el paquete, el tiempo de transmisión será mayor.
- Los componentes de la red de comunicaciones. Cualquier nodo o dispositivo final que forma parte de la ruta de transmisión, incluyendo routers, IEDs, RTUs, radios, etc. Cada equipo en la red que maneja un paquete de información requiere tiempo para examinar y posiblemente modificar el paquete. Ciertos protocolos de red también incluyen un medio para la retransmisión de datos recibidos incorrectamente, que se añaden al tiempo de tránsito total. También se puede necesitar tiempo para formular una respuesta, como es el caso cuando una RTU es interrogada por un sistema SCADA.

c) Disponibilidad de la Red

Además del requerimiento de latencia para soportar funciones críticas, tal como la operación del sistema de protección, otro parámetro principal de desempeño es la disponibilidad de la red, que normalmente está dada por el porcentaje de tiempo de funcionamiento normal de la red (por ejemplo 99.999%). El objetivo de tener una disponibilidad de la red sostenida, dependerá de la inversión realizada en la red para asegurar que esta se encuentre disponible cuando la necesiten los usuarios. Si una red no se encuentra disponible cuando un relé de protección lo requiera, puede producir pérdidas significativas de equipos, apagones, multas y mala publicidad. Normalmente, las empresas comparan las posibles pérdidas financieras con la inversión requerida para asegurar la disponibilidad de la red. Si las pérdidas son superiores, entonces la inversión es rentable. La tabla 2.1 muestra ejemplos de tiempos de inactividad permitidos, para diferentes disponibilidades de redes, basados en 24 horas del día, los 365 días del año.

Las interrupciones de energía pueden ocurrir una vez al año o todo el año. Con instalaciones arrendadas a un proveedor de servicios de telecomunicaciones, el tiempo de inactividad por mantenimiento e interrupciones, programados con la debida notificación, no entran en el cálculo de la disponibilidad de la red. Sin embargo, la

empresa eléctrica pierde el control de su red, cuando depende de estas instalaciones arrendadas.

TABLA 2.1 Disponibilidad de redes

Disponibilidad	Tiempo de inactividad permitido por año	Comentarios
99.999%	5.3 minutos	Cumple con el nivel más alto de configuraciones redundantes de equipos y diversidad de ruta
99.99%	53 minutos	Cumple con un nivel muy alto de configuraciones redundantes de equipos y diversidad de ruta
99.9%	8.8 horas	Cumple con un nivel alto de configuraciones redundantes de equipos y diversidad de ruta
99.5% o menos	44 horas o más	Cumple con un nivel moderado de equipos redundantes y configuraciones de rutas, pero con solo algunas "conexiones" en la red

La figura 2.1 muestra una red de alta disponibilidad para una subestación eléctrica, utilizando equipos y conexiones redundantes.

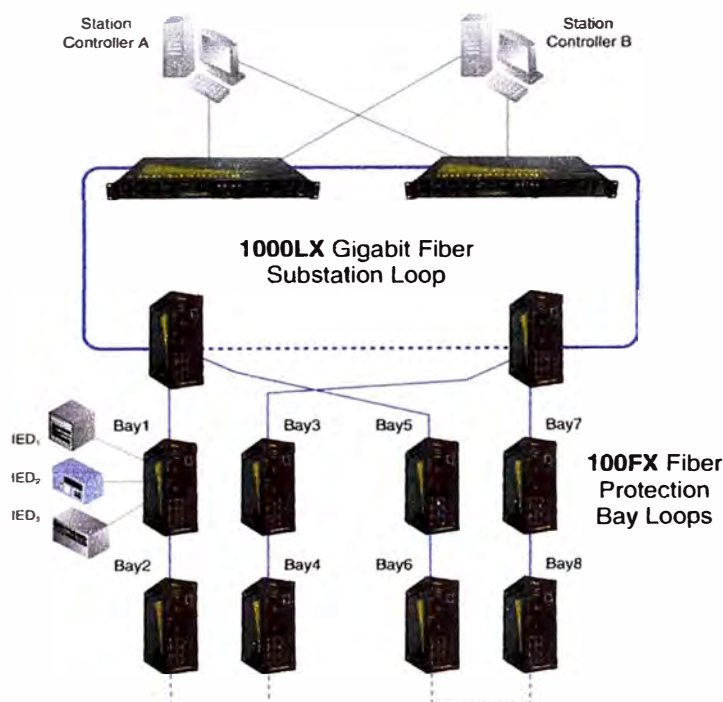


Fig. 2.1 Topología de red de alta disponibilidad

d) Gestión y Supervisión de Redes

Por lo general, las empresas eléctricas monitorean el estado de sus sistemas de comunicaciones a través de una variedad de técnicas de supervisión manejadas por los diversos componentes de comunicaciones a través de la red.

La cantidad y diversidad de componentes, así como el posible uso de elementos ópticos de banda ancha y otros en la red de transporte, requieren un sistema de gestión de red integrado (INMS) centralizado, que proporcione la calidad de servicio necesaria. La apertura, independencia de proveedores, escalabilidad y cumplimiento de estándares son requisitos fundamentales en la estrategia de instalación de la gestión de redes. La integración de sistemas de gestión de diferentes proveedores es posible, utilizando interfaces compatibles. Los componentes de hardware y software del sistema de gestión de red deben ser diseñados e integrados para asegurar la máxima disponibilidad posible de la red. Ejemplos de servicios soportados por el INMS son:

- Presentación gráfica de elementos de red físicos y lógicos
- Configuración de carga útil
- Gestión de puntos de acceso en la red
- Configuración de rutas: definición, asignación, implementación, prueba
- Supervisión de rutas: alarmas, desempeño.

Normalmente, las modernas plataformas del INMS utilizan servidores de alcance medio para las redes de tamaño medio/grande y PCs como terminales de operador, conectados a los servidores a través de la LAN. Las tareas que el operador puede realizar son:

- Establecimiento y supervisión de la conexión a los elementos de red
- Activación o desactivación de la supervisión de un elemento de red
- Carga y adaptación de datos de configuración física: parámetros del sistema, provisión de elementos de red, parámetros de operación, gestión de estado, etc.
- Parametrización de la configuración de transmisión
- Monitoreo en tiempo real de los elementos de red conectados: a través de alarmas de falla y notificaciones de eventos de operación normal. El operador puede visualizar las alarmas, filtrarlas, imprimirlas y registrarlas, así como habilitar/deshabilitar las alarmas secundarias.
- Mapeo de los servicios de gestión de cada uno de los elementos de la red
- Gestión de interconexión, con un conjunto de funciones para configurar y monitorear gráficamente las interconexiones en la red.

Debido a los diferentes proveedores de equipos de microondas, routers, bancos de canales y SONET en la red, un INMS basado en el protocolo SNMP (Protocolo Simple de Administración de Red) puede resultar más rentable.

2.2.2 Seguridad Informática

Las redes de computadoras han sido objeto de una variedad de ataques informáticos, debido a sus vulnerabilidades. A esto se le agregan las características de los sistemas de

automatización de subestaciones que dan pie a vulnerabilidades especiales, como por ejemplo RTUs o IEDs con procesadores lentos para las comunicaciones, sistemas operativos de IEDs que no incluyen políticas de seguridad, medios de comunicación inseguros, protocolos de comunicaciones abiertos, falta de autenticación, seguridad informática de baja prioridad, falta de un sistema centralizado de gestión y la gran cantidad de IEDs. Los caminos posibles de intrusiones informáticas a los equipos de una subestación son: dentro y fuera de la red corporativa.

Uno de los axiomas de la seguridad informática es que si bien es extremadamente importante tratar de evitar las intrusiones al sistema, es esencial que estas intrusiones sean detectadas cuando ocurren. [2]

La respuesta a las intrusiones debe ser el registro de todas las comunicaciones de datos de todos los dispositivos de las subestaciones, pero si estas no son detectadas ni registradas cuando ocurren, se deben desarrollar procedimientos para la restauración del servicio después del ataque informático.

Para poner estas recomendaciones en práctica, una empresa eléctrica debe establecer e implementar una política de seguridad informática y física (los activos de la empresa).

La aprobación de la Ley de Política Energética de los Estados Unidos, el año 2005, incluía una disposición para la creación de una Organización de Confiabilidad Eléctrica (ERO) sujeta a revisión y aprobación de la Comisión Federal Reguladora de Energía (FERC). La certificación ERO le fue concedida al Consejo Norteamericano de Confiabilidad Eléctrica (NERC), facultándolo para desarrollar normas de seguridad informática y otras normas de confiabilidad.

La misión del NERC es asegurar que el sistema eléctrico estadounidense sea confiable, adecuado y seguro. Funciona exitosamente como una organización voluntaria, basada en la reciprocidad, la presión del grupo y el interés mutuo de todos los involucrados. A través de este enfoque voluntario, ha contribuido en hacer del sistema eléctrico estadounidense el más confiable del mundo, y debido a su papel de líder desarrollando una norma de seguridad informática interna y permanente, viene influyendo en los demás países.

El propósito de las normas de seguridad informática del NERC es asegurar que todas las entidades responsables de la confiabilidad del sistema eléctrico estadounidense identifiquen y protejan los activos informáticos críticos que controlan o podrían afectar dicha confiabilidad. Fueron adoptadas permanentemente el 2006 y son obligatorias desde el 2007. Incluye ocho normas de Protección de Infraestructura Crítica (CIP) que tratan los siguientes tópicos [6]:

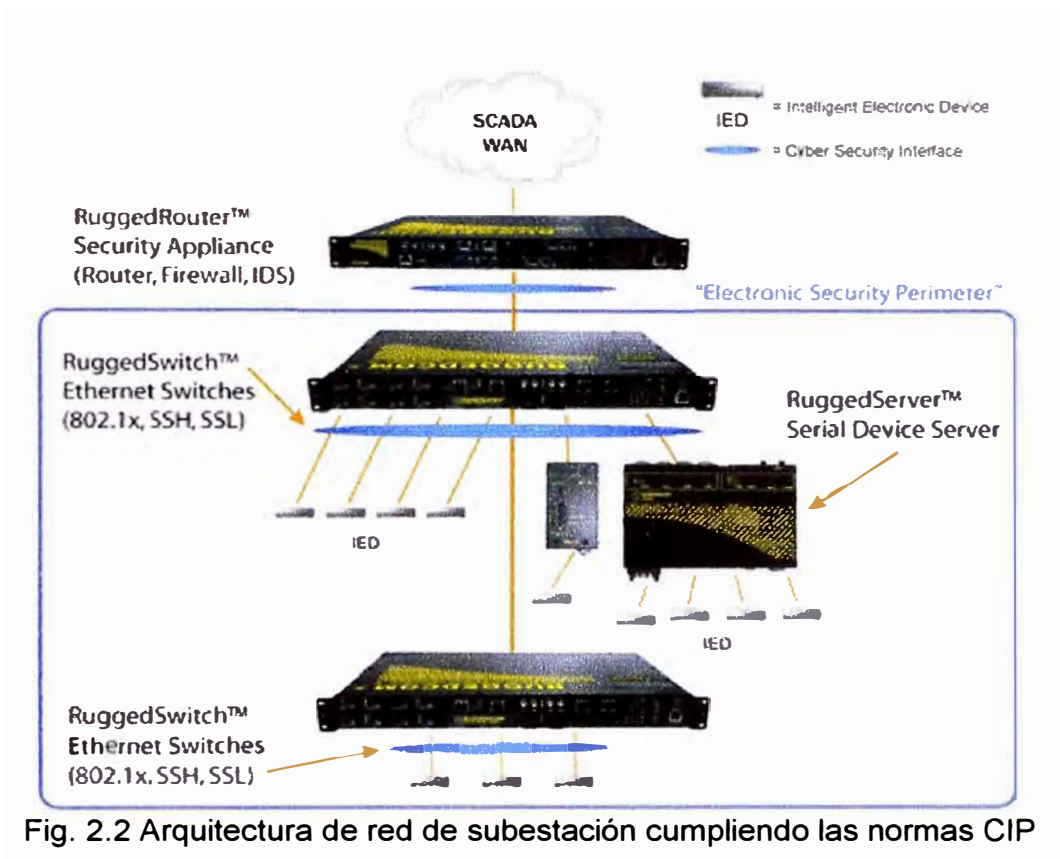
- CIP-002: Identificación de Activo Informático Crítico
- CIP-003: Controles de Gestión de Seguridad

- CIP-004: Personal y Formación
- CIP-005: Perímetros de Seguridad Electrónicos
- CIP-006: Seguridad Física de Activos Informáticos Críticos
- CIP-007: Dirección de Seguridad de Sistemas
- CIP-008: Información de Incidentes y Planificación de Respuestas
- CIP-009: Planes de Recuperación de Activos Informáticos Críticos

Estas normas son una base mínima sobre la cual se pueden y deben aplicar acciones de seguridad informática adicionales, como por ejemplo la capacitación constante y las reglas consistentes para la estructura y mantenimiento de contraseñas, aplicados a los activos que una empresa eléctrica considera críticos, tales como algunos circuitos de distribución. Algunas definiciones del NERC que se aplican a estas normas son:

- **Activos Críticos:** aquellas instalaciones, sistemas y equipos que, si se destruyeran, dañaran, degradaran o de alguna manera quedarán indisponibles, tendrían un impacto significativo en la capacidad de servicio a gran cantidad de clientes durante un periodo prolongado de tiempo, tendrían un impacto perjudicial sobre la confiabilidad y operatividad de la red eléctrica, o producirían un riesgo significativo a la salud y seguridad pública.
- **Activos Informáticos Críticos:** Aquellos activos informáticos esenciales para la operación confiable de los Activos Críticos.
- **Activos Informáticos:** Aquellos dispositivos electrónicos programables y redes de comunicaciones, incluyendo hardware, software y datos asociados con los activos del sistema eléctrico.
- **Incidente de Seguridad Informática:** Cualquier acto malicioso o evento sospechoso que:
 - Compromete, o intenta comprometer, el Perímetro de Seguridad Electrónica o Física de un Activo Informático Crítico, o,
 - Perturba o intenta perturbar la operación de un Activo Informático Crítico.
- **Perímetro de Seguridad Electrónica:** La frontera lógica en torno a la red o grupo de sub-redes (la "red de seguridad") a la cual se conectan los Activos Informáticos Críticos, y cuyo acceso es controlado.
- **Perímetro de Seguridad Física:** La frontera física en torno a las salas de computadoras, salas de telecomunicaciones, centros de operaciones, y otros lugares en los que se encuentran los Activos Informáticos Críticos y cuyo acceso es controlado.

La figura 2.2 muestra una arquitectura típica de red de subestación, cumpliendo las normas CIP.



2.3 Evaluación de Infraestructuras de Comunicación Existentes

El estado de la infraestructura de comunicaciones existente y su capacidad para soportar los requerimientos de datos de la arquitectura de automatización de subestaciones, deben evaluarse tomando en cuenta el tráfico, el tiempo de vida útil de los equipos, los parámetros de desempeño y la capacidad para soportar incorporaciones. Las actividades a realizar son:

1. Evaluación de la antigüedad: Esta es una evaluación cualitativa que resume la antigüedad, condición, uso y utilización de la red, en el entorno de la empresa eléctrica. La evaluación tratará de predecir el tiempo de vida útil restante y la capacidad de la red.
2. Análisis de la congestión: Se trata de un análisis cuantitativo identificando los lugares dentro de la red donde el uso del ancho de banda supera el nivel deseable, o donde podría originarse latencia.
3. Análisis de puntos únicos de falla: Este análisis identifica los lugares dentro de la red que no tienen redundancia, y que tienen un notable impacto negativo en usuarios y procesos críticos, si fallaran.
4. Proyección de la carga de trabajo: Se trata de una proyección de la carga futura de la red en una visión a 5 años. Estimaré el número de circuitos o paquetes que serán

impuestos en la red. El propósito es dimensionar la capacidad a la que una nueva red debería inicialmente ser construida o a la que una red existente debería ser extendida.

5. Evaluación de la tecnología: Para una nueva red o aplicación, se trata de una evaluación cualitativa de la conveniencia y viabilidad de empleo de tecnología dentro de la empresa eléctrica. Para una red o aplicación existente, se trata de una evaluación cualitativa de la capacidad de la tecnología para realizar el trabajo al que está destinada.

6. Evaluación de la plataforma: Se trata de una evaluación y proyección cualitativa de la capacidad de la(s) plataforma(s) de red, para seguir realizando el trabajo al que está(n) destinado(s), en una visión a 5 años.

7. Evaluación Futura: Se trata de una evaluación cualitativa de la capacidad prevista de la red para crecer, adaptarse, ser actualizada, migrada y soportada por el fabricante, con el fin de servir al propósito al que está destinada en una visión a 5 años de la arquitectura. La esperanza de vida también debería evaluarse y debería hacerse toda recomendación para eliminar una red existente, debido a su incapacidad para servir al propósito deseado.

8. Disponibilidad del espectro: se trata de una evaluación de las frecuencias disponibles, bandas de frecuencia, y posibles interferencias, para la consideración del uso de infraestructura inalámbrica para complementar, reemplazar o actualizar infraestructuras de comunicaciones existentes.

2.3.1 Redes Privadas y Redes Arrendadas

Uno de los objetivos de una empresa eléctrica debería ser utilizar redes privadas. Las ventajas de implementar estas redes son:

- Presupuesto de inversión (CAPEX) en lugar de presupuesto de operación (OPEX)
- Permite Ethernet nativa de próxima generación desde su implementación inicial
- Red bajo control de la empresa. Las adiciones y cambios se manejan fácilmente
- La supervisión del desempeño de la red es inherente. Las llamadas de asistencia técnica y tiempos de reparación se reducen porque no se tiene que esperar a los proveedores
- Ningún problema de instalación de circuitos adicionales

Las desventajas de las redes arrendadas son:

- Los costos presupuestarios no asumen problemas de instalaciones; la disponibilidad de la instalación suele verificarse una vez que se coloca una orden por un circuito. Las instalaciones adicionales o actualizaciones tendrán impacto en los costos del circuito.
- Las instalaciones adicionales dependen de los proveedores.

- El usuario del sistema necesita la presencia del proveedor en sitio, para asistencia técnica.

Las empresas eléctricas tradicionalmente utilizan proveedores de servicio de telecomunicaciones (carriers) para la conectividad entre sus centros de control y subestaciones remotas separadas geográficamente. Los servicios van desde líneas arrendadas directas hasta servicios de red como Frame Relay. Frame Relay es un servicio de datos basado en paquetes que puede enrutar protocolos TCP/IP o de sistema SCADA y es un medio eficaz de transporte de datos desde lugares fijos. La ventaja de Frame Relay es que puede establecer conexiones con varios centros de control, permitiendo un rápido re-enrutamiento de subestaciones a un centro de control alternativo, en caso de que el centro de control principal se deshabilitara. También puede ser utilizado como una ruta de respaldo a una ruta principal, por ejemplo de microondas. Tiene la capacidad de establecer Circuitos Virtuales Permanentes (PVCs) con una tasa de información comprometida (CIR). Esto proporciona un mecanismo para priorizar los datos críticos por PVC a través de una interfaz de usuario a red (UNI). Sin embargo, dado que la nube de Frame Relay es controlada por el carrier, la red es compartida por otros usuarios, y está sujeta a re-enrutamientos de gestión de red, que pueden cambiar la latencia y la transferencia bajo demanda. Los Acuerdos de Nivel de Servicio (SLAs), firmados con el carrier ayudarán a aliviar algunos problemas de servicio, sin embargo, normalmente el único recurso es conseguir créditos de servicio para el momento en que el desempeño está por debajo del nivel acordado. Estos créditos son pequeños en comparación con el posible daño que podría ocurrir si no se produce una acción de control por problemas de red.

Las empresas eléctricas utilizan la tecnología Frame Relay sobre instalaciones digitales arrendadas. Esto proporciona conectividad flexible y gestión de desempeño, basados en la CIR, que son fortalezas de la tecnología Frame Relay, pero aíslan a las empresas de utilizar una red compartida en modo paquete.

Si bien los servicios de Frame Relay tienen más de 15 años de madurez en la industria, los carriers están presentando nuevos servicios IP privados de red WAN, basados en MPLS (conmutación de etiquetas multiprotocolo), y están posicionándolo para finalmente sustituir los servicios de Frame Relay.

El Acuerdo de Nivel de Servicio, es un acuerdo formal escrito entre dos partes, el proveedor y el receptor del servicio. Define la base de entendimiento entre estas dos partes para la prestación del servicio. Es utilizado por proveedores y clientes, así como internamente por la TI y sus usuarios finales, para especificar la disponibilidad de ancho

de banda, los tiempos de respuesta para los servicios y consultas ad hoc, el tiempo de respuesta para la resolución de problemas, así como las actitudes y consideraciones del personal técnico. Con el fin de hacer cumplir estos acuerdos, todas las principales interacciones deben monitorearse y ser calculadas para asegurar que el desempeño de los sistemas cumpla con los objetivos empresariales.

2.3.2 Comunicaciones Telefónicas

El cambio de una importante infraestructura de comunicaciones toma años. Un ejemplo es la migración de una arquitectura de central privada de voz (PBX) con multiplexación por división de tiempo (TDM) a Voz sobre IP (VoIP). Si bien VoIP es la infraestructura del futuro, el cambio de una infraestructura existente que está trabajando es lento, a menos que haya una necesidad importante para el cambio, tal como fallas del sistema, pérdida de ingresos, etc. Del mismo modo, el cambio de las líneas dial-up a IP va por buen camino, pero tomará algunos años. Se prevé que dial-up será requerida en algún nivel en la infraestructura de comunicaciones de la empresa eléctrica, al menos por los próximos 5 años. Dial-up puede ser utilizada como un respaldo a una conexión IP en algunos lugares.

Para las líneas dial-up, la seguridad y el cumplimiento de normas (como por ejemplo NERC), debe ser considerada de manera similar a otros aspectos de una red de comunicaciones de una empresa eléctrica. Existen dispositivos de red que proporcionan acceso y control de líneas dial-up, y soportan funciones de seguridad. Un ejemplo de ello son los transceptores de encriptación serial, que protegen estos enlaces utilizando autenticación y encriptación.

2.3.3 Comunicaciones de Red IP

La principal tendencia de las empresas eléctricas que implementan la automatización de subestaciones, es la migración a redes basadas en IP, para el enrutamiento de la red WAN, y Ethernet dentro de la subestación. Como se indicó anteriormente, la actual implementación de IP es IPv4, con posibles migraciones futuras a IPv6. El uso de una red proporciona eficiencias de ancho de banda y servicios compartidos, a expensas de posibles problemas de latencia y seguridad. Ethernet y las comunicaciones IP pueden ser realizadas por varias funciones, diseñadas para superar estas posibles vulnerabilidades, como las redes LAN virtuales (VLANs) y el mecanismo de transporte MPLS. Para seguridad, la aplicación de IPSec proporciona un túnel seguro de extremo a extremo a través de redes no confiables. Las características de estas funciones, se mencionan a continuación.

a) Características Principales

VLAN

El switch de capa 2 previsto para la red LAN de la subestación, es capaz de agrupar subconjuntos de puertos en dominios de broadcast virtuales aislados entre sí, conocidos como redes LAN virtuales (VLANs). Las VLANs también pueden extenderse para construir una Red Privada Virtual (VPN) a través de la red WAN.

Las VLANs se pueden utilizar para establecer comunicaciones seguras en instalaciones compartidas. Algunas empresas eléctricas la utilizan para separar la información de TI corporativa y la información de gestión de datos de la subestación. Se trata además de utilizar todas las herramientas de seguridad probadas, disponibles en los dispositivos IP, desde la configuración básica de contraseñas del sistema, uso de filtros de permiso IP y banners de registro de inicio de sesión (login), hasta herramientas más avanzadas, como RADIUS, TACACS+, Kerberos, SSH, SNMPv3, IDS.

El concepto de VLAN es similar a otros conceptos de redes, donde el tráfico es identificado por el uso de una etiqueta (ID). La identificación es fundamental para el switch de capa 2 para poder aislar los puertos y reenviar correctamente el tráfico recibido. Si todo paquete en el dispositivo está asociado a una etiqueta VLAN adecuada, siempre es posible discriminar el tráfico, de manera confiable, en dominios separados e independientes.

El límite de número de etiquetas bajo el estándar IEEE 802.1q es de 4,904. Algunos proveedores ofrecen implementaciones de VLAN apiladas, pero estas son propietarias, renunciando a los beneficios de interoperabilidad entre proveedores, que ofrecen las implementaciones basadas en estándares. [2]

MPLS

En su forma más básica, MPLS es un protocolo basado en IP que utiliza etiquetas internas para enrutar los paquetes que pertenecen a diferentes VPNs a través de la red. Las etiquetas son cabeceras de longitud fija, de 32 bits en la mayoría de casos, que indican la VPN del paquete y la ruta a ser tomada a través de la red MPLS. Pero la etiqueta también puede ser utilizada para indicar el tipo de servicio (Calidad de Servicio QoS o Clase de Servicio CoS) y las rutas de respaldo a ser tomadas en caso de fallas de enlace o nodo. Los motivos para utilizar etiquetas son diferentes, de modo que llamando simplemente a una red MPLS no se indica exactamente que prestaciones de MPLS están incorporadas en dicha red. En general, cuantas más características de una red MPLS se deseen, más complicada será la configuración y administración de la red.

Un router MPLS trabaja mirando un paquete de un router de borde (edge router) conectado. Una vez que lo recibe, el router determina si este paquete pertenece a una ruta existente en la red MPLS. Si es así, añade la etiqueta adecuada al paquete (y la cabecera Ethernet necesaria para la transmisión a través de la red Ethernet SONET utilizada). Si el paquete del router de origen requiere una nueva ruta a través de la red MPLS, el router MPLS establece la ruta y la notifica (junto a su etiqueta asociada) a los routers de red adecuados y estos establecen la tabla de envío adecuada para la nueva etiqueta. El papel de los routers de la red se reduce luego a recibir el paquete de los otros routers, anotar la etiqueta y, a continuación, seguir las instrucciones de sus tablas de enrutamiento. En el router de red final, se extrae la etiqueta y el paquete es enviado, a través del puerto adecuado, a la red LAN de recepción.

MPLS permite garantizar la entrega de los niveles de servicio necesarios, bajo la modalidad end-to-end, dentro de la red MPLS.

La garantía de estos altos niveles de desempeño requiere alguna forma de ingeniería de tráfico, que reserve los recursos necesarios dentro de la red, para cumplir los requerimientos de Calidad de Servicio del tráfico de mayor prioridad. Existen varios protocolos que se pueden utilizar. La mayoría de ellos involucra el establecimiento de túneles que son rutas completas a través de la red desde la entrada hasta la salida. Si los requerimientos de latencia en el tráfico de mayor prioridad lo permiten, se puede realizar la reorganización de la red por cambios de condiciones por nodo, utilizando la toma de decisiones descentralizada. Sin embargo, este enfoque puede no satisfacer los requerimientos necesarios de latencia/jitter y la capacidad de Fast Reroute (FRR). FRR requiere que los túneles sean establecidos para la ruta principal a través de la red, y que cada nodo tenga una ruta alternativa en caso de falla de uno de sus vecinos.

Calidad de Servicio en Redes IP

Los datos SCADA en tiempo real, así como los circuitos de voz y video deben ser entregados del origen al destino en secuencia y sin retardo, de lo contrario, los datos se pierden o retrasan, y la aplicación se vuelve inutilizable. Si en la infraestructura de comunicaciones se utiliza SCADA sobre IP, debe existir un medio para asegurar que pueda ser entregado en el tiempo necesario. En una red IP, cuando los datos atraviesan los routers y switches, puede generarse una congestión en la red ya que distintos servicios compiten por el ancho de banda limitado, y debe implementarse un medio que garantice que los datos en tiempo real tengan prioridad sobre los datos no críticos. Para redes IP, este es el parámetro Calidad de Servicio (QoS).

Calidad de Servicio, en los campos de redes de conmutación por paquetes y redes de computadoras, se refiere a los mecanismos de control que pueden proporcionar diferente calidad de servicio o prioridades a diferentes usuarios o flujos de datos. Estos mecanismos pueden consistir en acordar contratos de tráfico durante una fase de establecimiento de sesión, reservar capacidad en los nodos de red, controlar las prioridades de programación en los nodos de la red, y liberar la capacidad reservada durante una fase de borrado. Esto es importante por ejemplo en servicios streaming multimedia en tiempo real, por ejemplo Telefonía IP o Televisión sobre IP, que requieren una tasa de bits fija y pueden ser sensibles a retardos. Lo contrario al concepto de Calidad de Servicio es proporcionar comunicación de mejor esfuerzo (best effort) a todos los flujos de datos.

Desde el punto de vista del emisor y receptor, los paquetes están expuestos a muchos problemas:

- Paquetes rechazados: los routers pueden rechazar algunos paquetes que llegan cuando sus memorias buffer están llenas.
- Retardo: un paquete podría tardar mucho tiempo en llegar a destino, porque se retrasó en largas colas, o tomó una ruta menos directa para evitar la congestión.
- Jitter: los paquetes del origen llegarán al destino con diferentes retardos. Esta variación en el retardo se conoce como jitter y puede afectar seriamente a la calidad de streaming de audio y/o video.
- Entrega fuera de orden: cuando una colección de paquetes relacionados son enrutados a través de Internet, distintos paquetes pueden tomar rutas diferentes, produciendo cada una de ellas un retardo diferente. El resultado es que los paquetes llegan en un orden diferente al que fueron enviados. Este problema requiere protocolos adicionales especiales, responsables de reordenar los paquetes fuera de orden a un estado isocrónico, una vez que ellos llegan a su destino. Esto es especialmente importante para flujos de video y VoIP, donde la calidad es afectada dramáticamente por la latencia o falta de isocronicidad.
- Error: a veces los paquetes son mal dirigidos, o combinados, o corrompidos, mientras se enrutan. El receptor tiene que detectar esto y, solo si el paquete fue rechazado, pedir al emisor que lo repita.

Para determinados tipos de tráfico de red se puede necesitar una Calidad de Servicio definida, por ejemplo:

- Streaming multimedia puede requerir rendimiento garantizado
- Telefonía IP o VoIP puede requerir límites estrictos de jitter y retardo
- Video Teleconferencia (VTC) requiere bajo jitter

- Señalización de alarma (por ejemplo, alarmas del sistema SCADA)
- Emulación de enlace dedicado requiere rendimiento garantizado e impone límites máximos de retardo y jitter

protocolo y la latencia de red, mejorando el desempeño crítico de protocolos SCADA seriales.

Uso de Entunelamiento Seguro IPSEC

IPSec permite túneles seguros a través de redes no confiables, soportando VPNs de red a red o red a host. Permite la criptografía con clave precompartida o pública, con protocolos de encriptación DES, 3DES, AES típicamente soportados.

b) Aplicaciones Futuras Habilitadas por IP

Se ha indicado que la tendencia que se nota en varias empresas eléctricas, es a la implementación de redes IP. Los proveedores también están ayudando a esto ofreciendo productos con puertos Ethernet. Se prevé que la mayoría de aplicaciones inteligentes futuras estarán basadas en IP, y la migración de la empresa eléctrica a plataformas de comunicación IP y Ethernet será consecuente con las tendencias de la industria.

Otra de las ventajas de IP para el sistema SCADA es la capacidad de reenrutar el tráfico SCADA a un centro de control de respaldo, si es necesario. Los concentradores de datos y procesadores de comunicaciones, tienen la capacidad para incluir destinos principales y secundarios de enrutamiento de tráfico, por lo que cuando un centro de control principal no se encuentra disponible, el tráfico puede enrutarse automáticamente al centro de control de respaldo.

c) Comunicaciones Seriales y Basadas en Red

Las comunicaciones de transporte pueden establecerse como circuitos punto a punto o basados en red. Las características de estos métodos se resumen en la Tabla 2.2.

TABLA 2.2 Comparación de Circuitos Basados en Red y Circuitos Punto a Punto

Circuito Basado en Red	Circuito Punto a Punto
<ul style="list-style-type: none"> - Permite reconfiguración flexible - Posible latencia de red - Uso eficiente de la capacidad de la red - Capacidad "Plug & Play" - Consideraciones de seguridad (por ejemplo, NERC CIP) - Tendencia de proveedores a interfaces IP - Permite rápido reenrutamiento para recuperación de desastres y respaldo al centro de control 	<ul style="list-style-type: none"> - Normalmente, interfaz serial y circuito dedicado - Mínima carga de protocolo - Circuitos arreglados para entrega de datos - Red más sencilla y menos requerimientos de operación y mantenimiento - Circuitos IP punto a punto siguen considerando protocolo enrutable si existe acceso a IEDs - Puede no ser tan rentable como la red enrutada de datos

Los circuitos punto a punto tienen muy baja latencia (del orden de los milisegundos), ya que una vez configurados, no requieren procesamiento significativo para mantener la conexión. La carga necesaria de protocolos de comunicaciones, que se agrega como carga de transporte es mínima (por lo general menos de 10% adicional a la carga útil de datos). En esencia, al circuito se le "fija" una configuración estática hasta que sea retirada físicamente. La desventaja de la baja latencia es la capacidad que debe dedicarse a la conexión, que en esencia, incrementa los requerimientos de ancho de banda y los costos de la red para suministrarla. Los requerimientos de entrega de datos operacionales desde la fuente al EMS pueden variar de 2 segundos para ciertos datos (como los datos de Control de Generación Automática), a 5 a 10 segundos para todos los demás datos. Los circuitos punto a punto garantizan que se cumpla este requerimiento de entrega.

Los circuitos basados en red utilizan routers a través de la red que, en realidad, realizan una función de enrutamiento de almacenamiento y reenvío (store and forward). Esto requiere una mayor cantidad de procesamiento y carga de protocolo de comunicaciones para un paquete de datos al pasar de un puerto de entrada a un puerto de salida en el router. Para que se realice una operación basada en conexión a red de manera eficiente, el tráfico esperado a través de la red debe ser cuidadosamente pronosticado para las cargas pico, a fin de garantizar que los procesadores del router y anchos de banda del circuito puedan acoplarse para acomodar la carga. De lo contrario, los paquetes serán rechazados, originando solicitudes de retransmisión que se agregan al tráfico de la red y congestión de enlace totales. En una red bien diseñada y planificada, una regla general para la latencia a través de un router es del orden de 10 a 20 ms. Sin embargo, esta cifra puede degradarse rápidamente, si se produce la congestión a través de un router y los paquetes se colocan en cola hasta que sean procesados y enrutados al puerto correcto del router. Con la implementación de las redes VLAN y MPLS, los circuitos operacionales críticos pueden priorizarse y garantizarse el ancho de banda necesario para mantener el nivel de desempeño requerido. En una red de recursos limitados esta Calidad de Servicio es proporcionada a expensas de los circuitos no operacionales de menor prioridad, afectando posiblemente el objetivo de entrega de los datos no operacionales. El escenario de limitación de recursos sólo se produciría cuando el tráfico supera los criterios de diseño de la red. Un ejemplo de esto es si se produjera un evento climatológico importante, que origina una participación mayor de las subestaciones que el escenario "más probable" diseñado: por ejemplo 10% de todas las subestaciones participan en el reporte de alarmas y cambios de estado, sobre una red diseñada para un máximo de 5% de participación.

La conexión IP basada en red puede proporcionar una conectividad de comunicaciones rentable a través de la red de transporte, en términos de ahorros de instalación y simplicidad de operación una vez establecida. Con una red bien planificada y diseñada para soportar el tráfico de comunicaciones, la latencia de extremo a extremo a través de la red para los datos no operacionales debe estar dentro de parámetros aceptables.

2.4 Comunicaciones Dentro de la Subestación Eléctrica

2.4.1 Requerimientos Ambientales de los Equipos del Sistema

Todos los componentes críticos del sistema de automatización deben estar diseñados para funcionar de manera correcta y confiable en entornos de subestaciones eléctricas. Los IEDs relés de protección y PLCs no tienen problemas en este aspecto, pero los componentes diseñados para operar principalmente en un entorno de oficina, tales como las computadoras personales, utilizadas como interfaz de usuario local, los switches, routers, etc., pueden ser fuentes de posibles fallas.

Los equipos del sistema de automatización, utilizados para la red LAN de la subestación o para interactuar con el sistema SCADA/EMS, como mínimo deben cumplir las normas IEEE 1613 o IEC61850-3, que definen las condiciones de servicio, rangos eléctricos, rangos térmicos y requerimientos de pruebas ambientales para dispositivos de redes de comunicaciones a ser instalados en subestaciones eléctricas.

La mayoría de empresas eléctricas utilizan computadoras estándares para la Interfaz Gráfica de Usuario (HMI) local. Sin embargo, si la HMI local es el único dispositivo desde el cual se realizan acciones de control local dentro de la subestación, la computadora de esta HMI también debe ser un dispositivo para el entorno de subestaciones.

Existen versiones robustas de los componentes del sistema de automatización, de fabricantes especializados, diseñados para soportar temperatura y humedad extremas, así como entornos eléctricos hostiles de subestaciones eléctricas. Varios fabricantes ofrecen productos de red diseñados específicamente para satisfacer las mismas exigencias ambientales y de inmunidad a interferencias electromagnéticas (EMI), que los relés de protección. Los sistemas de calidad industrial también pueden incluir teclados y ratones sellados con protección NEMA 4X. Las computadoras robustas están diseñadas para soportar una entrada de alimentación de rango amplio y sobretensiones, operando en condiciones extremas de temperatura y humedad. Algunas computadoras robustas también satisfacen las normas militares para golpes y vibraciones MILSPEC 810c y MILSPEC 810e.

Los equipos Ethernet para la subestación deben ser tan robustos como los IEDs que se conectan a ellos. La red LAN de la subestación será parte integrante de un sistema de protección y control de misión crítica que se debe desempeñar confiablemente en tiempo real cuando se produzca una condición de falla. Con el fin de garantizar un desempeño confiable, los switches Ethernet deben tener las siguientes características:

- Medios de comunicación de fibra óptica para conectividad y seguridad inmunes
- Amplio rango de temperatura de operación (-40 a 85 °C)
- Cumplimiento de las normas de ensayo IEC 61850-3 o IEEE 1613

2.4.2 Cableado de Campo

Con la amplia implementación de IEDs en subestaciones eléctricas y la tendencia creciente hacia la obtención de datos SCADA en tiempo real de estos, se ha reducido la cantidad de puntos de entrada y salida directamente cableados (o en algunos casos a través de transductores). Sin embargo, el sistema de automatización debe incluir un mecanismo para la adquisición de datos y control de aparatos eléctricos no equipados con IEDs, tales como seccionadores motorizados, bancos de capacitores y servicios auxiliares (detectores de humo, alarmas de intrusión, etc.).

Los IEDs o RTUs reciben entradas analógicas de transformadores de corriente (CTs), transformadores de tensión (PTs) y transductores, en los diferentes paneles de la subestación, así como entradas digitales de contactos auxiliares y transductores, de otros dispositivos o IEDs o de la estación maestra SCADA, a través de tarjetas de entradas analógicas y de estados disponibles para el cableado de estas señales. Ellos pueden desarrollar cálculos lógicos y matemáticos complejos y proporcionar una salida a la estación maestra SCADA, a otro instrumento de campo o IED, o retornar a los paneles de la subestación, para desarrollar algún comando, por ejemplo abrir un interruptor de potencia.

Si bien para el manejo de entradas y salidas digitales directamente cableadas, tradicionalmente se han utilizado RTUs, en la actualidad muchos proveedores de sistemas de automatización distribuidos, basados en redes LAN, optan por PLCs más económicos. Las limitaciones anteriores de los PLCs, tales como la incapacidad para soportar etiquetado de tiempo de SOE y dificultades en la sincronización con una unidad de referencia de tiempo, han sido resueltas por productos de terceros.

Muchas empresas eléctricas también utilizan las interfaces de entrada/salida de los IEDs para la recolección de estas señales. Si se tiene un IED protegiendo a un interruptor de potencia, es probable que el IED necesite conocer el estado del interruptor. Este estado se puede obtener a través de una conexión cableada al IED.

2.4.3 Topologías de Comunicaciones

Los sistemas de automatización de subestaciones basados en IEDs comparten información y funcionalidad en virtud de su capacidad de comunicaciones. Las interconexiones de comunicaciones pueden utilizar cables de cobre, fibra óptica, inalámbrico, o una combinación de estos, y pueden variar en complejidad, dependiendo de los objetivos finales del sistema. Las diferentes topologías de esta red interna se explican a continuación.

a) Redes cableadas

Redes Punto a Punto

El enlace de comunicaciones de un IED al sistema de automatización puede ser una simple conexión punto a punto, donde el IED se conecta directamente a un controlador de subestaciones. Muchos IEDs pueden conectarse punto a punto a un controlador o concentrador con múltiples puertos, que hace de nodo central de las comunicaciones del sistema de automatización. En las primeras integraciones, estas conexiones eran simples canales seriales EIA-RS-232, similares al que interconectaba una computadora con un módem. La figura 2.3 muestra una conexión punto a punto EIA-RS-232.

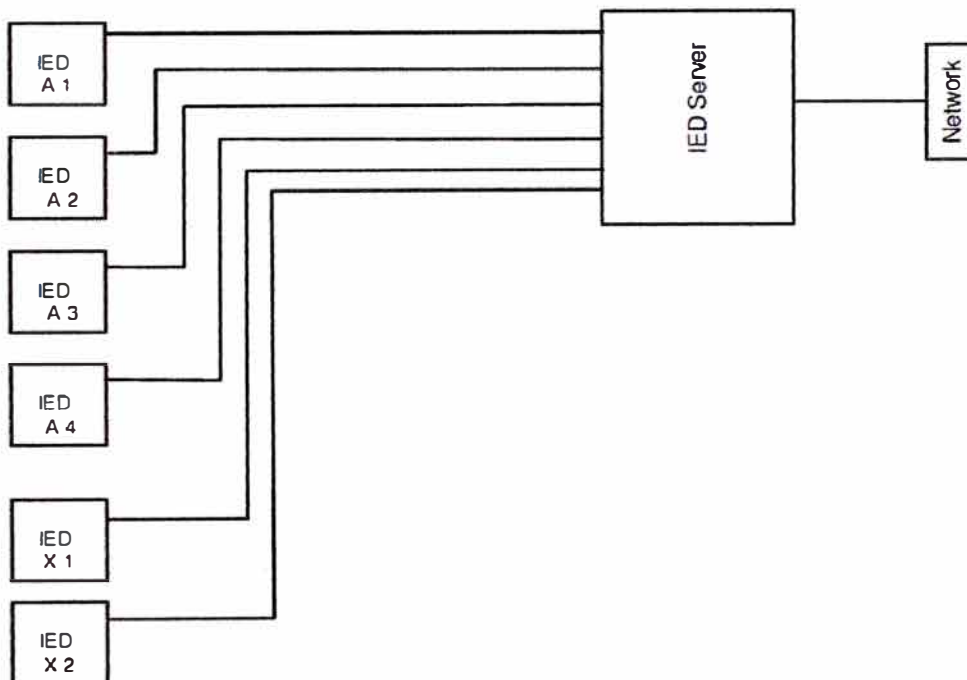


Fig. 2.3 Conexiones punto a punto entre IEDs y Servidor

EIA-RS-232 no soporta múltiples dispositivos en un canal. Este tipo de conexión lo utilizan algunos IEDs, que no se pueden comunicar a través de una línea compartida, ya

que no manejan protocolos que soportan direccionamiento. El medio es de cobre y suele ser utilizado en distancias cortas de hasta 15m (50 pies). La mayoría de conexiones EIA-RS-232 son directas de dispositivo a dispositivo y para su aislamiento requieren hardware especial. A menudo, las empresas eléctricas utilizan enlaces punto a punto de fibra óptica, que se conectan a puertos RS-232 utilizando módems, para asegurar el aislamiento y permitir un incremento de las distancias entre dispositivos. [5]

Redes Multipunto

La mayoría de sistemas de automatización de subestaciones emplean conexiones punto a multipunto a los IEDs. Los IEDs que comparten un protocolo común, generalmente soportan un canal de comunicaciones de línea compartida. Un controlador de subestaciones puede utilizar este canal como un bus de comunicaciones maestro-esclavo para controlar el tráfico en el canal. Todos los dispositivos de un bus común deben ser direccionables y el dispositivo maestro debe garantizar que solo un dispositivo se comunique a la vez, para evitar colisiones de comunicaciones. Estos dispositivos se deben configurar a una velocidad común. Los canales de línea compartida pueden también configurarse para soportar múltiples maestros utilizando un mensaje de paso de control de un dispositivo a otro, dando al dispositivo receptor autoridad para tomar el control del canal como un "maestro". [5]

El bus punto a multipunto más común es el EIA-RS-485. Es un par de cobre trenzado apantallado, terminado en cada extremo del bus por una resistencia terminal igual a la impedancia característica del cable del bus. La figura 2.4 muestra un bus de comunicaciones EIA-RS-485.

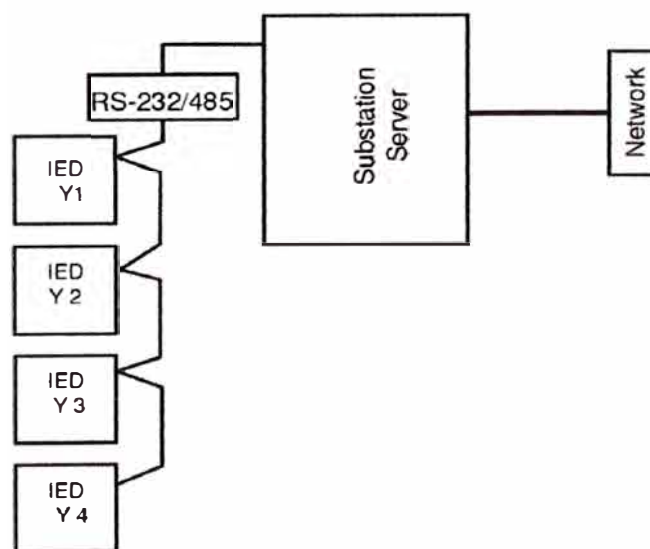


Fig. 2.4 Bus de Comunicaciones EIA-RS-485

Los buses EIA-RS-485 soportan hasta 32 dispositivos en el canal. La máxima longitud del canal es de 1200m. Cuanto más largo es el bus, es más probable que ocurran errores de comunicaciones debido a reflexiones en la línea y su velocidad de transferencia de datos es más lenta. EIA- RS-485 puede correr a 1.0 Mbps, aunque la mayoría la opera a 19.2 kpbs o menor. RS-422 es similar a EIA-RS-232 (no direccionable y de configuración punto a punto) excepto que es de dos pares: uno para emisión y otro para recepción. RS-422 tiene como objetivo permitir distancias de hasta 1200m en lugar del estándar EIA-RS-232 que llega hasta 15m.

En esta topología, muchos dispositivos se conectan sobre el mismo medio de comunicación. Esta comunicación soporta solo un intercambio de datos a la vez y se requiere algún protocolo que permita que un dispositivo a la vez utilice el medio de comunicación. En una configuración multi-drop, un maestro IED interroga a un IED a la vez y espera respuesta antes de interrogar al siguiente dispositivo. Transmite un mensaje que es recibido por todos los dispositivos conectados al medio. La información de direccionamiento en el mensaje indica el dispositivo de destino.

Topología en Estrella

En una topología en estrella, cada IED se conecta a un nodo central denominado hub. El hub puede ser pasivo, proporcionando una ruta para que pase el mensaje, o activo, regenerando la señal eléctrica. Los hubs ahora son más inteligentes y capaces de enrutar el mensaje al puerto al que está conectado el IED de destino. [5]

La figura 2.5 muestra la topología en estrella.

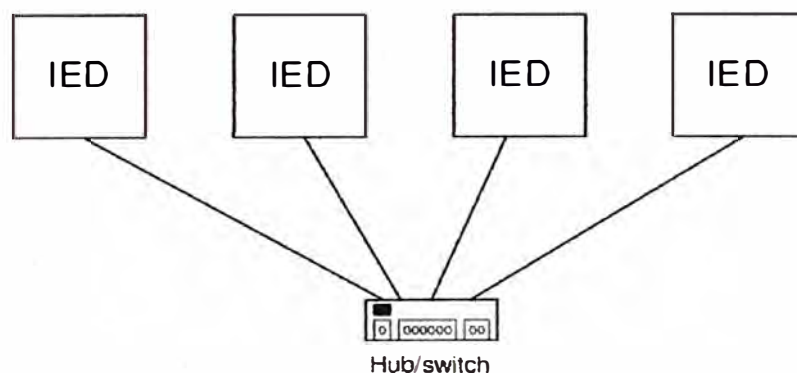


Fig. 2.5 Topología en Estrella

En la tecnología Ethernet, el intercambio de datos sobre cada segmento es aislado y utilizan fibras ópticas o cables de par trenzado diferentes, para los datos transmitidos y recibidos, evitando colisiones.

Un switch LAN es similar a un hub, con la diferencia de que el switch filtra mensajes dejando pasar sólo los mensajes al IED adecuado, los mensajes a otros IEDs son bloqueados. Esto crea una situación en la que cada IED parece estar sobre una única LAN "virtual", de modo que los problemas de colisión y contención se reducen al mínimo o se eliminan.

Redes Peer-to-Peer

Existe una tendencia creciente en las comunicaciones de IEDs para soportar mensajería peer-to-peer, en la que cada dispositivo tiene igual acceso al bus de comunicaciones y puede enviar mensajes a cualquier otro dispositivo. Esto es sustancialmente diferente a un entorno maestro-esclavo. Una red peer-to-peer debe proporcionar un medio para evitar las colisiones de mensajes, o para detectarlas y atenuarlas. [5]

Una forma de compartir un bus común como pares es utilizando un esquema CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones), tal como Ethernet. Si bien Ethernet puede ser una red de dispositivo a dispositivo de conexión en cadena (daisy chain), es más común conectar los dispositivos a un hub o switch. La figura 2.6 muestra dispositivos conectados a un hub.

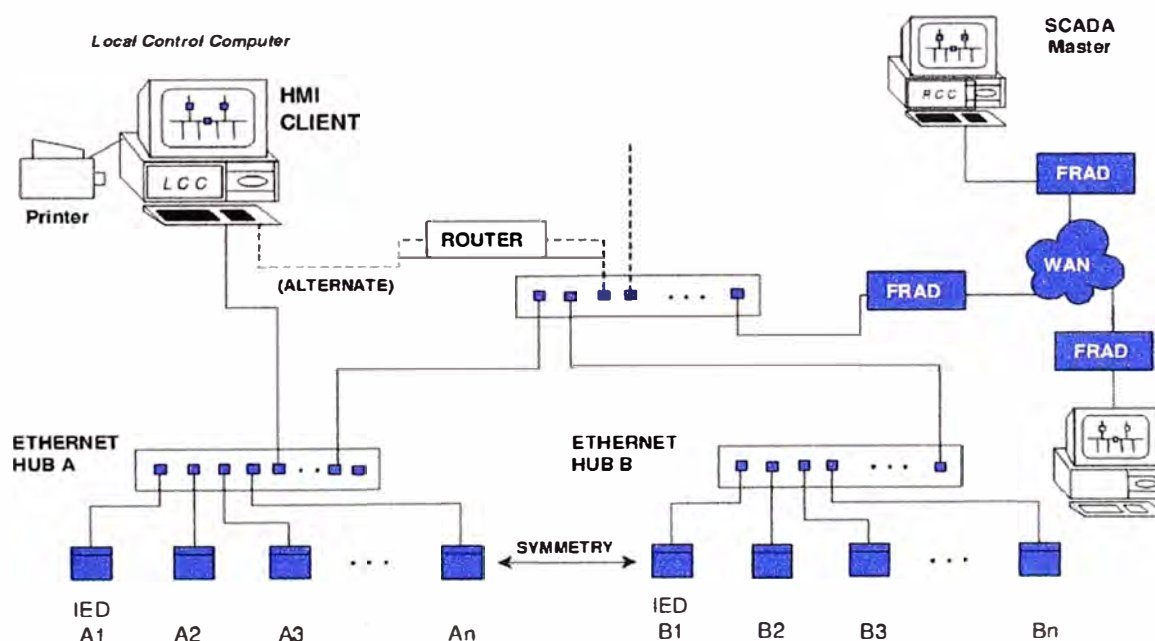


Fig. 2.6 Dispositivos Conectados con Hubs

Red LAN de la Subestación

Las empresas eléctricas vienen implementando sistemas estandarizados de automatización de subestaciones, basados en redes LAN Ethernet. Por lo tanto Ethernet

es la elección para el manejo de los requerimientos de la red LAN de la subestación. Los equipos de la red LAN Ethernet de la subestación deben cumplir los siguientes requerimientos:

- Deben ser equipos para el entorno de subestaciones eléctricas, incorporando inmunidad al ruido de la subestación y aislamiento.
- La red LAN debe tener la capacidad y el ancho de banda suficientes para soportar los requerimientos de adquisición de datos, control y protección.
- La red LAN debe soportar la capacidad de comunicaciones peer-to-peer (entre dos o más nodos de la red, en la que cualquiera de los nodos puede iniciar sesión) para la transferencia de archivos de configuración de IEDs y programas de PLC.
- La red LAN debe soportar routers de interfaz con la red WAN corporativa de la empresa eléctrica.

b) Sistemas de Fibra Óptica

La fibra óptica es un excelente medio para las comunicaciones dentro de la subestación. Proporciona aislamiento eléctrico entre dispositivos de comunicación y aísla al personal y equipos, de tensiones peligrosas e incremento del potencial de tierra. Es totalmente inmune al ruido producido por campos electromagnéticos y puede ser tendida en zonas donde el uso de cable de cobre sería peligroso o corrompería los datos, como para la conexión de dispositivos en diferentes instalaciones físicas de la subestación o en el patio de llaves. Nuevos desarrollos hacen de la fibra óptica una alternativa práctica, económica y segura frente a las comunicaciones utilizando cables de cobre.

La fibra óptica puede ser utilizada para hacer conexiones punto a punto, en lugar de tendidos de cable de cobre. Para hacer esta transición del medio eléctrico al de fibra, se requiere un convertidor de medios, disponible en diferentes configuraciones. Las más comunes son Ethernet, RS-232, RS-485 y RS-422 a fibra.

Topología Anillo

Se suele proveer canales de comunicaciones de fibra óptica de baja velocidad, para enlazar múltiples IEDs de subestaciones en un canal común. Si bien la fibra óptica permite una conexión punto a punto, existen módems de fibra óptica que proporcionan una función de repetidor. Los mensajes pasan a través del módem por un puerto (RD) y salen por otro (TX), formando un anillo como se muestra en la figura 2.7. Si se rompe el anillo todos los IEDs son inaccesibles. Una alternativa a esta arquitectura es utilizar

módems bidireccionales formando dos rutas de anillo, inmunes a la rotura de una fibra, y que permiten un fácil mantenimiento.

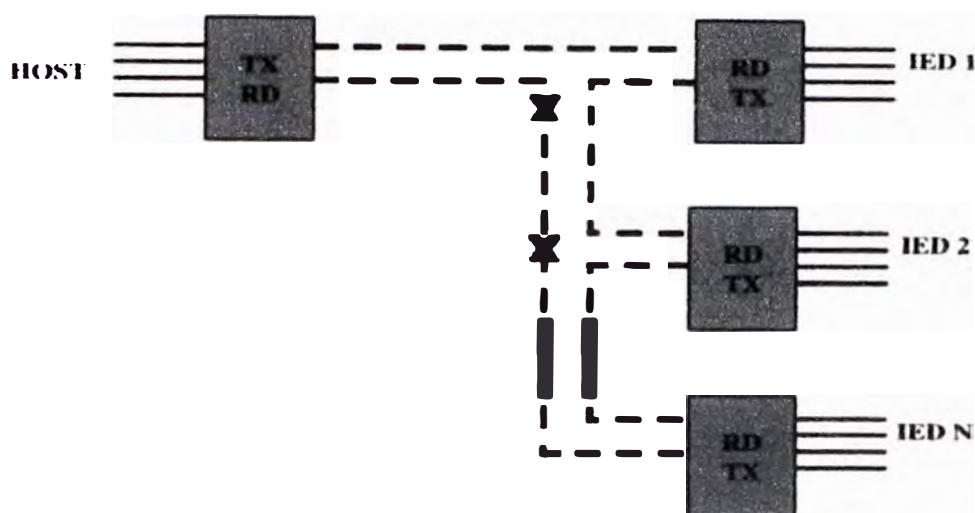


Fig. 2.7 Anillo de Fibra Óptica

Topología Estrella

Algunos diseños de subestaciones se adecuan mejor a una configuración en estrella, donde todas las fibras son tendidas hacia un solo punto. Para tratar esta tecnología existen módems de fibra óptica con múltiples puertos de fibra que se combinan en un solo puerto, típicamente RS-232. Los mensajes recibidos en el puerto RS-232 son enviados a todos los puertos ópticos de salida y los mensajes de retorno de estos, son canalizados al puerto RS-232 de recepción. La figura 2.8 muestra esta topología.

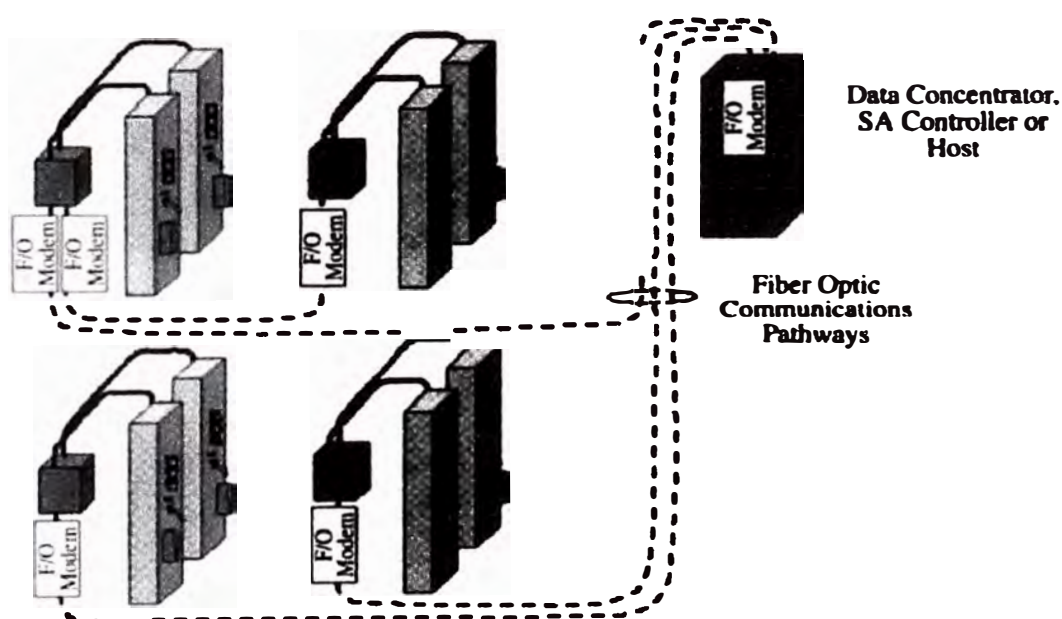


Fig. 2.8 Topología Estrella de Fibra Óptica

Limitaciones

Existen dos limitaciones impuestas por el medio de fibra óptica. No existe provisión de contención de mensajes y detección de colisión. Por tanto, el protocolo de mensajería debe ser maestro-esclavo. No funcionará tampoco el reporte no solicitado por la falta de detección de colisión.

Ethernet sobre Fibra Óptica

Como los IEDS ya cuentan con interfaces de red y las instalaciones SCADA de subestaciones tienen una topología orientada a red, los enlaces de fibra óptica para Ethernet tienen mayor aplicación en las subestaciones. Al igual que las conexiones de fibra óptica de baja velocidad, Ethernet sobre fibra óptica es excelente para aislar dispositivos y zonas en las subestaciones. Existen convertidores de medios, así como routers, hubs y switches con interfaces de fibra óptica para estas aplicaciones. Como Ethernet tiene un sistema de detección de colisiones, el requerimiento para controlar los mensajes mediante un entorno maestro-esclavo es innecesario. Los routers y switches se pueden encargar de este problema. La configuración en estrella es también soportada por routers con múltiples puertos de conexión.

c) Redes Inalámbricas

En el entorno de subestaciones eléctricas, los enlaces inalámbricos podrían ser una buena elección, sin embargo, por la criticidad de los datos operacionales de la subestación y la preocupación por la seguridad de estos enlaces, estos no son implementados dentro de la subestación para la automatización.

2.4.4 Protocolos de Comunicaciones Soportados por los IEDs

Los dos estándares que están siendo considerados principalmente para la arquitectura del sistema de automatización de subestaciones, DNP3 e IEC 61850, tienen sus ventajas y desventajas. Su selección depende de varios factores, tales como los requerimientos funcionales, plazos para la implementación de los sistemas de automatización, la disponibilidad de productos y el costo.

Las principales ventajas de DNP3 sobre IEC 61850 son su gran base instalada, el gran número de productos disponibles con protocolo DNP3, la familiaridad de la empresa eléctrica con el protocolo que permite una fácil implementación, su idoneidad para ciertos IEDs y su bajo costo.

Las ventajas de IEC 61850 sobre DNP3 incluyen la disponibilidad de mensajería peer-to-peer superior (GOOSE o GSSE), que puede ser elegida por la empresa eléctrica para

implementar funciones de protección de alta velocidad, capacidades de navegador de red y una configuración de usuario más fácil. El diseño orientado a objetos de IEC 61850, basado en dispositivos, es considerado generalmente como más adecuado para la integración de aplicaciones empresariales.

La principal desventaja de la norma IEC 61850 es su inmadurez, en términos de experiencia, en implementaciones en empresas eléctricas.

Muchas empresas eléctricas se están estandarizando a soluciones IEC 61850 para todo trabajo en nuevas subestaciones, con ventajas de reducción de tiempos en ingeniería y costos, así como beneficios de ingeniería re-utilizable, que contribuye significativamente a la reducción de costos y la justificación de la inversión. IEC 61850 sobre Ethernet es aplicable a la automatización y protección interna de una subestación. El transporte fuera de la subestación, todavía no se ha desarrollado, pero el grupo de trabajo TC57 de IEC está trabajando en esto.

En el anexo A de este informe se resumen las principales diferencias entre los estándares DNP3 e IEC 61850.

2.5 Comunicaciones con la Empresa Eléctrica

Si bien un sistema de automatización puede estar totalmente contenido dentro de una subestación, son pocos los sistemas implementados sin conexiones externas a la empresa eléctrica. Al igual que con otras partes del sistema, estas interfaces deben cumplir los requerimientos funcionales y de rendimiento de los usuarios, en cualquier lugar en que ellos residan. La disponibilidad de la tecnología de comunicaciones para soportar conexiones externas tiene un impacto económico y de desempeño en los usuarios y la empresa eléctrica. Las interfaces externas también exponen la subestación al entorno más extenso, y por lo tanto, a peligros de acciones externas incontrolables, así como acceso no autorizado o intrusión. La interfaz entre la tecnología de comunicaciones y el sistema de subestaciones se vuelve así, un componente crítico en las expectativas de la empresa eléctrica.

Las interfaces de comunicaciones externas atienden a dos clientes claramente diferentes; los usuarios de operaciones, que realizan monitoreo y control en tiempo real (o casi real) en centros de operaciones e ingeniería, y los usuarios orientados a sesión, que desempeñan actividades de recuperación de datos, mantenimiento y configuración. Las interfaces de monitoreo y control en tiempo real, por lo general son conexiones sostenidas, dedicadas a un solo usuario y/o propósito, tales como un SCADA, un Sistema de Gestión de Energía (EMS) o un Sistema de Gestión de Distribución (DMS). Esta interfaz con frecuencia debe mantener compatibilidad entre un sistema EMS o DMS

existente de la empresa eléctrica y la subestación. Tal interfaz puede tomar diferentes formas:

- Una RTU tradicional SCADA con interfaces cableadas a los equipos de la subestación
- Una RTU moderna donde su interfaz es un gateway de comunicaciones a los IEDs y su(s) red(es)
- Una RTU con función integrada dentro de un host de subestación o un controlador de automatización.

El enlace de comunicaciones dedicado al SCADA/EMS/DMS puede operar con un protocolo tipo serial de legado, con tecnología de comunicaciones de baja velocidad, hasta que las actualizaciones del sistema den paso a una tecnología de comunicaciones moderna. Con canales analógicos facilitando la ruta a enlaces de comunicaciones digitales, tal como Frame Relay, que incorpora protocolos basados en paquetes, se requiere el soporte para transporte de los mensajes de legado con estos protocolos. Los canales basados en red son también capaces de soportar mensajes de legado integrados en el protocolo TCP/IP junto con otro tráfico de red.

Otros usuarios externos se conectan a través de interfaces y enlaces de comunicaciones orientados a sesión, para interactuar bajo demanda, con el sistema de automatización y/o sus IEDs. Por lo general, esta es una interfaz separada a la red de subestación, que se conecta a los puertos de mantenimiento seriales de los IEDs, aislada de la red que soporta el monitoreo en tiempo real, y puede tomar diferentes formas:

- Una red conmutada pública o privada, "dial-up", conexión a un modem con un mecanismo selector de puerto que permita al usuario conectarse a IEDs destino.
- Un dispositivo de interfaz dedicado, que sirve como un punto de conexión para IEDs y un punto de acceso para usuarios externos.
- Un dispositivo de acceso dedicado de interfaz WAN, con suficiente inteligencia para enrutar mensajes hasta IEDs específicos y desarrollar la traducción de protocolos o "empaquetamiento" de mensajes, si fuera necesario.
- Una conexión de red WAN a una red TCP/IP interna de subestación, que se interconecta a los IEDs mediante un gateway, switch de red o firewall.

La configuración de la interfaz de usuario orientada a sesión, es manejada por las capacidades de comunicaciones de los IEDs y la justificación económica para la funcionalidad soportada. Se debe estar consciente de los posibles problemas de seguridad que se pueden presentar al proporcionar acceso del exterior a los puertos de "mantenimiento" de los IEDs.

Toda interfaz externa puede adolecer de problemas de confiabilidad relacionadas con la mensajería a grandes distancias. En muchos casos, tales canales atraviesan diferentes medios físicos que pueden también tener impacto en el desempeño y la confiabilidad. Así mismo, se deben evaluar los posibles efectos de pérdida de cualquier parte de una vía de comunicación debido a la pérdida de alimentación, acceso no autorizado o falla de un dispositivo de interfaz, la exposición del medio del canal a daño físico, la respuesta del propietario del canal a solicitud de servicio de reparación o la reconfiguración de canales por parte de los propietarios sin notificación a los usuarios.

2.5.1 Acceso de la Subestación a la Red de Transporte

Las consideraciones para el tramo de la ruta de comunicación de la subestación a la troncal de transporte de comunicaciones se analizan a continuación.

a) Modelo de Tráfico Representativo

El desarrollo del modelo de tráfico de la subestación a la red de transporte se basa en supuestos típicos:

- El tráfico operacional toma en cuenta el “peor de los casos” de ocurrencia de eventos, donde los cambios son reportados cada ciclo de barrido, para puntos de datos analógicos y digitales.
- El tráfico no operacional desde las subestaciones de transmisión es un archivo (por ejemplo de 9 MB), extraído por dispositivos o personas que inician el proceso de recuperación de datos. Se considera que esta información sea entregada en 10 minutos.
- El tamaño del archivo no operacional de la subestación de distribución es el 25% del archivo de la subestación de transmisión, con recuperación y entrega de menor prioridad.

Las figuras 2.9 y 2.10 muestran los requerimientos de datos operacionales y no operacionales estimados, de subestaciones de transmisión y distribución típicas. Estas figuras indican un número de puntos de barrido de IEDs para IEDs pequeños, medianos, y grandes. Para los datos operacionales de una subestación de transmisión típica, se asume que los barridos de IEDs se producen simultáneamente cada 2 segundos para los puntos digitales y 6 segundos para los puntos analógicos. Además, cuando se producen los barridos, los datos deben ser entregados en tiempo real al Centro de Control antes del comienzo del próximo barrido. Basados en estos parámetros, la Figura 2.9 muestra que la carga burst por segundo en la conexión de la subestación de transmisión a la red WAN para soporte de datos operacionales es de 1,787Bytes o 14.3 Kilobits. Del mismo modo,

para una subestación de distribución, los datos burst operacionales se estiman en 7.1 kilobits. La tasa de datos equivalente por segundo se obtiene asumiendo que los datos digitales de 2 segundos y datos analógicos de 6 segundos, se envían de manera uniforme en los intervalos respectivos entre barridos. Por lo tanto, la tasa de transferencia promedio por segundo requerida sería igual a: ((burst de datos analógicos)/6 segundos + (burst de datos digitales)/2 segundos). En realidad, los barridos de IEDs pueden ser escalonados más que simultáneos, por lo que el tráfico de burst pico más probable sería menor que el mostrado en las figuras. Sin embargo, para fines de planificación, se supone el escenario de "peor caso" de burst. Se añade a los datos burst, las cargas de los protocolos de comunicaciones DNP y red IP, incluyendo reconocimientos, solicitudes de retransmisión y cabeceras, que para este ejemplo se asume se agregan en 10% a la carga útil de los datos.

Para los datos no operacionales de una subestación de transmisión típica, la carga burst es de 90.3 MB o 480 Kbps. Esta incluye los puntos de datos analógicos y digitales, además de los archivos de eventos (SER) y datos de registros de fallas (DFR), generados por cada IED en la subestación en las cantidades mostradas. Se asume que cuando se produce un evento importante, cierto porcentaje de IEDs se verá afectado (columna "% of Interest"). Una latencia aceptada para que los datos sean recibidos por los usuarios en respuesta a una recuperación de datos es de 600 segundos (10 minutos). Del mismo modo, para subestaciones de distribución típicas, se calcula una carga burst de alrededor de 8 Kbps para los datos no operacionales, basados en los parámetros e hipótesis dados.

	# of IEDs	Operational										Non-Operational									
		A point	D Point	Total Point Count	Sec / Scan		Accepted Latency (Sec)		Bytes / Scan	Burst Loading/ Sec	A point	D Point	SER	DFR	% of Interest	Sec / Upload Scan	Accepted Latency (sec)	Bytes / Upload	Burst Bytes / Sec		
Small IED	40	160	320	480	6	2	6	2	3,200	747	160	320	40	0	30%	600	600	2,624,640	1,312		
Medium IED	10	320	160	480	6	2	6	2	1,600	373	160	160	10	0	30%	600	600	658,240	329		
Large IED	10	640	240	880	6	2	6	2	3,040	667	320	240	10	10	40%	600	600	87,060,960	58,041		
Total SA	60	1120	720	1840	6				7,840	1,787	640	720	60	10		600		90,343,840	59,682		
		Equivalent data in kilobits								62.72	14.293	Equivalent traffic in megabits								722.75	0.48
DNP/IP Comm Overhead 10%		Communications Load offered to Network (kbps)								7.9		Communications Load offered to Network (kbps)								625.2	

Fig. 2.9 Datos ofrecidos a la red WAN por una subestación de transmisión típica

	# of IEDs	Operational										Non-Operational									
		A point	D Point	Total Point Count	Sec / Scan		Accepted Latency (Sec)		Bytes / Scan	Burst Loading/ Sec	A point	D Point	SER	DFR	% of Interest	Sec / Upload Scan	Accepted Latency (sec)	Bytes / Upload	Burst Bytes / Sec		
Small IED	10	40	80	120	6	2	6	2	800	187	40	80	10	0	10%	1200	1200	658,160	55		
Medium IED	10	80	160	240	6	2	6	2	1,600	373	160	160	10	0	10%	1200	1200	658,240	55		
Large IED	5	60	120	200	6	2	6	2	1,520	333	160	120	5	5	10%	1200	1200	11,130,480	928		
Total SA	25	200	360	360	6				3,920	893	360	360	25	5		1200		12,444,880	1,037		
		Equivalent data in kilobits								31.36	7.1467	Equivalent traffic in megabits								99.56	0.008
DNP/IP Comm Overhead 10%		Communications Load offered to Network (kbps)								7.9		Communications Load offered to Network (kbps)								9.1	

Fig. 2.10 Datos ofrecidos a la red WAN por una subestación de distribución típica

b) Medios de Comunicación

Los modelos de tráfico de subestaciones de las figuras 2.9 y 2.10 identifican una necesidad de una conexión de red para soportar datos operacionales y no operacionales. Dado que los datos operacionales tienen requerimientos diferentes a los de los datos no operacionales, tales como una latencia más rigurosa y una mayor necesidad de seguridad y protección, deben ser separados de los datos no operacionales tanto como sea posible. Esto se puede lograr en una sola conexión física, segmentando los datos en diferentes redes lógicas de la subestación, a través de la red troncal corporativa, si son enrutados sobre instalaciones privadas compartidas. Esto permite mayor flexibilidad de protección de los datos operacionales de intrusiones no autorizadas, involuntarias o maliciosas. Otras consideraciones para las comunicaciones de la subestación a la red WAN son:

Diversidad y Criticidad

Si se han establecido redes separadas para los datos operacionales y no operacionales, es innecesario el uso de un esquema de prioridades para separar el tráfico, a menos que exista una necesidad de priorizar el tráfico dentro de cada tipo de datos. Si es necesaria la priorización, entonces se requiere la capacidad de priorizar el tráfico IP, basado en la dirección de origen, puerto de origen, dirección de destino y puerto de destino.

Acceso Remoto y Cambio de Configuraciones de Dispositivos

El acceso remoto se producirá a través de diversos firewalls y mecanismos de seguridad que se implementan en la subestación, utilizando VPN. Las VPNs requieren un nivel de autenticación del usuario final (dispositivo) que solicita la conexión, y protegen los datos en el transporte de escuchas ilegales o modificación no detectada.

Los esquemas de conexión típicos con la empresa eléctrica son los siguientes:

Fibra Óptica

La instalación de fibra óptica de la subestación al punto de entrada más cercano de la troncal (por ejemplo un nodo SONET o un tributario que se conecta eventualmente al nodo de SONET) garantizaría un servicio seguro de máxima confiabilidad. Generalmente, la fibra óptica puede ser de tipo ADSS (Cable Dieléctrico Autosoportado), instalado como un cable más sobre postes y torres eléctricas, u OPGW (Cable de Guarda Óptico), donde la fibra está incluida en un cable de tierra instalado sobre las torres.

Conexiones inalámbricas

Establecen una conexión de radio a la subestación. La ruta de radio puede ser tipo punto a punto o punto a multipunto. La ruta debe ser diseñada para garantizar una confiabilidad de propagación superior a 99.999%. El uso de banda no licenciada está sujeta a posibles interferencias. Se puede usar como alternativa una radio licenciada (por ejemplo microondas de banda estrecha), pero los costos pueden incrementarse.

Servicios Arrendados

El arrendamiento de servicios T1 o Frame Relay de un proveedor de telecomunicaciones siempre es una opción, pero con la transferencia del tráfico al proveedor, se pierde cierto grado de control. Las desventajas de las líneas arrendadas se han mencionado anteriormente, considerándose además las implicaciones desde el punto de vista de la seguridad.

Las configuraciones típicas de acceso de subestaciones a la red de transporte se muestran en la figura 2.11.

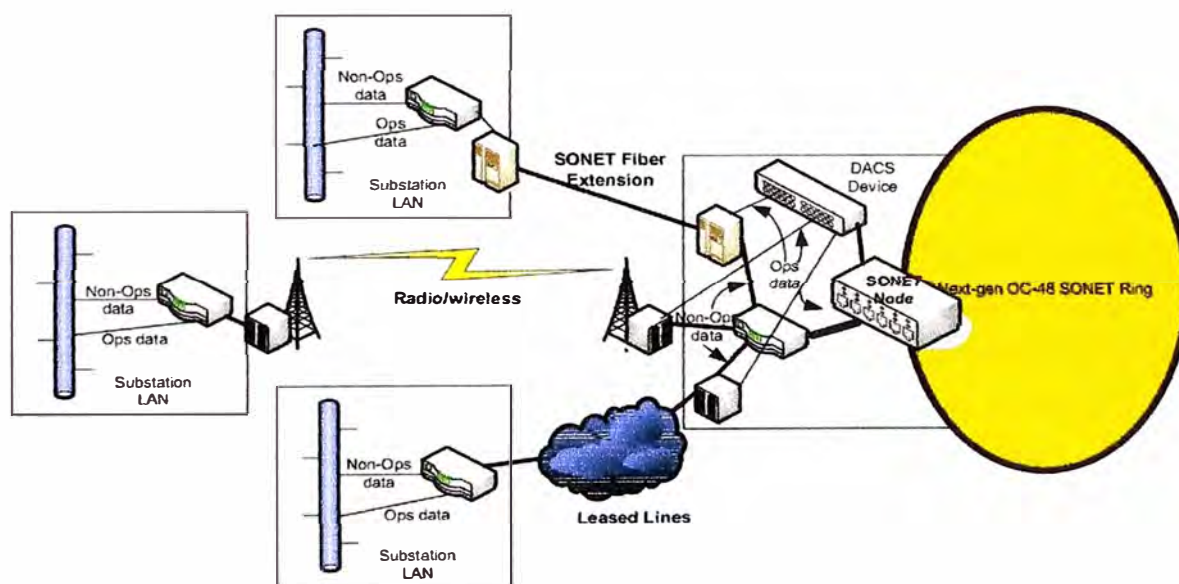


Fig. 2.11 Configuración Típica de Acceso de una Subestación a la Red de Transporte

Existen otros medios que pueden emplearse para la comunicación con la empresa eléctrica. Los más utilizados se describen a continuación.

Comunicaciones de Onda Portadora

Durante décadas las soluciones de Onda Portadora han sido utilizadas por las empresas eléctricas para la transmisión de información vital de protección y operación de la red eléctrica de transmisión.

El uso de las líneas eléctricas como medio de comunicación, proporciona el enlace más directo para la teleprotección (donde los tiempos de transmisión son fundamentales), es confiable y está completamente bajo control de la empresa eléctrica. A pesar de la creciente importancia de los sistemas de comunicaciones digitales de banda ancha, en especial los que utilizan fibra óptica o equipos de microondas, la Onda Portadora sigue siendo una solución rentable para enlazar distancias muy largas (cientos de kilómetros) sin repetidores. La Onda Portadora es una de las soluciones principales de respaldo de los sistemas de banda ancha y permite aumentar la disponibilidad de servicios de misión crítica.

En la actualidad coexisten dos grupos de Onda Portadora que se clasifican como se muestra en la figura 2.12.

PLC type	Modulation principle	Application	RF bandwidth
Single purpose (Analog)	- On/Off carrier - FSK (Frequency Shift Keying)	- Teleprotection signaling	typical < 2 kHz
Multi purpose (Analog/Digital)	- SSB (Single Sideband) - MCM (Multi-Carrier Modulation)	- Teleprotection signaling - Voice - Data - Teleoperation	typical \geq 2 kHz

Fig. 2.12 Clases de Onda Portadora

En los últimos años, los avances tecnológicos para aumentar la velocidad de transmisión de datos de estos sistemas ofrecen nuevas oportunidades para las aplicaciones de Onda Portadora, en particular las relacionadas con la provisión de mayor ancho de banda e integración a redes digitales, junto con mejoras funcionales, así como facilidad y flexibilidad de uso. Estas nuevas posibilidades, junto con las consideraciones económicas y de confiabilidad de la Onda Portadora, han dado lugar a una notable reactivación de los sistemas de Onda Portadora en todo el mundo.

Las últimas generaciones de equipos de Onda Portadora, son sistemas realmente embebidos, que integran el suministro de múltiples servicios en una sola plataforma, cubriendo todas las aplicaciones críticas de las empresas eléctricas:

- Transmisión rápida, confiable y segura de comandos de protección (señalización de teleprotección)
- Transmisión transparente de señales de voz
- Comunicación totalmente transparente de datos de baja velocidad con retardo mínimo en aplicaciones punto-multipunto, típico para interrogación de SCADA/RTU con velocidades de datos de hasta 9600 bps

- Multiplexación adaptativa de servicios de datos con control de flujo de tráfico para velocidades de transmisión de hasta 256 kbps
- Conectividad a switches, multiplexores o routers externos, con el fin de soportar total integración en TDM, Ethernet o redes WAN basadas en IP

La figura 2.13 muestra un ejemplo de múltiples enlaces digitales de Onda Portadora proporcionando canales de datos a nodos de acceso y formando una red de comunicación de servicio múltiple.

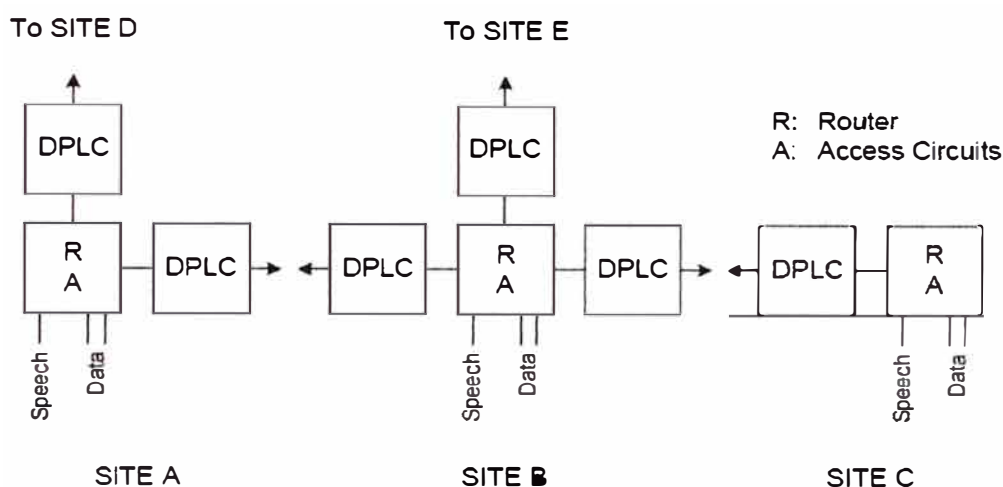


Fig. 2.13 Nodos de Acceso en Enlaces de Onda Portadora

Aunque la Onda Portadora es utilizada principalmente para propósitos de teleprotección, el aumento del ancho de banda también ofrece oportunidades para la comunicación SCADA tales como datos seriales (DNP 3.0/IEC 60870-5-101) y LAN (DNP 3.0/IEC 60870-5-104). Además se pueden transmitir simultáneamente, voz y servicios de teleprotección. La Onda Portadora puede ser la única forma viable de llegar a una subestación remota con menores requerimientos de servicio. El costo típico de un enlace de Onda Portadora es de alrededor de \$100K, incluyendo las piezas de alta tensión, acopladores y filtros y trampas de onda. La distancia que se puede lograr depende de las características de la línea. Un enlace de Onda Portadora puede llegar a 150-200 kilómetros sin repetidores, aunque existen enlaces de hasta 1000 kilómetros.

Enlaces Satelitales

Se considera el uso de satélites cuando el acceso a una subestación es limitado por las condiciones del terreno (áreas de difícil acceso) o por la distancia. El servicio por satélite más utilizado por las empresas eléctricas es VSAT (Terminal de muy Pequeña Apertura). La mayoría de productos comerciales VSAT emplean la tecnología de multiplexación por

división de tiempo/acceso múltiple por división de tiempo (TDM/TDMA), la modulación QPSK y codificación para transmisiones de baja tasa de error de bits.

La oferta de servicios VSAT soporta comunicaciones de datos con las siguientes características:

- Capacidad de ancho de banda de 30 a 100 kbps
- Latencia de red de 2 a 8 segundos (latencia mayor para algunos servicios)
- Disponibilidad en la mayoría de lugares
- Capacidad bidireccional
- Precio competitivo para determinadas líneas arrendadas, en función del área y número de subestaciones a ser incluidas en la red VSAT.

Respecto al último punto, el establecimiento de un sistema VSAT requiere cierto nivel de costos fijos: existe un cargo fijo por una determinada capacidad del transpondedor, por lo general vendido como capacidad para un "bloque" de terminales VSAT. A medida que más terminales se incluyen en el sistema, baja el costo efectivo por terminal. También existe un costo por el terminal VSAT, así como costos recurrentes de operación y mantenimiento, tales como los costos asociados a las operaciones del hub e interfaz con el centro de control. Los procesadores de comunicaciones del centro de control necesitan ser configurados para trabajar con el retardo integrado inherente de ida y vuelta de la tierra al satélite.

2.5.2 Red de Transporte

Considerada la "columna vertebral" de la red WAN de comunicaciones, normalmente se establece como un anillo de alta confiabilidad con nodos en las subestaciones y conexiones a las subestaciones periféricas.

a) Modelo de tráfico representativo

Esta sección analiza el impacto de los requerimientos de tráfico de las subestaciones explicadas en la sección 2.5.1, sobre la troncal de transporte. Si bien cada enlace de la subestación a la troncal de transporte debe diseñarse para el "peor de los casos", la troncal de transporte debe diseñarse para un escenario de carga de tráfico más probable. En otras palabras, no es rentable ni práctico diseñar la troncal para soportar, por ejemplo, descargas simultáneas de datos no operacionales de 525 kbps del 100% de las subestaciones de transmisión. Por el contrario, se debe considerar la ocurrencia más probable, con un margen para casos extremos. Las ocurrencias más probables toman en cuenta el número de subestaciones que están realmente involucradas durante un evento

típico, tal como un evento meteorológico o una falla de línea. Para desarrollar el modelo para una empresa eléctrica, se consideran los siguientes supuestos:

- Un evento típico puede involucrar hasta un 3% del total de las subestaciones
- La recuperación de datos no operacionales es iniciada por el centro de control, los datos son extraídos en lugar de ser colocados
- No más de 4 a 8 recuperaciones de datos se inician al mismo tiempo

b) Carga de Transporte

La figura 2.14 muestra el efecto de la carga de tráfico en toda la troncal de transporte, cuando se incrementa la participación de subestaciones durante un evento. Las capacidades que se muestran en la figura indican el efecto si todos los archivos no operacionales fueran recuperados al mismo tiempo (es decir, no se limita al total supuesto de 4 a 8 archivos). En el nivel de participación típico de 1.5 a 3%, los datos no operacionales agregan a la red de transporte hasta 4.35 Mbps de carga adicional y 250 Kbps de datos operacionales. La infraestructura de transporte ha de ser adecuada para dar cabida a este incremento de carga de tráfico. Una buena práctica, por lo general, consiste en diseñar una capacidad para el doble de las expectativas "típicas". Basado en esta regla general, puede ser adecuado diseñar la red del ejemplo para asegurar que se pueda dar cabida a un máximo de 5 a 10% de participación de la subestación.

		241 Transmission Substations 533 Distribution Substations			Operational Data		Non-Operational Data	
	# of Substations	Analog Count	Digital Count	Total Count	MBits / Scan	Burst Loading (MBits/Sec)	Mbits / Upload	Burst Loading Mbits / Sec
1.5% of Substations participating								
Transmission	4	4,480	2,880	7,360	0.251	0.06	2,891	1.91
Distribution	8	1,600	2,880	4,480	0.251	0.06	796	0.07
Total	12	6,080	5,760	11,840	0.502	0.11	3,687	1.98
DNP/IP Comm Overhead		10%	Communications Load (Mbps)		0.13		2.17	
3% of Substations participating								
Transmission	8	8,960	5,760	14,720	0.502	0.11	5,782	3.82
Distribution	16	3,200	5,760	8,960	0.502	0.11	1,593	0.13
Total	24	12,160	11,520	23,680	1.004	0.23	7,375	3.95
DNP/IP Comm Overhead		10%	Communications Load (Mbps)		0.25		4.35	
5% of Substations participating								
Transmission	13	14,560	9,360	23,920	0.815	0.19	9,396	6.21
Distribution	27	5,400	9,720	15,120	0.847	0.19	2,688	0.22
Total	40	19,960	19,080	39,040	1.662	0.38	12,084	6.43
DNP/IP Comm Overhead		10%	Communications Load (Mbps)		0.42		7.07	
10% of Substations participating								
Transmission	25	28,000	18,000	46,000	1.568	0.36	18,069	11.94
Distribution	54	10,800	19,440	30,240	1.693	0.39	5,376	0.45
Total	79	38,800	37,440	76,240	3.261	0.74	23,445	12.38
DNP/IP Comm Overhead		10%	Communications Load (Mbps)		0.82		13.62	

Fig. 2.14 Efectos de Participación de Subestaciones en la Troncal de Transporte

Como se mencionó anteriormente, la infraestructura de comunicaciones debe ser desarrollada de manera que la entrega de datos operacionales no se retrase, si los

recursos o capacidad de las comunicaciones llegan a ser limitados. Debe implementarse un medio que asegure la prioridad a los datos operacionales sobre los datos no operacionales, garantizando siempre su entrega. Esto se puede hacer limitando las extracciones de datos no operacionales en momentos de alta actividad SCADA o mediante la segmentación de los tipos de datos en el transporte, dedicando un ancho de banda para cada tipo de datos.

2.6 Consideraciones de Implementación

Debido a las limitaciones de presupuesto y recursos, una estrategia de implementación puede durar varios años.

La implantación de soluciones de automatización de la subestación debe ser consecuente con la implantación de mejoras a la infraestructura de comunicaciones de la empresa eléctrica, para aprovechar al máximo y optimizar las nuevas funciones y la información disponible.

2.6.1 Coexistencia de Redes Nuevas y Existentes

Un tema clave en la planificación de la implementación es determinar la coexistencia de los nuevos sistemas y los sistemas existentes. Debido al largo período de implementación, existirán requerimientos de soporte de equipos, operaciones especiales y consideraciones de mantenimiento. Se debe ejecutar un plan de migración con componentes de corto plazo (por subestación) y de largo plazo (coexistencia de sistemas nuevos y existentes). Una adecuada planificación de la migración es clave en el desarrollo del plan de implementación de largo plazo.

La planificación de la migración no es una tarea trivial. Sin embargo, un plan bien pensado producirá menos riesgos, costos más bajos, menos molestia al usuario y menos dolores de cabeza al personal de campo. Las principales consideraciones para que una migración soporte tecnologías nuevas y existentes son:

- Mantenimiento de interfaces de comunicaciones existentes y nuevas en procesadores de comunicaciones (Front-End) del Centro de Control. Un centro de control puede tener sólo interfaces seriales y una migración a IP es la futura ruta de la red de comunicaciones. Debe desarrollarse un plan para soportar los dos tipos de datos, ya sea utilizando convertidores IP a seriales, reemplazando a los procesadores de comunicaciones por interfaces IP o una combinación de ambos.
- Elaboración de un plan para convertir los datos seriales de la RTU a IP para el transporte sobre la red WAN o para mantener una red punto a punto serial aparte con el centro de control.

Con la disponibilidad de equipos Terminal Server, las conversiones de serial a IP pueden ser rentables.

2.6.2 Períodos de Tiempo

Las instalaciones iniciales de automatización de subestaciones suelen tomar varios meses, incluyendo la planificación, las adquisiciones y la instalación. Una vez que el personal de la empresa eléctrica o contratistas han adquirido cierto nivel, la implementación será mucho más rápida debido a las lecciones aprendidas, las mejoras resultantes del proceso, la eliminación de esfuerzos de desarrollo y diseño, la familiaridad con los sistemas, la disponibilidad de planos, base de datos, despliegues, mapeos, etc., estándares.

2.6.3 Requerimientos Organizacionales

Las organizaciones dentro de una empresa eléctrica tienen diferentes prioridades, funciones y preocupaciones, que se deben tratar y no se deben comprometer con un diseño estándar de la red de comunicaciones de la subestación o la red WAN.

Por ejemplo, las organizaciones de protección y operaciones tienen requerimientos funcionales críticos totalmente diferentes, que históricamente se realizan utilizando redes separadas e independientes, con cada organización responsable de la rendición de cuentas, acceso y control de su propia red. La red convergente, enrutable y automatizada, hace que las organizaciones se unan, con una necesidad renovada de coordinar el acceso a la red, evitar el uso no autorizado, asegurar que se asignen las instalaciones adecuadas para satisfacer los requerimientos particulares, compartir los recursos, y quizás designando una sola organización responsable por los requerimientos de aislamiento, implementación de firewalls y seguridad entre las redes LAN, para proteger los activos de cada organización.

La solución de este problema de organización debe ser el primer paso a considerar en las implementaciones de la red LAN o WAN para la automatización. También es esencial elegir el marco de seguridad de la información (por ejemplo, cumplimiento de las normas de seguridad informática del NERC). Estos temas deben tratarse con la alta gerencia y las sesiones iniciales de toma de decisiones deben incluir a todos los interesados.

2.6.4 Alternativas de Implementación

Cuando se producen las actualizaciones a las nuevas plataformas de automatización y comunicaciones de las subestaciones, las empresas eléctricas pasan por las curvas de aprendizaje de las nuevas tecnologías, participando activamente en las

implementaciones y utilizando sus recursos propios (personal). La implementación de las nuevas tecnologías suele hacerse primero como un piloto de pruebas y luego de los resultados exitosos de este piloto, se desarrolla un plan de implementación más amplio.

a) Implementaciones hechas por la empresa eléctrica

Muchas grandes empresas eléctricas prefieren hacer ellas mismas las actualizaciones o instalaciones de equipos de comunicaciones de subestaciones o a través de sus subcontratistas y desarrollan planes de implementación que coinciden con el nivel de recursos y presupuesto disponible. La ventaja de que las mismas empresas realicen la implementación es el ahorro de costos, que son mayores después de las primeras instalaciones iniciales. La desventaja es el riesgo. Las principales lecciones aprendidas de estas empresas durante la implementación, son la curva de aprendizaje que su personal tiene que pasar para llegar al punto de eficiencia y su preocupación es la adaptación de los trabajadores a las nuevas tecnologías, puesto que muchos de ellos trabajan con equipos antiguos a los que están familiarizados.

Las empresas eléctricas más pequeñas pueden estar más inclinadas a contratar personal para las nuevas instalaciones, ya que normalmente no tienen la mano de obra disponible para dedicarla completamente al proyecto de instalación.

b) Proyectos Pilotos

La mayoría de implantaciones de nuevas tecnologías en las empresas eléctricas primero se ejecutan mediante una instalación experimental o piloto. Esta estrategia tiene muchas ventajas, incluyendo la reducción del riesgo, e involucran bastante al proveedor. El piloto permite que la empresa eléctrica aprenda la tecnología a su propio ritmo, dejando que el proveedor sea el responsable de su éxito. Este proceso de aprendizaje es un trampolín, para asumir la responsabilidad de las instalaciones posteriores durante la implantación a escala completa. Las instalaciones pilotos han sido utilizadas para la implementación de nuevas tendencias, tales como IEC61850 y SCADA sobre IP. La plataforma privada de comunicaciones de red WAN tiende a ser implementada a escala completa, o por etapas hasta la implementación completa, ya que tiene que estar instalada, cuando se requiera utilizarla. Sin embargo, los nuevos servicios arrendados de comunicaciones de carriers, tales como MPLS, también se implementan con frecuencia mediante proyectos pilotos.

c) Subcontratos

Las empresas eléctricas pueden recurrir a subcontratar la planificación, ingeniería, e instalaciones llave en mano, cuando no tienen recursos para hacerlo, especialmente

cuando se trata de la implementación de nuevas tecnologías. Este enfoque tiene sus ventajas para la implementación de un proyecto piloto o si la fuente contratada tiene un buen manejo de las mejores prácticas de la industria. Esto permitirá desarrollar una estrategia de trabajo consecuente con la industria, haciendo que las justificaciones de presupuesto y recursos sean una tarea más fácil. Normalmente, las empresas eléctricas contratan la asistencia en la planificación e ingeniería, agregándola a su personal que aún tiene la responsabilidad por el resultado final. Las empresas pueden subcontratar un proyecto de instalación llave en mano en grandes proyectos, pero por lo general utilizarán sus recursos propios para operaciones y mantenimiento, o pequeños proyectos de instalación.

2.6.5 Plan de Proyecto

Un buen plan de proyecto proporciona un repositorio central de información para el equipo del proyecto y cubre al menos los siguientes tópicos:

- a) Alcance del Proyecto
- b) Plan de Calidad
- c) Plan de Gestión
- d) Documentación
- e) Plan de Transición
- f) Plan de pruebas
- g) Plan de Capacitación
- h) Plan de Instalación
- i) Plan de Seguimiento

El Gerente de Proyecto desarrolla el Plan de Proyecto para todos los participantes del proyecto (personal de Diseño/Especificaciones, Proveedor(es), Integrador(es) y el propio Gerente del Proyecto). El Plan de Proyecto debe ser realizado en el inicio del proyecto y sostenido a través de todo el proyecto.

CAPÍTULO III

APLICACIÓN DE LA IMPLEMENTACIÓN DE SISTEMA DE COMUNICACIONES PARA LA AUTOMATIZACIÓN DE SUBESTACIONES ELÉCTRICAS

3.1 Introducción

Se explica a continuación una aplicación de implementación de sistema de comunicaciones para la automatización de subestaciones eléctricas de la Compañía Minera Antamina.

Compañía Minera Antamina es integrante del Sistema Eléctrico Interconectado Nacional (SEIN) como Cliente Libre. La legislación eléctrica peruana considera como Clientes Libres, a aquellos usuarios que estando situados en cualquier punto de la red, tienen potencias conectadas mayores de 1 MW o exceden al 20% de la demanda máxima de la zona de concesión de distribución. Estos usuarios potencialmente tienen una capacidad de negociación tal, que pueden pactar un nivel de precios en forma directa, ya sea con la empresa distribuidora, o bien con cualquiera de las empresas generadoras existentes en el SEIN. [7]

Antamina es una empresa constituida en el Perú, regida por leyes peruanas, y cuyos accionistas son cuatro compañías líderes en la minería internacional: [8]

- Xstrata con el 33,75%
- BHP Billiton Plc., con el 33,75%
- Teck - Cominco Limited, con el 22,5%
- Mitsubishi Corporation, con el 10%

Inició sus operaciones de prueba el año 2001, luego de concretarse la mayor inversión en la historia de la minería peruana, y comenzó su producción comercial el 1º de Octubre de ese año. El yacimiento se encuentra ubicado en la quebrada del mismo nombre, en el distrito de San Marcos, provincia de Huari, en la región Ancash, entre los 4,200 y 4,700 metros sobre el nivel del mar. El depósito mineral de Antamina es el Skarn de cobre-zinc, plata, molibdeno y bismuto, más grande del mundo conocido en la actualidad. Antamina es una mina con método de explotación a tajo abierto, como se muestra en la figura 3.1.

En la actualidad posee una producción promedio diaria de 360,000 toneladas de material, y opera las 24 horas del día los 365 días del año, en turnos de 12 horas lo cual la convierte en una de las diez primeras minas a escala mundial en cuanto a volumen de operación.



Fig. 3.1 Tajo Abierto de Antamina

La fuente de suministro eléctrico de Antamina proviene de la Subestación Vizcarra, ubicada en el distrito de Huallanca, Provincia Dos de Mayo, en la región Huanuco, ubicada a dos horas de Antamina, por carretera. Consta de un patio de llaves de 220 kV a la intemperie con una configuración de juego de barras en anillo, y cuatro celdas de 220 kV con sus respectivos IEDs relés de protección, medidores y otros. Las figuras 3.2 y 3.3 muestran la Subestación Vizcarra y sus celdas.



Fig. 3.2 Subestación Vizcarra



Fig. 3.3 Celdas de la Subestación Vizcarra

A través de la Subestación Vizcarra, el sistema de transmisión de Antamina se interconecta con el sistema de transmisión de Eteselva, empresa del Grupo Energético Aguaytia dedicada a las operaciones vinculadas específicamente con la actividad comercial de transmisión de electricidad. [9]

Dos celdas de 220 kV de la Subestación Vizcarra pertenecen a Antamina. La línea de transmisión Vizcarra - Antamina (L-2255) se conecta a una de estas celdas y en el otro extremo a la Subestación Principal Antamina en mina.

La Subestación Principal Antamina de 220/23 kV consta de un patio de llaves con dos transformadores con capacidad de transformación instalada de 2 x 75/100/125 MVA. [10] Cuenta con una celda de 220kV y veintiséis celdas de 23 kV para alimentación de cargas, bancos de condensadores y filtros de armónicos, con sus respectivos relés de protección, medidores y otros. Las figuras 3.4 y 3.5 muestran la Subestación Principal y sus celdas.



Fig. 3.4 Subestación Principal Antamina



Fig. 3.5 Celdas de la Subestación Principal

El diagrama unifilar de estas dos subestaciones se muestra en el Anexo B.

3.2 Niveles de Automatización

La figura 3.6 muestra los niveles de automatización de subestaciones eléctricas, desde los equipos de campo hasta el centro de control, y cuyas características son:

- Nivel Equipos de Campo: comprende todos los equipos de campo, que en este caso serían principalmente los seccionadores, interruptores, y transformadores.
- Nivel IEDs: comprende los diferentes IEDs de la subestación (relés, medidores, etc.), comunicados a través de una red de campo.
- Nivel Subestación: comprende la comunicación de la red de campo con la RTU, PLC, concentrador o controlador, para la supervisión, control y adquisición de datos, que puede realizarse mediante una interfaz de usuario. Comprende también la comunicación con el centro de control mediante la red de subestación.
- Nivel Centro de Control: comprende la comunicación de la red de subestación con el centro de control.

El sistema de comunicaciones debe especificar las interfaces y protocolos de comunicaciones entre el nivel IEDs y nivel Subestación; así como entre el nivel Subestación y el nivel Centro de Control. Se considera también la comunicación del Centro de Control de Antamina con el Centro de Control del COES SINAC, la comunicación directa desde el Centro de Control Antamina con los IEDs para configuración y el acceso remoto externo a la subestación. Para el proyecto se utilizó la tecnología Ethernet para crear la red LAN en la Subestación Principal Antamina para el

monitoreo de esta subestación y de la Subestación Vizcarra. Incluye concentradores que agrupan los datos en cada subestación.

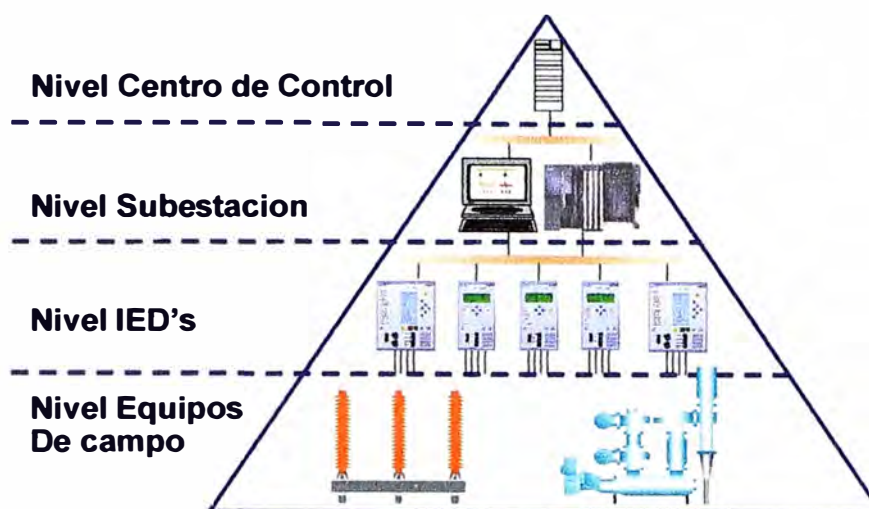


Fig. 3.6 Niveles de Automatización de una Subestación Eléctrica

3.3 Centro de Control de Antamina

Al conjunto de dispositivos, módulos funcionales e interfaces con los canales de comunicación que permiten llevar a cabo correctamente las funciones de supervisión, se le da el nombre de Centro de Control. [11]

Los centros de control llevan a cabo las funciones del SCADA: sistema de supervisión, control y adquisición de datos. Con el tiempo se han ido añadiendo otras funciones de aplicación a los centros de control, obteniéndose sistemas de gestión, tales como el Sistema de Gestión de Energía (EMS), Sistema de Gestión de Generación (GMS) y Sistema de Gestión de Distribución (DMS), así como sistemas de almacenamiento y recuperación de la información. Para llevar a cabo estas tareas, el centro de control en particular, y el sistema de automatización en general, deben estar diseñados bajo las premisas de fiabilidad, seguridad, confiabilidad, alto desempeño, flexibilidad, alta disponibilidad, computación distribuida, manejo real y economía. A fin de aumentar la confiabilidad del sistema todos los componentes tanto en hardware como en software deben presentar sistemas redundantes, además se requiere un alto desempeño de estos componentes, así como también una alta funcionalidad del centro de control.

Para Antamina, el Centro de Control tendrá básicamente de las siguientes funciones:

- a) Obtener los datos periódicamente de los Concentradores de Datos de sus dos subestaciones de 220kV.
- b) Controlar dispositivos remotos por el operador del Centro de Control.

Para realizar estas funciones, se establecerán las comunicaciones con los Concentradores de Datos e IEDs en cada subestación. La información será procesada por un Sistema SCADA instalado en el Centro de Control a implementarse en la Subestación Principal Antamina, como se muestra en la figura 3.7.

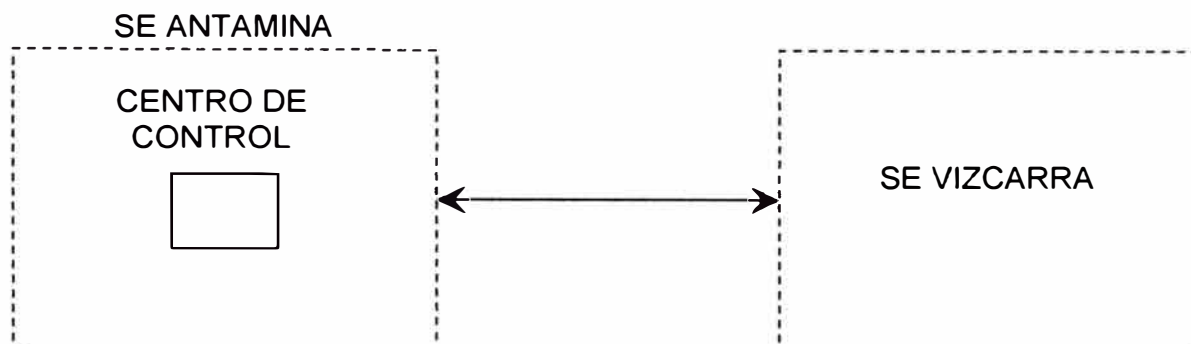


Fig. 3.7 Ubicación del Centro de Control

3.4 Comunicaciones en Subestación Antamina

3.4.1 Entre Niveles IEDs - Subestación

La Subestación Antamina dispone de los siguientes IEDs y dispositivos de control:

- 25 relés General Electric SR750, con dos interfaces seriales RS-485 y protocolos DNP3 y MODBUS
- 15 medidores General Electric PQM, con dos interfaces seriales RS-485 y protocolos DNP3 y MODBUS
- 01 medidor PML ION 7600 totalizador, con una interfaz serial RS-232/RS-485 y una interfaz serial solo RS-485, con protocolos DNP3 y MODBUS
- 02 indicadores de posición de taps de transformadores de potencia Treotech PI, con interfaz serial RS-485 y protocolo MODBUS
- 02 monitores de temperatura de transformadores de potencia, con interfaz serial RS-485 y protocolo MODBUS
- 02 analizadores de gases de transformadores de potencia, con interfaz serial RS-232 y protocolo GE Hydran
- 01 dispositivo de control PLC Allen-Bradley PLC5 del sistema de control del factor de potencia (PFC)
- 02 dispositivos de control del sistema UNITROL de monitoreo de condensadores síncronos

Los relés y medidores reciben la información de tensiones y corrientes de líneas y alimentadores de esta subestación, a través de cableado físico conectado directamente a los bornes específicos de estos IEDs. Con esta información, estos dispositivos realizan

cálculos para obtener los demás valores analógicos (frecuencia, potencia, energía, etc.). Los relés realizan funciones de protección, de acuerdo a umbrales configurados por los operadores del sistema eléctrico. Las medidas eléctricas analógicas se obtendrán de los relés mediante una interfaz serial RS-485 con protocolos DNP3 y de los medidores mediante una interfaz serial RS-485 con protocolos MODBUS. Para los relés se utilizará el protocolo DNP3, puesto que se desea su sincronización desde el Centro de Control, utilizando este protocolo, para el secuenciamiento de eventos. Para los medidores se utilizará el protocolo MODBUS, puesto que no requieren sincronización.

Los estados de interruptores de esta subestación serán conectados desde sus contactos auxiliares hasta los bornes de entrada de los relés General Electric SR750, asociados a dichos interruptores.

Con los medidores PQM y relés SR750, se establecerán ocho buses RS-485 que serán conectados a las interfaces seriales de un Concentrador de Datos de múltiples puertos, concentrando toda la información de esta subestación (medidas analógicas, estados de interruptores y alarmas de protección).

Los estados de seccionadores y algunas alarmas en 220kV serán recopilados mediante un módulo de entradas digitales del Concentrador de Datos.

Se establecerá un bus RS-485 con los indicadores de posición de taps, monitores de temperatura de transformadores y medidor ION 7600, que será conectado a otra interfaz serial del Concentrador de Datos, utilizando protocolo MODBUS. Los analizadores de gases se integrarán a este bus mediante convertidores de protocolo (de GE Hydran a MODBUS).

La integración del PLC del sistema PFC, para analizar su comportamiento durante eventos del sistema de potencia, se realizará instalando un módulo gateway en un rack disponible del PLC, proporcionando una interfaz serial con protocolo DNP3 para lectura de datos.

La integración de los dispositivos de control UNITROL a fin de establecer monitoreo de los Condensadores Síncronos, se realizará formando un anillo de fibra óptica conectado a un módem con interfaz serial y protocolo MODBUS.

3.4.2 Entre Niveles Subestación - Centro de Control

Para una alta confiabilidad del sistema, en el Centro de Control se implementará una red LAN TCP/IP redundante, basada en switches Ethernet de 12 puertos 10/100 Mbps.

La información agrupada en el Concentrador de Datos accederá a la red LAN redundante a través de un switch Ethernet de 24 puertos 10/100 Mbps, para ser procesada por el Sistema SCADA Survalent, utilizando protocolo DNP3.

3.4.3 Comunicaciones entre Centros de Control

Parte de la información procesada por el Sistema SCADA Survalent, que reside en los dos servidores industriales redundantes conectados a la red LAN redundante del Centro de Control, es utilizada para el envío de datos al COES SINAC, utilizando el protocolo ICCP.

Debido a la dificultad de acceso a la subestación Antamina, el medio para la transferencia de la información será satelital, utilizando un servicio arrendado al carrier de telecomunicaciones Global Crossing (antes IMPSAT), que incluirá el suministro del equipo de comunicaciones en mina (router) y la interconexión desde el hub de Global Crossing al Centro de Control del COES. El ancho de banda será de 64Kbps.

3.4.4 Configuración de IEDs

La comunicación directa desde el centro de control con los IEDs de la SE Antamina para su configuración y monitoreo de información, mediante el software del fabricante, se realizará mediante dos Terminal Server con puertos seriales desde los cuales se formarán cuatro buses RS-485 que se conectarán a las interfaces seriales de todos los equipos de protección y medición de esta subestación.

3.4.5 Acceso Remoto

Se considera también un canal dial-up de acceso remoto al centro de control para el integrador del sistema, que le permita monitorear de manera remota el sistema SCADA. Para ello se instalará un switch telefónico que se conectará a cada una de las tarjetas módem de los servidores y en el otro extremo a un anexo de la central telefónica de Antamina.

3.5 Comunicaciones en Subestación Vizcarra

3.5.1 Entre Niveles IEDs - Subestación

La Subestación Vizcarra dispone de los siguientes IEDs y dispositivos de control:

- 03 relés ABB REL316, con interfaz de fibra óptica y protocolo SPA
- 03 relés ABB REL521, con interfaz de fibra óptica y protocolo SPA
- 03 relés ABB REL551, con interfaz de fibra óptica y protocolo SPA
- 04 medidores Electroindustries, con salida analógica de 4-20mA
- 01 sistema de control ABB del compensador de potencia reactiva (SVC)
- 04 medidores PML ION 7600, con una interfaz serial RS-232/RS-485 y una interfaz serial solo RS-485, con protocolos DNP3 y MODBUS

Los relés y medidores reciben la información de tensiones y corrientes del anillo y celdas de 220kV, a través de cableado físico, conectado directamente a los bornes específicos de estos IEDs. Con esta información, estos dispositivos realizan cálculos para obtener los demás valores analógicos (frecuencia, potencia, energía, etc.). Los relés realizan funciones de protección, de acuerdo a umbrales configurados por los operadores del sistema eléctrico. Las medidas eléctricas analógicas se obtendrán de las salidas 4-20 mA de los medidores Electroindustries mediante el cableado físico, conectado directamente a los bornes del módulo de entradas analógicas de un Concentrador de Datos en esta subestación.

Los estados de interruptores, seccionadores y algunas alarmas de esta subestación serán conectados desde sus contactos auxiliares hasta los bornes de los módulos de entradas digitales del Concentrador de Datos de esta subestación.

Las alarmas de protección se obtendrán de los 09 relés de protección ABB. Se utilizarán acopladores ópticos para la conexión de los relés, en topología estrella, cuya salida con interfaz RS-232 se conectará a un convertidor de protocolos (de SPA Serial a DNP3 sobre TCP/IP), que a su vez se conectará a una interfaz serial del Concentrador de Datos de múltiples puertos.

Se establecerá un bus RS-485 con los medidores ION 7600, que será conectado a otra interfaz serial del Concentrador de Datos, utilizando protocolo DNP3.

La integración del sistema de control ABB del SVC, se realizará instalando un gateway ABB GWS, que proporcionará una interfaz serial y protocolo DNP3, que se conectará a una interfaz serial del Concentrador de Datos.

3.5.2 Entre Niveles Subestación - Centro de Control

Desde el punto de vista operativo, la SE Antamina es una subestación principal y la SE Vizcarra una subestación secundaria. Por lo tanto, la SE Vizcarra no contará con interfaz de usuario. El equipamiento de comunicaciones existente en cada subestación comprendía equipos terminales de Onda Portadora ABB ETL500 que utilizaba la línea de transmisión L-2255 que unía ambas subestaciones para la teleprotección y comunicación de voz.

Debido a la dificultad de acceso a la SE Vizcarra y necesidad de reducir tiempos de implementación, se decidió utilizar los equipos terminales de Onda Portadora para integrar la información de la SE Vizcarra a la SE Antamina.

La información agrupada en el Concentrador de Datos de la SE Vizcarra, accederá a la red LAN TCP/IP redundante de la SE Antamina, para ser procesada por el Sistema SCADA Survalent utilizando protocolo DNP3 sobre TCP/IP. Para ello, en la SE Vizcarra

se conectará la interfaz serial RS-232 del Concentrador de Datos directamente a la interfaz serial RS-232 del Terminal de Onda Portadora en esta subestación. En el lado de la SE Antamina, se instalará un convertidor Serial a IP para llevar la interfaz serial RS-232 del Terminal de Onda Portadora de esta subestación a Ethernet y poder conectarlo al switch Ethernet de 24 puertos 10/100 Mbps de esta subestación.

3.6 Hardware del Sistema

3.6.1 Subestación Antamina

El hardware del Centro de Control en la subestación Antamina se compone de:

- Dos servidores de grado industrial
- Un monitor TFT LCD de 17" para la interfaz gráfica de usuario
- Una estación de operación con dos monitores TFT LCD de 20"
- Dos switches Ethernet administrables de 12 puertos 10/100 Mbps para establecer la red LAN redundante de la SE Antamina.
- Un Concentrador de Datos para agrupar la información de relés, medidores, dispositivos de control y demás IEDs. Cuenta con un módulo de entradas digitales para la conexión cableada de contactos de seccionadores e interruptores de potencia
- Dos relojes GPS con puerto IRIG-B para la sincronización de tiempo de los servidores a la unidad de referencia de tiempo GPS satelital
- Un switch Ethernet de 24 puertos 10/100 Mbps para la conexión del Concentrador de Datos, el convertidor serial a IP para el Terminal de Onda Portadora, los Terminal Servers y los dispositivos de control de los sistemas existentes
- Un convertidor serial a IP para convertir la interfaz RS-232 del equipo terminal de Onda Portadora de la SE Antamina a TCP/IP, conectado en el otro extremo de la línea de transmisión al Concentrador de Datos de la SE Vizcarra para la integración de su información
- Un sistema de alimentación ininterrumpida, como sistema de respaldo de energía de los equipos, con las baterías suficientes para dar una autonomía de una hora.
- Dos Terminal Servers para acceder a los puertos seriales RS-485 de los equipos de protección y medición desde la red LAN de la subestación para configuración y monitoreo de información con software del fabricante de los IEDs
- Un Switch KVM que permite utilizar un solo monitor, teclado y mouse para acceder a los servidores
- Un switch telefónico conectado a los modems de los servidores para acceso remoto del integrador del sistema

- Un tablero de dimensiones 2000 x 800 x 800 mm para albergar todos los equipos descritos anteriormente

La distribución de este hardware y del sistema de comunicaciones de esta subestación se muestra en el Anexo C.

3.6.2 Subestación Vizcarra

El hardware de la subestación Vizcarra se compone de:

- Un Concentrador de Datos para agrupar la información de relés y medidores. Esta información, luego es enviada a la SE Antamina mediante el sistema de Onda Portadora existente. Cuenta con dos módulos de entradas digitales, para la conexión cableada de contactos de seccionadores e interruptores de potencia, así como un módulo de entradas analógicas para la conexión de señales de 4 a 20mA (analógicas) de medidores.
- Tres convertidores de medios electro-ópticos para las interfaces de relés.
- Tres acopladores ópticos para la conexión de las interfaces ópticas de relés.
- Un convertidor de protocolos SPA Serial a DNP3 sobre TCP/IP que recibirá la información de los relés y la enviará al concentrador de datos.

Estos equipos serán instalados en un tablero existente. La distribución de este hardware y del sistema de comunicaciones de esta subestación se muestra en el Anexo C.

3.7 Presupuesto y Tiempo de Ejecución

El proyecto será ejecutado por subcontratación. El cuadro de costos del proyecto aprobado se detalla en la Tabla 3.1.

TABLA 3.1 Presupuesto del Proyecto

Ítem	Descripción	TOTAL (US\$)
1	COSTOS DE HARDWARE, SOFTWARE Y MATERIALES	
2	SERVICIO DE INSTALACION, MONTAJE Y TRANSPORTE	
3	PRUEBAS, PUESTA EN SERVICIO	
4	SERVICIO DE INGENIERIA BASICA E INGENIERIA DE DETALLE Gastos Generales + Utilidades (15%)	
		140,940

El monto indicado no incluye el Impuesto General a las Ventas (IGV) de 19%.

El tiempo de ejecución del proyecto será de 10 meses.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La integración de subestaciones con el uso de redes de área local (LAN) y dispositivos electrónicos inteligentes (IEDs), unidades terminales remotas (RTUs) o sistemas SCADA, pueden influir en la gama de oportunidades para que las empresas eléctricas desarrollen un plan de automatización de las subestaciones más completo.
2. La automatización, facilitada por un sistema de comunicaciones altamente disponible, reduce la frecuencia y duración de las interrupciones de energía. Las entidades eléctricas de infraestructura crítica están claramente motivadas por estos beneficios para hacer las inversiones financieras necesarias en comunicaciones y tecnologías de la información (TI) y esta tendencia continuará a un ritmo acelerado en el futuro inmediato.
3. Los datos de campo deberán ser adquiridos con dispositivos electrónicos inteligentes de última tecnología, es decir IEDs. Estos dispositivos deben presentar interfaces y protocolos de comunicación estandarizados. Entre los protocolos estándares deben constar el DNP3 y el IEC 61850. Además, la conexión en campo de estos dispositivos debe ser mediante una red de fibra óptica. Debe comprobarse que los datos sean adquiridos por estos equipos en tiempo real, y que la confiabilidad y seguridad de los datos cumplan con los requerimientos determinados en este estudio.
4. Los protocolos de comunicación entre los equipos de campo y el Centro de Control deben ser abiertos, a fin de que no exista la restricción de alguna marca específica de equipos. Entre los principales protocolos a considerar se tienen: IEC 61850, para la comunicación entre dentro de las subestaciones y el protocolo DNP3 para la comunicación entre los equipos de campo y la RTU. La comunicación entre centros de control se realizará mediante el protocolo abierto ICCP. Los sistemas de automatización de subestaciones deben estar adaptados para poder operar en un

futuro protocolos estándares de arquitectura abierta más avanzados y actualizados, como el IEC 61850.

5. Los sistemas de comunicación deben exhibir una alta disponibilidad, mayor de 99.9% sobre cualquier período de un año, así como, los sistemas de automatización e incluso los dispositivos individuales, incluyendo procesadores, a fin de conseguir los beneficios esperados.
6. La arquitectura básica de los componentes del sistema de automatización, como son las redes LAN, servidores, consolas, medios de comunicación y dispositivos periféricos, debe ser redundante y distribuida, a fin de elevar los niveles de confiabilidad y desempeño del sistema.
7. El centro de control básicamente estará compuesto por el sistema SCADA y las funciones de medición, control y monitoreo, que a su vez cuentan con diferentes aplicaciones.
8. La implementación del proyecto de Antamina permitirá obtener beneficios técnicos como:
 - a) La disponibilidad de mayor información que permita reestructurar los métodos y procedimientos de la operación de las subestaciones, obteniendo menores costos de operación, reduciendo tiempos y evitando el traslado del personal a campo.
 - b) La sistematización de los procedimientos operativos de Antamina.
 - c) El mejoramiento del nivel de acción frente a fallas, reduciendo los tiempos de reposición, ya que se puede localizar en un menor tiempo los elementos que operaron y la causa de las fallas.
 - d) El desarrollo de nuevas aplicaciones para mejorar constantemente los procesos técnicos – administrativos de conformidad a los requerimientos de la empresa.
 - e) El envío de las señales hacia el centro de control del COES SINAC y de esta manera cumplir con la regulación establecida para los operadores independientes.
 - f) Si bien el sistema no contará con un sistema de almacenamiento y recuperación de información, basado en un sistema de bases de datos relacionales que permita a los operadores almacenar y acceder a la

información de todos los componentes del sistema de una forma eficaz y eficiente, se tendrá el registro de eventos en los servidores SCADA, quedando listo cuando se implemente servidores de bases de datos históricos para un análisis post-operativo de la gestión.

- g) La entrega de información oportuna, confiable y completa en tiempo real de los sucesos operativos que ocurren en las subestaciones.

- 9. El presupuesto del proyecto considera diferentes servicios, incluyendo instalación, pruebas y capacitación.

RECOMENDACIONES

En base al proyecto de Antamina, se hacen las siguientes recomendaciones:

1. Se recomienda reemplazar los relés de protección de las subestaciones, con interfaces seriales, por IEDs inteligentes con interfaces de red, o en su defecto instalar convertidores de medios o Terminal Servers para poderlos integrar a una red.
2. Se recomienda que los equipos que se van en el sistema de automatización presenten protocolos de comunicación abiertos, a fin de que el sistema no se encuentre ligado a una marca específica.
3. Se recomienda, además en la parte del software utilitario, emplear paquetes computacionales de Microsoft, debido a su manejo fácil e interfaz humano máquina amigable.
4. Es recomendable que la redundancia del sistema de comunicaciones y de los componentes del sistema de automatización, sea lo suficientemente adecuada para cumplir con los requerimientos de disponibilidad, desempeño y funcionalidad establecidos.
5. Una parte muy importante de la implementación de nuevas tecnologías, como es el caso de los sistemas de automatización y centros de control, es la capacitación del personal que permita el aprovechamiento de los beneficios mediante un incremento del nivel de ingeniería y tecnología del personal de la empresa.

ANEXO A
COMPARACIÓN ENTRE ESTÁNDARES DNP3 E IEC 61850

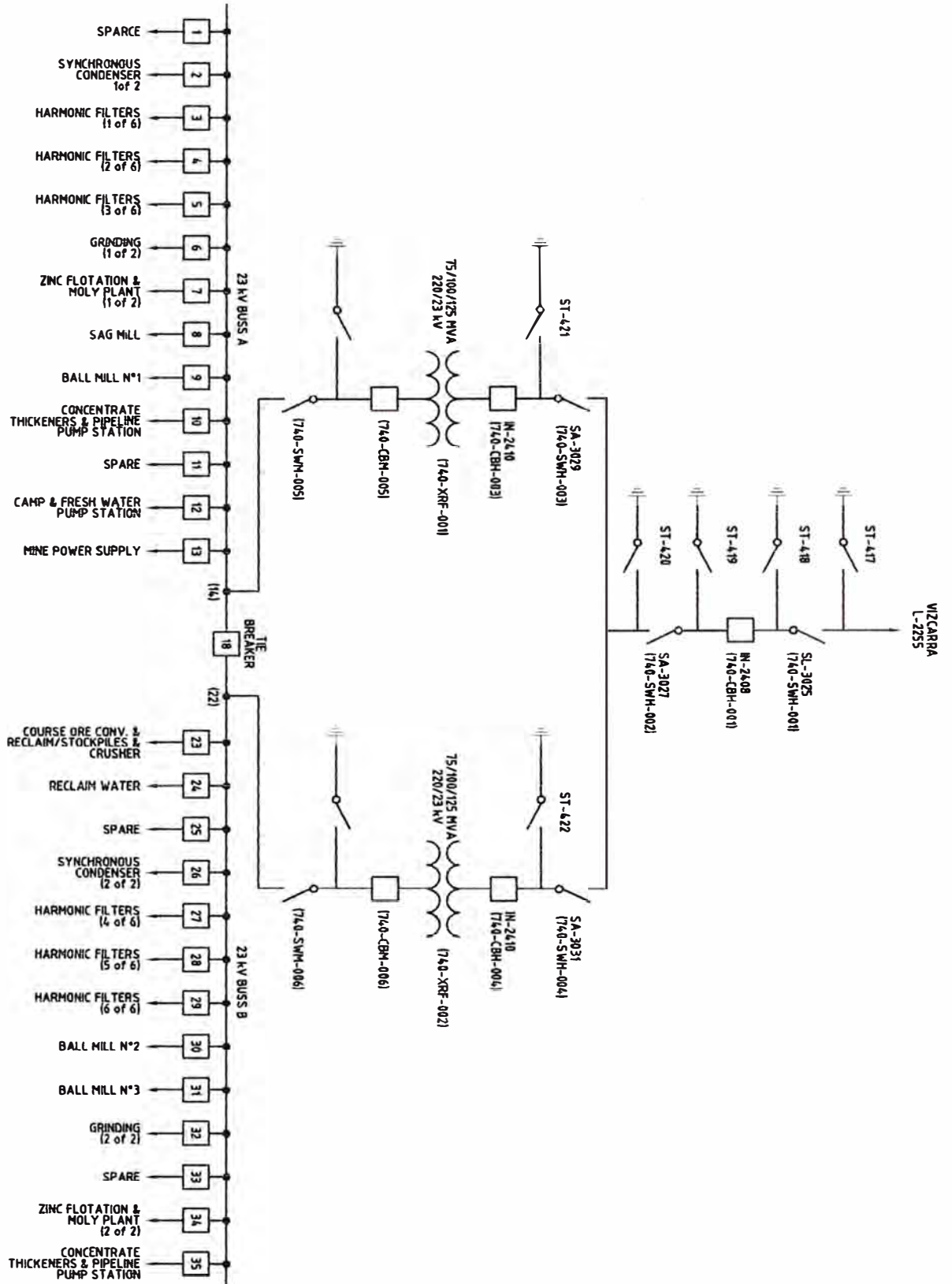
COMPARACIÓN ENTRE ESTÁNDARES DNP3 E IEC 61850

ITEM	DNP3	IEC 61850
Disponibilidad del producto	Soportado por la mayoría de los fabricantes de IEDs para empresas eléctricas	Varios líderes en la fabricación de IEDs relés de protección ofrecen actualmente productos basados en IEC 61850: ABB, Areva, GE, SEL y Siemens.
Aplicación en empresas eléctricas	Estándar de facto para interactuar con IEDs de subestación. Ampliamente utilizado en proyectos de automatización de subestaciones	Número creciente de proyectos en curso, en empresas eléctricas, como proyectos pilotos o estandarizado en nuevas instalaciones.
Idoneidad para aplicaciones distribuidas de protección (basadas en red)	Desarrollado como un protocolo Maestro - Esclavo para la adquisición de datos y control de sistemas eléctricos. No está diseñado para aplicaciones de protección peer-to-peer de alta velocidad.	Diseñado para manejar comunicaciones peer-to-peer de alta velocidad utilizando mensajes GOOSE o GSSE. Los métodos de multicasting y suscripción, definidos en el protocolo, proporcionan la entrega oportuna de la información de cambio de estados y datos analógicos.
Configuración de IEDs	No está diseñado para soportar la configuración de relés de protección con cientos de seteos, ni para representar adecuadamente la jerarquía funcional de múltiples capas de tales dispositivos. Sin embargo, soporta la transferencia de archivos, que permite la carga y descarga de archivos de configuración entre la estación de ingeniería y el IED de protección.	Está diseñado para soportar la configuración de relés basada en los modelos de objeto de funciones de protección y funciones relacionadas. El estándar requiere archivos de configuración de dispositivos en Lenguaje de Configuración de Subestaciones (SCL). Estos archivos son proporcionados por los proveedores de IEDs.
Análisis de operación del relés	Soporta transferencia de archivos, por tanto puede ser utilizado para recuperar registros de formas de onda guardados como un archivo o conjunto de archivos (según las especificaciones de COMTRADE).	Soporta transferencia de archivos, por tanto puede ser utilizado para recuperar registros de formas de onda guardados como un archivo o conjunto de archivos (según las especificaciones de COMTRADE).
Control	Las funciones de control se basan en tres modelos: <ul style="list-style-type: none"> • Operación directa no reconocida, permite broadcasting de control a múltiples IEDs • Operación directa reconocida, control de 1 paso con feedback de aceptación de control • Selección antes de operación, control de 2 pasos con feedback de aceptación de control. No especifica las acciones adoptadas en la recepción de las operaciones de control. 	Define un modelo de Control que incluye una especificación de servicios y comportamiento. Los datos que proporcionan atributos de control son: <ul style="list-style-type: none"> • Punto simple de control (SPC) • Punto doble de control (DPC) • Estado entero de control (ISC) • Información de posición de paso controlado binario (BSC) • Información de posición de paso controlado entero (TSI) • Punto de ajuste analógico de control (APC)

ITEM	DNP3	IEC 61850
Medidas	<p>Las medidas están disponibles mediante objetos de entrada analógica y contadores (acumuladores). Cada IED mapea las diferentes medidas en números de índice de punto no estructurado, de manera específica por proveedor. Las entradas analógicas representan cualquier tipo de valor continuo y pueden ser reportadas en formato entero o de coma flotante. Los contadores representan valores incrementándose monótonamente (tales como contadores de operación y valores de energía) y son reportados como enteros.</p>	<p>Define diferentes clases de datos comunes para la información de medidas, por ejemplo:</p> <ul style="list-style-type: none"> • Valor medido (MV) • Valor medido complejo (CMV) • Valor muestreado (SAV) • WYE • Delta (DEL) • Secuencia (SEQ) • Valor armónico (HMY) • Valor armónico para WYE (HWYE) • Valor armónico para Delta (HDEL)
Configuración de usuario de subestación	<p>La configuración del usuario de subestación, en el caso de servidores de datos con protocolo DNP3, es mediante un proceso de ingreso manual de datos</p>	<p>Desarrollado para permitir la eliminación de configuración manual del usuario de subestación. El concepto implementado de "descripción automática" ofrece al usuario la posibilidad de leer el modelo de objeto de cada servidor basado en IEC 61850, identificar los objetos de datos que tienen que ser mapeados a la base de datos de la subestación (basado en sus nombres estándares), y mapear estos objetos de datos a la base de datos.</p>

ANEXO B
DIAGRAMAS UNIFILARES DE SUBESTACIONES DE ANTAMINA

DIAGRAMA UNIFILAR SUBESTACION ANTANIMA 220/23 KV



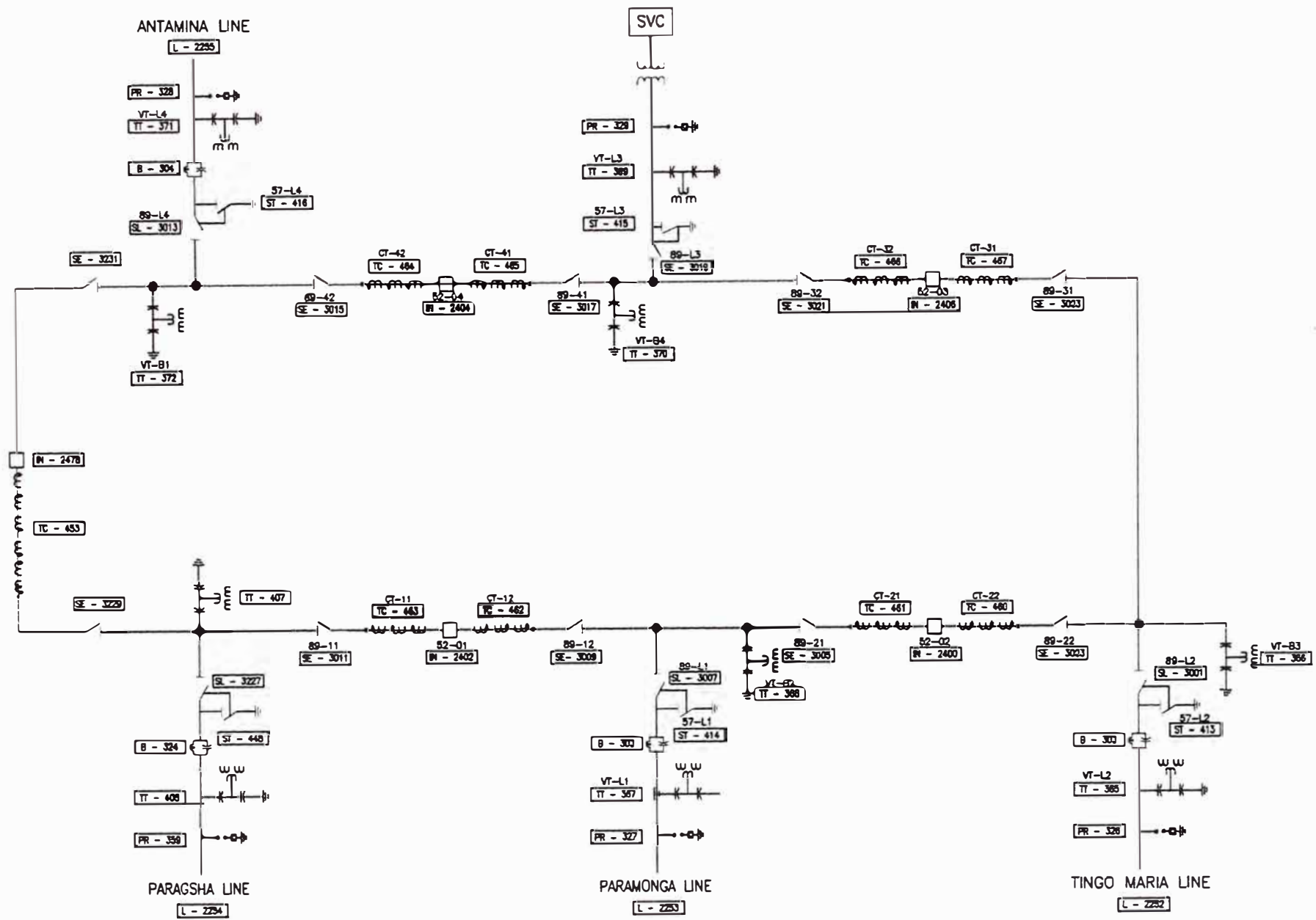
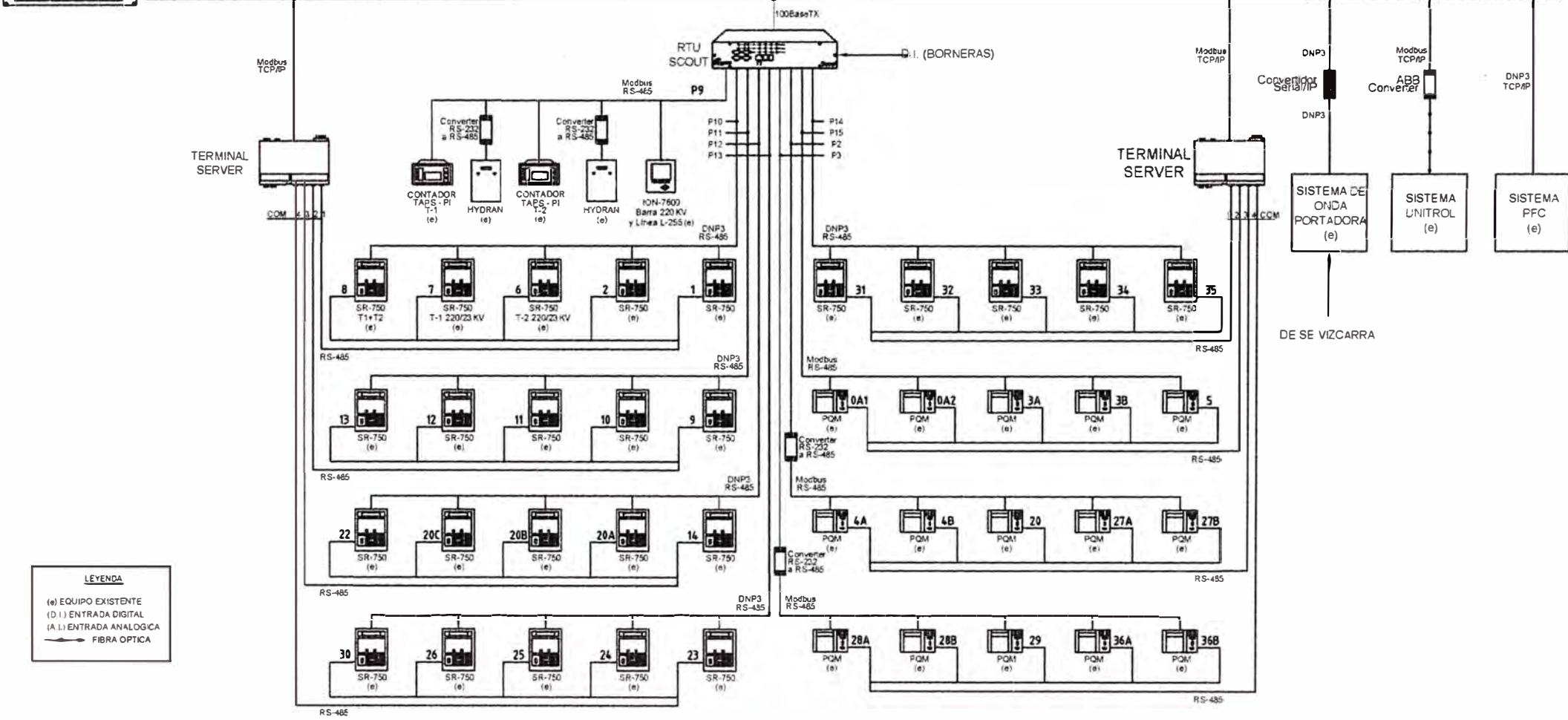
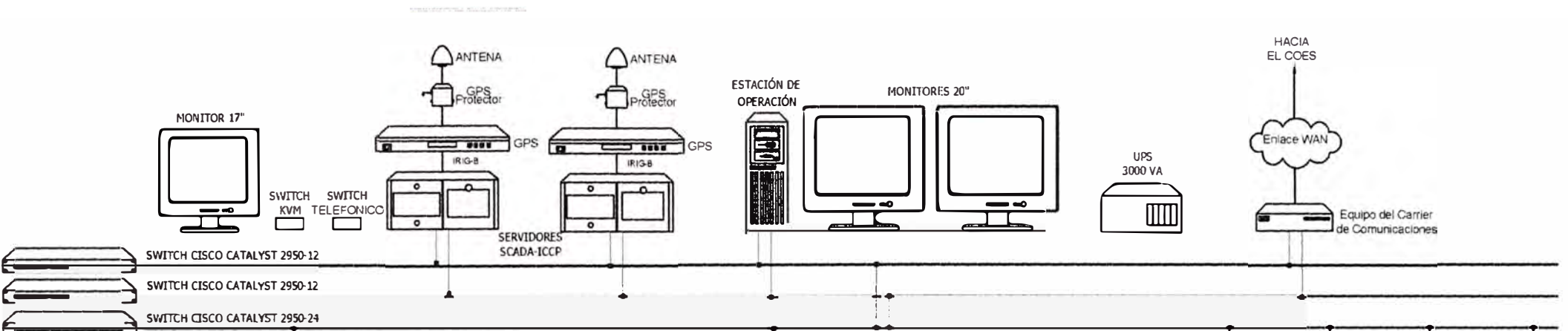


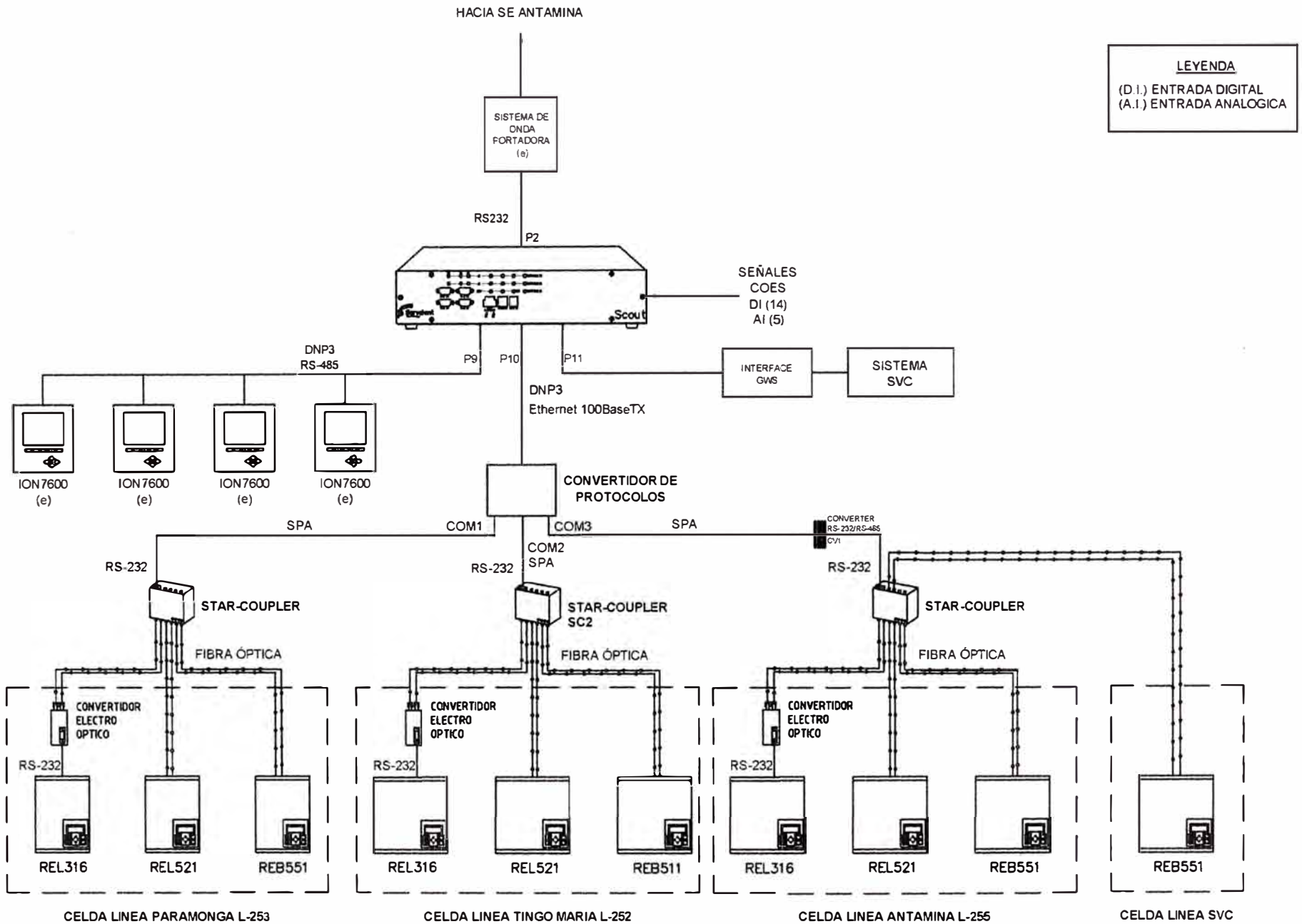
DIAGRAMA UNIFILAR SUBESTACION VIZCARRA 220kV

ANEXO C
DISTRIBUCIÓN DE HARDWARE Y SISTEMA DE COMUNICACIONES



LEYENDA
 (e) EQUIPO EXISTENTE
 (D.I.) ENTRADA DIGITAL
 (A.L.) ENTRADA ANALÓGICA
 — FIBRA OPTICA

DISTRIBUCIÓN DE HARDWARE Y SISTEMA DE COMUNICACIONES EN SUBESTACIÓN ANTIMINA



DISTRIBUCIÓN DE HARDWARE Y SISTEMA DE COMUNICACIONES EN SUBESTACIÓN VIZCARRA

BIBLIOGRAFIA

1. Norma DGE (Dirección General de Electricidad), Parte I: Generación, Transmisión, Distribución, Utilización y Tarificación de la Electricidad. Sección 6 Subestaciones. "Terminología en Electricidad", Perú
2. Jhon D. McDonald, "Electric Power Substations Engineering", CRC Press, Estados Unidos, 2003
3. Alex Apostolov, Michael Dood, and John Tengdin, "Developing IEEE 1613 Standards for Communications Network in Substations", IEEE Power and Energy Magazine, 2004
4. Manuel Jiménez Buendía, "Comunicaciones Industriales", Universidad Politécnica de Cartagena, Departamento de Tecnología Electrónica
5. IEEE Power Engineering Society, "IEEE Standard for SCADA and Automation Ssystems IEEE Std C37.1-2007", Nueva York (USA), 2008
6. J.Martin-Giraldo, "La FERC Aprueba las Nuevas Normas de Fiabilidad para la Seguridad Informática de las Redes Eléctricas", Blog de Internet: Power Encounter (<http://powerencounter.blogspot.com>), Febrero 2008
7. Organismo Supervisor de la Inversión en Energía (OSINERG), "Reporte Estadístico del Mercado Libre de Electricidad", Año 1 N° 1 Julio 2001
8. Página Web de Antamina: <http://www.antamina.com/>
9. Página Web del Grupo Energético Aguaytia: <http://www.aguaytia.com/>
10. Página Web de la empresa de ingeniería de consulta Cesel S.A.: http://www.cesel.com.pe/mineria_hidrocarburos/equipamiento_minero_1.htm
11. Fabián Mauricio Calero Freire, "Estudio Técnico-Económico de la Implementación del Centro de Control de las Centrales Hidroeléctricas Illuchi 1 E Illuhi 2 de ELEPCO S.A.", Proyecto Previo a la Obtención del Título de Ingeniero Eléctrico, Escuela Politécnica Nacional, Quito – Ecuador, 2007