UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DE ADQUISICIÓN DE INFORMACIÓN EN TIEMPO REAL DEL SISTEMA ELECTRICO INTERCONECTADO NACIONAL DEL ORGANISMO REGULADOR DEL SECTOR ENERGÍA

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRICISTA

PRESENTADO POR:

RUBEN ROJAS RAMÍREZ

PROMOCIÓN
1996 – II
LIMA – PERÚ
2006

SISTEMA DE ADQUISICIÓN DE INFORMACIÓN EN TIEMPO REAL DEL SISTEMA ELÉCTRICO INTERCONECTADO NACIONAL DEL ORGANÍSMO REGULADOR DEL SECTOR ENERGÍA

En agradecimiento a mis padres y hermanos por la educación adquirida, a mis amigos por el apoyo incondicional.

SUMARIO

El presente trabajo recopila información de normas y documentos relacionados con la transferencia de información en tiempo real entre centros de control del sector eléctrico peruano, asimismo información obtenida de la implementación de sistemas SCADA, así como la implementación del sistema de monitoreo en tiempo real del Organismo Regulador del Sector Energía, también acopia información de Seminarios, Conferencias, Revistas, Papers, Catálogos, Internet relacionadas con los sistemas SCADA, así como la experiencia personal en estos temas y la Operación del Sistema Eléctrico Interconectado Nacional, con la finalidad de presentar el trabajo efectuado para dotar al Organismo Regulador del Sector Energía de un Sistema de Adquisición de Información en Tiempo Real del Sistema Eléctrico Interconectado Nacional

ÍNDICE

CAPITULO III

FUNCIONALIDAD DEL SISTEMA SCADA DEL COORDINADOR DEL SEIN

ANEXO B
APLICACIONES DEL SISTEMA DE MONITOREO EN TIEMPO REAL DEL REGULADOR

BIBLIOGRAFIA

PROLOGO

El presente trabajo de ingeniería ha sido elaborado para identificar y describir las actividades a desarrollar para dotar al Organismo Regulador del Sector Energía (en adelante el Regulador) de un sistema de adquisición de información en tiempo real del Sistema Eléctrico Interconectado Nacional, (en adelante SEIN).

En el primer capítulo se analiza los requerimientos de información del Regulador, y las alternativas que se tienen para obtener información desde el Coordinador de la Operación en Tiempo Real del SEIN (en adelante el Coordinador), considerándose para ello el marco legal para la transferencia de información en tiempo real entre centros de control del SEIN.

En el segundo capítulo se describe el principio de funcionamiento de los sistemas SCADA, incidiéndose básicamente en el relacionado con los sistemas SCADA para empresas eléctricas.

En el tercer capítulo se muestra la funcionalidad del sistema SCADA del Coordinador.

En el cuarto capítulo se desarrolla la parte principal del presente trabajo, se describe el equipamiento e ingeniería necesarios para implementar el sistema SCADA del Regulador y las aplicaciones del mismo.

Finalmente, se desarrolla las conclusiones del trabajo donde se resume los principales análisis, diagnósticos y propuestas.

Antecedentes

En conformidad con lo establecido por la Ley de Concesiones Eléctricas (LCE) corresponde al Regulador supervisar el cumplimiento de la normatividad que garantiza la calidad, confiabilidad y eficiencia en la prestación del servicio público de electricidad, así como supervisar el cumplimiento de las obligaciones contraídas por los concesionarios en los contratos de concesión eléctrica.

La información de tiempo real remitida desde los centros de control de las empresas integrantes del sistema es de suma importancia, para que el Coordinador disponga de información confiable, para que tome correctas decisiones. En la actualidad mucha de la información que reportan las empresas no cumplen con los requerimientos establecidos por el Coordinador, adicionalmente se percibe que parte de la información enviada no es actualizada en la periodicidad requerida o existe información enviada en forma incorrecta en calidad y/o valor.

Asimismo, el Regulador requiere procesar en tiempo rea, cierta información del SEIN, para obtener indicadores que permitan evaluar de manera transparente el estado operativo del mismo.

Objetivo

En ese sentido se requiere dotar al Organismo Regulador del Sector Energía de un sistema de información en tiempo real, que permita obtener información en tiempo real desde el sistema SCADA del Coordinador, para lo cual se evaluarán alternativas que permitan obtener un diagnóstico para lograr la transferencia de información en tiempo real de la operación del SEIN, detallándose el equipamiento y el trabajo de ingeniería necesario para la implementación del Sistema SCADA requerido.

Alcances

El presente trabajo de ingeniería pretende identificar y analizar las alternativas para que el Regulador pueda disponer de un sistema de adquisición de información en tiempo real del estado operativo del SEIN.

Para ello los alcances planteados en el presente trabajo son los siguientes:

- Análisis del requerimiento de un sistema de monitoreo en tiempo real del Regulador.
- Descripción de un sistema de adquisición de datos en tiempo real (SCADA).
- Descripción de las funcionalidades del Sistema SCADA del Coordinador del SEIN.
- Análisis y propuesta de equipamiento e ingeniería necesaria para implementar el sistema SCADA del Regulador.

CAPITULO I

REQUERIMIENTO DE UN SISTEMA DE MONITOREO EN TIEMPO REAL DEL ORGANISMO REGULADOR DEL SECTOR ENERGIA

1.1 Requerimiento de información del Regulador

El Comité de Operación Económica del Sistema (COES-SINAC) es el organismo técnico responsable de la programación y operación a corto plazo del SEIN. Asimismo, es responsable de coordinar la operación en tiempo real del SEIN de conformidad con el Artículo 92° del Reglamento de la LCE.

El Regulador dentro de las funciones que le corresponden requiere evaluar la información utilizada por el COES-SINAC para el cumplimiento de sus funciones y verificar la calidad de datos que las empresas integrantes del COES entregan al Coordinador, con lo finalidad de que la operación se realice a mínimo costo bajo criterios de seguridad y de calidad del servicio.

Para obtener acceso a la información operativa del Coordinador, que permita conocer la situación en tiempo real del SEIN la cual esta conformada por los estados operativos de las instalaciones de unidades de generación, instalaciones de transmisión y de cierto nivel de distribución, así como para contribuir con los principios de transparencia del sector, se requiere tener acceso al SCADA del Coordinador a través de la implementación de un Sistema de Monitoreo en Tiempo Real (SMTR), que implica la adquisición del equipamiento necesario, así como realizar la respectiva instalación y configuración y enlace con el centro de control del Coordinador.

1.2 Marco legal para la transferencia de información entre centros de control del SEIN

El Regulador tiene la función de supervisar que la operación del Sistema se realice al mínimo costo, bajo criterios de seguridad y de calidad del servicio, y con transparencia de toda la información relacionada con el despacho y operación del Sistema.

En el artículo 92º del Reglamento de la Ley de Concesiones Eléctricas (en adelante RLCE), se establece que la operación en tiempo real de las unidades generadoras, de los sistemas de transmisión, de distribución y de los clientes libres del SEIN es efectuada directamente por sus titulares, bajo su propia responsabilidad, y el COES-SINAC es el encargado de Coordinar la operación del conjunto de instalaciones, de tal manera que la operación sea económica, segura y confiable. Dicha operación se hace ciñéndose a los programas establecidos por la Dirección de Operaciones, siendo de cumplimiento obligatorio para todos los Integrantes del Sistema (se entiende por Integrante del Sistema a las entidades que conforman el COES-SINAC, a las distribuidoras, a los clientes libres y a los generadores no integrantes del COES-SINAC pero que están interconectados eléctricamente).

La coordinación de la operación en tiempo real del SEIN es efectuada por el COES-SINAC en representación de los Integrantes del Sistema, en calidad de "Coordinador de la Operación en Tiempo Real del Sistema", para lo cual contará con el equipamiento necesario para el cumplimiento de sus funciones.

El Coordinador, en resguardo de la calidad y seguridad del sistema eléctrico, debe supervisar y controlar el suministro de electricidad. Para el cumplimiento de estas funciones los Integrantes del Sistema deben proporcionar al Coordinador la información requerida por éste.

Asimismo, de acuerdo a lo indicado en el numeral 1.4 de la Norma Técnica para la Coordinación de la Operación en Tiempo Real (en adelante NTCOTR), cada Integrante del Sistema debe contar necesariamente con un Centro de Control para la operación en tiempo real de sus instalaciones; así como, esta obligado a cumplir las disposiciones del Coordinador y contar con los recursos humanos y materiales necesarios para operar físicamente sus instalaciones, adquirir automáticamente información de su Sistema, coordinar e intercambiar información en tiempo real con el Coordinador. Los distribuidores y clientes libres con una demanda total menor o igual a 30 MW y titulares de generación con centrales cuya suma total de potencias efectivas sea menor o igual a 10 MW no están obligados a contar con un Centro de Control, pero deben contar durante las 24 horas del día con un supervisor responsable de la operación de sus instalaciones.

En el numeral 1.5 de la NTCOTR se establece cual debe ser la infraestructura necesaria para la coordinación del SEIN. Así mismo, se establece que el Coordinador

debe contar con sistemas y equipos adecuados que permitan y faciliten la transmisión y recepción en tiempo real de todo tipo de información durante las 24 horas de todos los días del año con los Integrantes del Sistema. Para tal fin, cada uno de los Integrantes del Sistema se mantendrá enlazado con el Coordinador a través de un sistema de comunicación confiable y compatible.

Por otro lado se indica que el Coordinador es el encargado de determinar el protocolo de comunicaciones entre el Centro de Control del Coordinador y los Centros de Control de los Integrantes del Sistema, basado en normas internacionales, e indicar las especificaciones técnicas mínimas de este protocolo para todos los Centros de Control. Asimismo, establece los requisitos mínimos de calidad y condiciones para el intercambio de información en tiempo real que requiera, especialmente en cuanto a calidad de las medidas y estados, sincronización horaria de las mismas, señalización horaria de los cambios de estado, entre otros, que considere necesarios por su importancia, lo cual será de cumplimiento obligatorio. Por otro lado, el Coordinador dispone las topologías de comunicación técnicamente más adecuadas, bajo criterios uniformes para todos los integrantes, y debe contar con programas de aplicación en línea para evaluar la seguridad operativa del Sistema, tales como Estimador de Estado, Flujo de Carga en Línea, Análisis de Contingencias, Pronóstico de Demanda, Control Automático de generación y otros que considere necesarios.

En el manual para el intercambio de información entre el Coordinador y los integrantes del SEIN, se define la "Red ICCP del SEIN" (en adelante RIS), la cual es una red de intercambio de datos operativos en tiempo real entre el Coordinador y las empresas integrantes del SEIN.

Los integrantes de la RIS actúan como proveedores de datos del Coordinador, a través de sus centros de control. Las comunicaciones deben ser siempre entre la empresa propietaria de los equipos monitoreados y el Coordinador, aun cuando la empresa propietaria remita sus señales a través de una tercera empresa.

1.3 Tipo de información que el Coordinador requiere de los Integrantes del Sistema

Los titulares de generación que operen conectados al SEIN deben presentar al Coordinador en tiempo real y en la forma que éste establezca, la siguiente información:

- La posición de los interruptores;
- La posición de los seccionadores;

- En caso de centrales hidroeléctricas, los caudales, el nivel y volumen de los embalses;
- En caso de centrales térmicas, el combustible almacenado;
- Los niveles de tensión en bornes de generación y en barras;
- La frecuencia en las barras de generación;
- Las potencias activa y reactiva de cada generador y transformador;
- Las señales con niveles de alarma grave de centrales, subestaciones, generadores y transformadores de manera centralizada por equipo, así como las señales con niveles de alarma leve que defina el Coordinador ;
- La información técnica adicional que el Coordinador requiera.

La presentación de la información no es obligatoria para los titulares de generación que no superen los diez (10) MW de potencia efectiva; sin embargo, aquellos que sean requeridos por el Coordinador están obligados a:

- Disponer de un medio de comunicación principal, como mínimo el de la red de telefonía pública, y un medio de respaldo compatible con el del Coordinador;
- Informar periódicamente a requerimiento del Coordinador las magnitudes de potencia activa, potencia reactiva y tensión de cada unidad de generación de la central, por medio magnético en el formato que el Coordinador defina;
- Transmitir información inmediatamente después de la ocurrencia de algún evento de cualquier unidad de generación o equipo de la central;
- Entregar la información técnica adicional que el Coordinador requiera.

Los titulares de transmisión con niveles de tensión iguales o superiores a 100 kV deben presentar al Coordinador, en tiempo real y en la forma que éste establezca, la siguiente información:

- La posición de los interruptores;
- La posición de los seccionadores;
- La posición de los gradines de los transformadores con conmutadores de toma bajo carga;
- Los niveles de tensión de barra;
- Las potencias activa y reactiva de las líneas y transformadores;
- La potencia reactiva de equipos de compensación reactiva inductiva/capacitiva;
- Las señales de alarma de subestaciones, líneas, transformadores y equipos de compensación reactiva de manera centralizada por equipo;
- La información técnica adicional que el Coordinador requiera.

Tratándose de redes de transmisión con niveles de tensión inferiores a 100 kV, el Coordinador solicita la correspondiente información que le permita efectuar adecuadamente la coordinación de la operación en tiempo real del Sistema.

Los titulares de redes de distribución y los clientes libres presentan al Coordinador, en tiempo real y en la forma que éste establezca, la información sobre la operación de sus instalaciones que, a criterio del Coordinador, pueda afectar la calidad del servicio o la seguridad del Sistema.

Para llevar a cabo la transferencia de información, los Integrantes del Sistema deben enlazar sus respectivos Centros de Control a través de un sistema de comunicaciones confiable y compatible con el Centro de Control del Coordinador.

El Coordinador establece la referencia horaria para el registro de todos los eventos y actividades vinculadas con la Operación en Tiempo Real del Sistema utilizando información de tipo satelital. Los Integrantes del Sistema están obligados a usar esta referencia.

1.4 Información que el Coordinador pondrá a disposición de los integrantes del Sistema.

Periódicamente el Coordinador pondrá a disposición de los Integrantes del Sistema la siguiente información:

- El despacho real de las unidades de generación: potencia activa y reactiva;
- Los costos marginales, costos diarios de operación/racionamiento del Sistema;
- Las perturbaciones ocurridas;
- Las horas de salida y reconexión de equipos por mantenimiento/falla;
- Las horas de orden de arranque/parada y las de ingreso/salida de unidades;
- Las disposiciones de reprogramación de la operación del sistema;
- Las disposiciones de regulación de tensión, frecuencia y otros;
- Los registros de frecuencia y tensión;
- La información técnica adicional que los Integrantes del Sistema requieran para evaluar la operación del Sistema.

El Coordinador retransmitirá en tiempo real a los integrantes del Sistema que lo soliciten, la información de la operación en tiempo real que cada uno considere necesaria, y sólo a aquellos Integrantes que hayan cumplido con enviar el total de sus señales requerida por el Coordinador.

1.5 Análisis de alternativas para la transferencia de información en tiempo real

Los sistemas SCADA de centros de control de energía cumplen con estándares y que permiten a los usuarios acceso y administración de la base de datos en tiempo real e históricos, son escalables, extremadamente flexibles a los requerimientos de los usuarios así como permiten el diagnóstico de la red y datos e incluyen subsistemas para el manejo de situaciones críticas.

Con la finalidad de que Regulador pueda contar con un sistema SCADA que le permita fortalecer el cumplimiento de sus funciones de fiscalización se plantea las siguientes alternativas:

- Sistema de Monitoreo en Tiempo Real propio (SCADA propio)
- Sistema de Monitoreo en Tiempo Real con software del COES-SINAC (software SCADA del COES-SINAC)
- Estación de trabajo extendida de la red LAN del COES

1.5.1 Sistema de Monitoreo en Tiempo Real con software SCADA propio

Consiste de un Sistema SCADA con opciones básicas y con características funcionales similares a los Centros de Control de las empresas integrantes del COES-SINAC.

Ventajas

- Sistema ICCP (Cliente /Servidor) abierto, estándar e independiente de cambios en el COES-SINAC
- Interfases con el usuario y crecimiento futuro acorde con las necesidades propias.
- Bases de Datos Históricas propias e independientes.
- Desarrollo de múltiples aplicaciones orientadas a tareas específicas de fiscalización.
- Facilidad y Flexibilidad de fiscalizar a los agentes integrantes de COES-SINAC directamente en puntos estratégicos (a través de Protocolo ICCP u Protocolos de Telemetría tales como DNP3, IEC).
- Capacidad de instalar programas de gestión y análisis de redes eléctricas con fines de contraste de datos y resultados
- Inversión Escalable, inicialmente aplicación Básica de SCADA + ICCP, y sobre el mismo software capacidad modular para crecer en ambiente totalmente gráfico, manejo de topología geográfica, módulos de reportes y conteo de operación de interruptores, SCADA Web Server, etc.

- Manejo ilimitado en asignación de usuarios, enlaces ICCP, pantallas gráficas y desarrollos propios respecto a publicaciones de datos que puedan ser llevados en tiempo real a aplicaciones Intranet e Internet.

Costo inicial

Se estima un costo aproximado de US$ 123 000 (ciento veinte tres mil dólares estadounidenses).

- Hardware de la Estación de Trabajo.
- Hardware del servidor de la sistema SCADA, Base de Datos e ICCP.
- Software del sistema operativo del servidor.
- Software del sistema operativo de la estación de trabajo.
- Software del sistema SCADA Básico + ICCP.
- Software de Base de Datos (Oracle o similar).
- Ingeniería para el Desarrollo de la aplicación.

Costos operativos

- Mantenimiento de Hardware.
- Uso de línea de comunicación dedicada.

En la Figura Nº 1.1 se muestra la configuración propuesta.

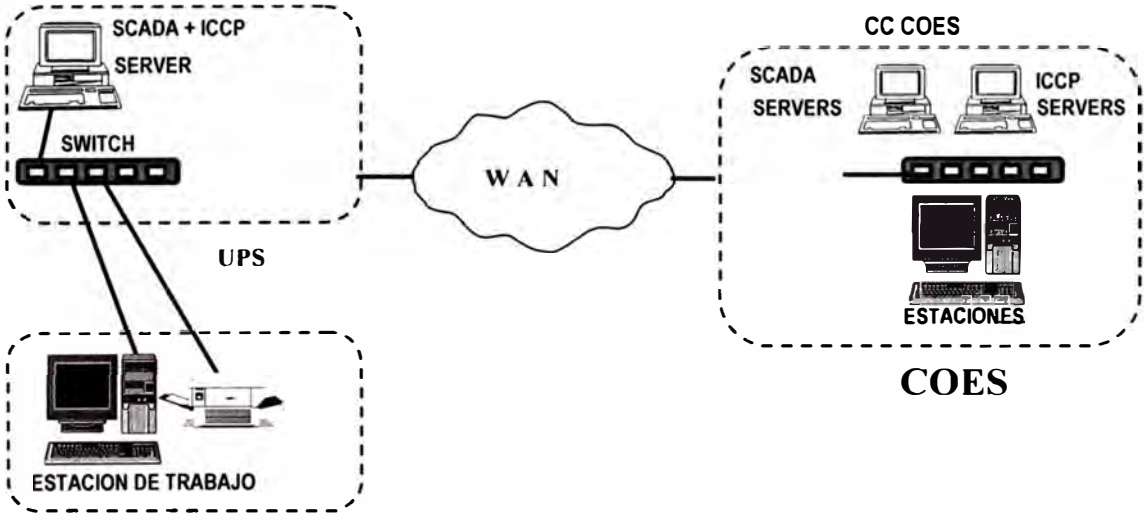


Figura Nº 1.1 : Configuración del Sistema de Monitoreo en Tiempo Real con software SCADA propio

1.5.2 Sistema de Monitoreo en Tiempo Real con software SCADA del COES-SINAC

Consiste en instalar en el Regulador el paquete del sistema SCADA y subsistemas que actualmente el COES-SINAC tiene instalado en su Centro de Control, con la finalidad de que el Regulador disponga de una estación de trabajo en tiempo real con características funcionales similares a los Centros de Control de las empresas integrantes del COES-SINAC.

Ventajas

- Menor costo del Software SCADA y subsistemas que han sido desarrollados por el COES-SINAC, sin embargo no son productos comerciales ni cuentan con una óptima interfaz hombre máquina.
- Interfaces gráficas del SEIN ya implementadas por el COES-SINAC.

Desventajas

Considerando que el software SCADA es de desarrollo propio del COES-SINAC no existe el marco legal que permita que nos puedan proporcionar la licencia de su software SCADA y de su protocolo ICCP. Cabe indicar que el software SCADA desarrollado por el COES-SINAC no es un producto comercial que sea difundido y probado mundialmente, sino es un desarrollo propio al cual se esta continuamente probando y añadiendo funciones y no se descarta la posibilidad que en un futuro opten por adquirir un sistema SCADA de reconocido prestigio mundial, lo cual complicaría mucho más que proporcionen una licencia SCADA al Regulador.

Adicionalmente se pueden notar las siguientes desventajas:

- Interfaces definidas por el coordinador de acuerdo a sus propias necesidades.
- Soporte del software online que estará a cargo del Coordinador.
- Cambios y actualizaciones supeditadas al COES-SINAC.
- Rigidez en el desarrollo de aplicaciones en reportes específicos y futuras.
- La orientación del desarrollo de las aplicaciones son propias de las necesidades del COES-SINAC.

Costo inicial

Se estima un costo aproximado de US$ 85000 (ochenta y cinco mil dólares estadounidenses).

- Hardware de la Estación de Trabajo.
- Hardware del servidor del sistema.
- Hardware del servidor ICCP (licencia).
- Software del sistema operativo del servidor del sistema.
- Software del sistema operativo del servidor del ICCP.
- Software del sistema operativo de la estación de trabajo.
- Software ICCP.
- Software de Base de Datos (Oracle o similar).

Costos operativos

- Mantenimiento de Hardware.
- Uso de línea de comunicación dedicada.

En la Figura Nº 1.2 se muestra la configuración propuesta.

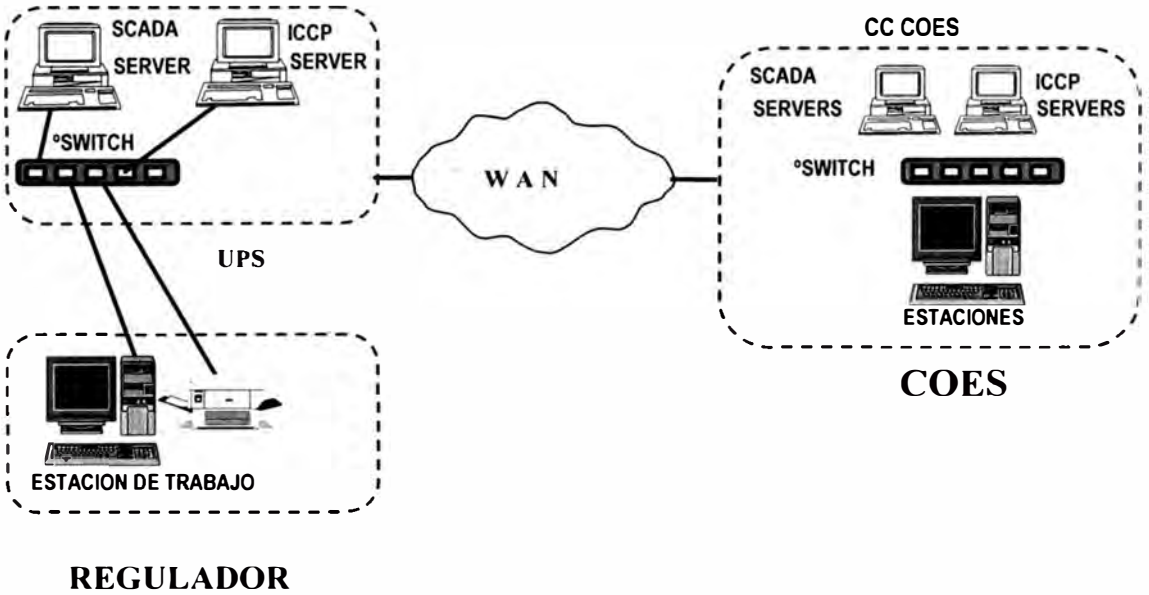


Figura Nº 1.2 : Configuración del Sistema de Monitoreo en Tiempo Real con software SCADA del COES-SINAC

1.5.3 Estación de trabajo extendida de la red LAN del COES-SINAC

Consiste de una estación de trabajo extendida a la red LAN del COES el cual mantiene la misma funcionalidad de la Estación de Trabajo del Coordinador

Ventajas

- Disponer de una Estación de Trabajo extendida
- Uso inmediato de los programas, aplicaciones y recursos que el COES-SINAC dispone para cumplir con sus funciones.

Desventajas

Considerando que el software SCADA es de desarrollo propio del COES-SINAC no existe el marco legal que permita que nos puedan proporcionar la licencia de su software SCADA y de su protocolo ICCP. Cabe indicar que el software SCADA desarrollado por el COES-SINAC no es un producto comercial que sea difundido y probado mundialmente, sino es un desarrollo propio al cual se esta continuamente probando y añadiendo funciones y no se descarta la posibilidad que en un futuro opten por adquirir un sistema SCADA de reconocido prestigio mundial, lo cual complicaría mucho más que proporcionen una licencia SCADA al Regulador.

Adicionalmente se pueden notar las siguientes desventajas:

- Indisponibilidad de una Bases de Datos Históricas propia.
- Desarrollo limitado de aplicaciones orientados a la fiscalización
- Uso de los recursos y aplicaciones que han sido desarrollados de acuerdo a las necesidades del COES-SINAC y no de acuerdo a las necesidades del Regulador.
- Dependencia tecnológica presente y futura en vista que se tiene que estar supeditada a las decisiones del COES-SINAC en relación a su Centro de Control.

Costo inicial

Se estima un costo aproximado de US$ 20000 (veinte mil dólares estadounidenses)

- Hardware de la Estación de Trabajo
- Software del sistema operativo de la estación de trabajo
- Licencia de usos del software de interfase
- Ingeniería y desarrollo

Costos operativos

- Mantenimiento de Hardware.
- Uso de línea de comunicación dedicada

En la Figura Nº 1.3 se muestra la configuración propuesta.

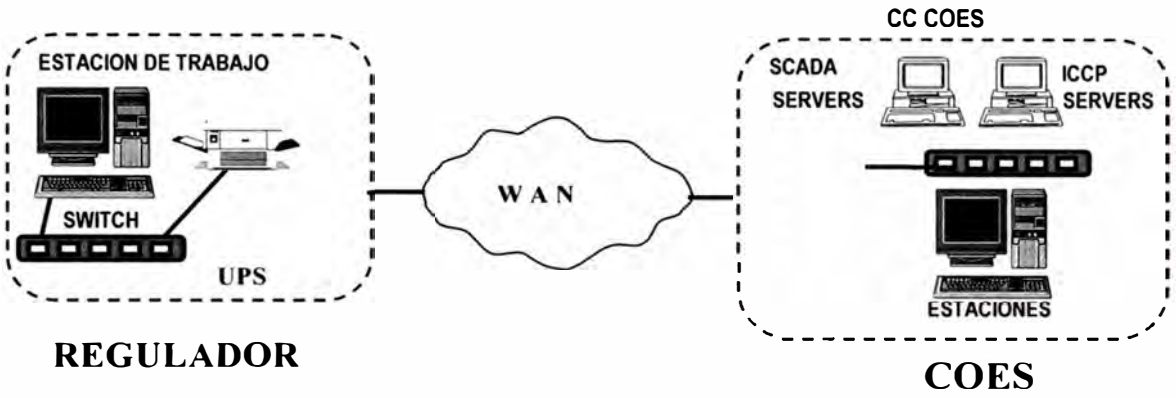


Figura Nº 1.3 :Estación de trabajo extendida de la red LAN del COES-SINAC

1.5.4 Sistema de Monitoreo en Tiempo Real seleccionado

De las tres alternativas planteadas, y considerando las grandes ventajas funcionales de tener un Sistema de Monitoreo en Tiempo Real propio y que el costo de los sistemas SCADA para la funcionalidad requerida (que se describe en el Capítulo IV) normalmente supera varios cientos de miles de dólares, el mayor costo que asciende a US$ 38000 (treinta y ocho mil dólares) para esta alternativa, resulta siendo marginal. En ese sentido, sobre la base de las ventajas y desventajas señaladas y las necesidades mediatas y futuras del Regulador para cumplir con el rol de supervisión, se selecciona la primera alternativa y el Regulador dispondrá de un **Sistema de Monitoreo en Tiempo Real con SCADA propio.**

ALTERNATIVAS	VENTAJAS	DESVENTAJAS
Sistema de Monitoreo en Tiempo Real con software SCADA propio	- Sistema ICCP (Cliente /Servidor) independiente de cambios en el COES-SINAC - Interfases con el usuario y crecimiento futuro acorde con las necesidades propias - Bases de Datos Históricas propias e independientes. - Interfases con el usuario y crecimiento futuro acorde con las necesidades propias - Desarrollo de múltiples aplicaciones orientadas a tareas especificas de fiscalización - Capacidad de instalar programas de gestión y análisis de redes eléctricas con fines de contraste de datos y resultados - Manejo ilimitado en asignación de usuarios, enlaces ICCP, pantallas gráficas y desarrollos propios respecto a publicaciones de datos que puedan ser llevados en tiempo real a aplicaciones Intranet e Internet.	Costo estimado en US$ 123 000 (ciento veinte tres mil dólares estadounidenses)
Sistema de Monitoreo en Tiempo Real con software SCADA del COES-SINAC	- Menor costo del Software SCADA y subsistemas que han sido desarrollados por el COES-SINAC, sin embargo no son productos comerciales ni cuentan con una óptima interfaz hombre máquina. Se estima un costo aproximado de US$ 85000 (ochenta y cinco mil dólares estadounidenses). - Interfaces gráficas del SEIN ya implementadas por el COES-SINAC.	- El software SCADA desarrollado por el COES-SINAC no es un producto comercial, difundido y probado mundialmente. Es un desarrollo propio al cual esta continuamente probandose y añadiendo funciones. No se descarta la posibilidad que en un futuro opten por adquirir un sistema SCADA de reconocido prestigio mundial, lo cual complicaria mucho más que proporcionen una licencia SCADA al Regulador. - Interfaces definidas por el coordinador de acuerdo a sus propias necesidades - Cambios y actualizaciones supeditadas al COES-SINAC - Rigidez en el desarrollo de aplicaciones en reportes especificos y futuras - La orientación del desarrollo de las aplicaciones son propias de las necesidades del COES-SINAC
Estación de trabajo extendida de la red LAN del COES-SINAC	- Estación de Trabajo extendida - Uso inmediato de los programas, aplicaciones y recursos que el COES-SINAC dispone para cumplir con sus funciones - Se estima un costo aproximado de US$ 20000 (veinte mil dólares estadounidenses)	- El software SCADA desarrollado por el COES-SINAC no es un producto comercial, difundido y probado mundialmente. Es un desarrollo propio al cual esta continuamente probandose y añadiendo funciones. No se descarta la posibilidad que en un futuro opten por adquirir un sistema SCADA de reconocido prestigio mundial, lo cual complicaria mucho más que proporcionen una licencia SCADA al Regulador. - Indisponibilidad de una Bases de Datos Históricas propia - Rigidez en el desarrollo de aplicaciones en reportes especificos y futuras - Uso de los recursos y aplicaciones que han sido desarrollados de acuerdo a las necesidades del COES-SINAC y no de acuerdo a las necesidades del Regulador • Dependencia tecnológica presente y futura en vista que se tiene que estar supeditada a las decisiones del COES-SINAC en relación a su Centro de Control.

Tabla Nº 1.1: Cuadro resumen de ventajas y desventajas para seleccionar el Sistema de Monitoreo en Tiempo Real del Regulador

CAPITULO II

DESCRIPCIÓN DE LOS SISTEMAS SCADA Y EL PROTOCOLO DE COMUNICACIÓN ICCP

2.1 Sistemas SCADA

SCADA viene de las siglas de "Supervisory Control And Data Adquisition", es decir: adquisición de datos y control de supervisión. Se trata de una aplicación software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, etc.) y controlando el proceso de forma automática desde la pantalla del ordenador. Además, provee de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros supervisores dentro de la empresa: control de calidad, supervisión, mantenimiento, etc.

En este tipo de sistemas usualmente existe un ordenador, que efectúa tareas de supervisión y gestión de alarmas, así como tratamiento de datos y control de procesos. La comunicación se realiza mediante buses especiales o redes LAN. Todo esto se ejecuta normalmente en tiempo real, y están diseñados para dar al operador de planta la posibilidad de supervisar y controlar dichos procesos.

Los programas necesarios, y en su caso el hardware adicional que se necesite, se denomina en general sistema SCADA.

Un sistema SCADA realiza un control supervisorio y de adquisisión de datos, de ahí su nombre mientras que un HMI es una interfase Hombre-Máquina que usualmente es para visualización del proceso y arranque y para de las máquinas. (ver figura Nº 2.1)

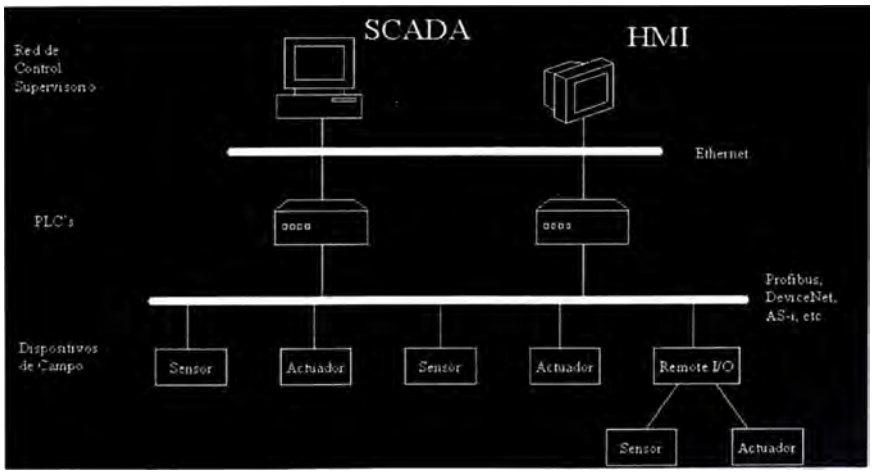


Figura Nº 2.1 :Configuración de un sistema SCADA

2.1.1 Prestaciones.

Un sistema SCADA debe estar en disposición de ofrecer las siguientes prestaciones:

- Posibilidad de crear paneles de alarma, que exigen la presencia del operador para reconocer una parada o situación de alarma, con registro de incidencias.
- Generación de históricos de señal de planta, que pueden ser volcados para su proceso sobre una hoja de cálculo.
- Ejecución de programas, que modifican la ley de control, o incluso anular o modificar las tareas asociadas al autómata, bajo ciertas condiciones.
- Posibilidad de programación numérica, que permite realizar cálculos aritméticos de elevada resolución sobre la CPU del ordenador.

Con ellas, se pueden desarrollar aplicaciones para ordenadores (tipo PC, por ejemplo), con captura de datos, análisis de señales, presentaciones en pantalla, envío de resultados a disco e impresora, etc.

Además, todas estas acciones se llevan a cabo mediante un paquete de funciones que incluye zonas de programación en un lenguaje de uso general (como C, Pascal, o Basic), lo cual confiere una potencia muy elevada y una gran versatilidad. Algunos SCADA ofrecen librerías de funciones para lenguajes de uso general que permiten personalizar de manera muy amplia la aplicación que desee realizarse con dicho SCADA.

2.1.2 Requisitos

Un SCADA debe cumplir varios objetivos para que su instalación sea perfectamente

- Deben ser sistemas de arquitectura abierta, capaces de crecer o adaptarse según las necesidades cambiantes.
- Deben comunicarse con total facilidad y de forma transparente con los operadores.
- Deben ser programas sencillos de instalar, sin excesivas exigencias de hardware, y fáciles de utilizar, con interfaces amigables con el usuario.

2.1.3 Módulos de un SCADA.

Los módulos o bloques software que permiten las actividades de adquisición, supervisión y control son los siguientes:

- Configuración: permite al usuario definir el entorno de trabajo de su SCADA, adaptándolo a la aplicación particular que se desea desarrollar.
- Interfaz gráfico del operador: proporciona al operador las funciones de control y supervisión de la planta. El proceso se representa mediante sinópticos gráficos almacenados en el ordenador de proceso y generados desde el editor incorporado en el SCADA o importados desde otra aplicación durante la configuración del software.
- Módulo de proceso: ejecuta las acciones de mando preprogramadas a partir de los valores actuales de variables leídas.
- Gestión y archivo de datos: se encarga del almacenamiento y procesado ordenado de los datos, de forma que otra aplicación o dispositivo pueda tener acceso a ellos.
- Comunicaciones: se encarga de la transferencia de información entre la planta y la arquitectura hardware que soporta el SCADA, y entre ésta y el resto de elementos informáticos de gestión.

2.2 Protocolo de Comunicación ICCP (Inter-control Center Communications Protocol – ICCP TASE.2) (IEC 870-6-802)

Es un protocolo especialmente diseñado para el intercambio de información entre centros de control (sistemas SCADA) para la industria del sector. Permite el envío y reenvío de información en forma eficiente permitiendo que la información se actualice por barrido o por excepción, la implementación se puede realizar por bloques.

Por ser de importancia las comunicaciones para transferencia de datos que se establezcan entre los Centros de Control de los integrantes del COES-SINAC y el Centro de Control de éste ultimo, se incluye en el **Anexo A** una Guía para los Usuarios del Protocolo ICCP. Esta Guía se preparó para el EPRI (Energy Power Research Institute), el cual ofrece un panorama general de las características del Protocolo ICCP.

CAPITULO III

FUNCIONALIDAD DEL SISTEMA SCADA DEL COORDINADOR DEL SEIN

3.1 Generalidades

El sistema SCADA del Coordinador del SEIN en lo posible debe ajustarse a las exigencias indicadas en el presente capitulo. A través de la descripción de la funcionalidad del mismo observaremos con mayor detalle los componentes de un sistema SCADA.

Las funciones básicas de un sistema SCADA son: adquisición y proceso de datos de la red, diálogo Hombre – Máquina, archivo histórico de informes y gestión de base de datos asociada a la red.

Para la implementación de un sistema SCADA se deben establecer cuales son los requerimientos de hardware, requerimientos de software los requerimientos de las funciones SCADA

Para explicar la infraestructura y funcionalidades de un sistema SCADA, mostraremos el requerido por el Coordinador del Sistema el cual es uno de los más completos por la naturaleza de sus funciones.

La funcionalidad del sistema SCADA debe cumplir con los siguientes requerimientos:

- Todos los periféricos pueden ser accesibles individualmente por cualquier equipo conectado a la red LAN. La falla de un procesador no debe afectar el funcionamiento de un dispositivo conectado a otro procesador.

- Todos los componentes del sistema deben ser interconectados utilizando los estándares para redes de área local.

- Los componentes del sistema necesarios para mantener la operación de funciones críticas, deben ser conmutados automáticamente a equipos de reserva.

- Cualquier componente del sistema, tal como: servidores, estaciones de trabajo, consola de operador, PCs, etc. pueden ser reemplazados, ampliados o puestos al día por un simple cambio o reconexión, sin afectar al resto del sistema y sin requerir software especializado que no pueda ser atendido por el suministrador.

- La configuración del sistema debe estar basado en estándares de sistemas abiertos, dando como resultado arquitecturas abiertas, en la cual el software podrá correr independientemente de la concepción del hardware.

- Las características de seguridad del hardware y software deben incluir facilidades que impidan el acceso a los dispositivos y programas de personas no autorizadas. Los dispositivos de administración de la red proporcionarán las facilidades para monitorear y manejar toda la red LAN.

- El programa debe permitir una interacción con la base de datos del sistema sin intervenir en la operación del tiempo real. Así mismo debe permitir la simulación completa de todos los componentes del sistema eléctrico, incluyendo los fenómenos transitorios y los de estado estable. Simulación de maniobras en la red tales como: apertura y cierre de interruptores, parada de máquinas, desconexión de líneas y otros similares deberán ser posibles ser simulados. Se debe incluir la simulación del proceso de eventos y todas las funciones SCADA aplicables a la operación. La interacción "full gráfica" es un requisito indispensable de este programa.

- Las estaciones de trabajo y las estaciones de los operadores y de los ingenieros de análisis deben incluir también el software de oficina.

A continuación se describirá lo que debe requerir un sistema SCADA similar al que debe tener implementado el Coordinador del SEIN:

3.2 Requerimientos del Hardware

Se requieren equipos y estaciones de trabajo de última generación, los cuales deben ser probados en fabrica (FAT), bajo los protocolos aceptado por el propietario. Pruebas después de la instalación (SAT) deben ser llevadas a cabo para asegurar el comportamiento del sistema instalado. Las pruebas antes señaladas deberán comprender el software suministrado y, principal atención, se pondrá en los tiempos de respuesta solicitados, así como el comportamiento del sistema para eventos en que se presenten avalanchas de datos, debido a perturbaciones en la red eléctrica.

Los servidores deben contar como mínimo con procesadores de características similares del tipo XEON Dual Core, y el respaldo de los datos se efectuará con la técnica RAID 5, contando con tres discos duros, siendo cualquiera de ellos respaldo de los otros.

La estación principal y la estación de reserva del Coordinador se ubicarán en áreas físicamente diferentes. Las dos redes estarán unidas con enlaces alternos de comunicaciones, preferentemente con fibra óptica y mantendrán permanentemente actualizados los datos del sistema eléctrico. Seguridades confiables, mediante software, se implantaran para asegurarse que solamente una estación tome el comando de la red a la vez.

En la estación principal se ha considerado útil una sub-red LAN conectada a la principal que dará acceso a estaciones dedicadas al análisis post-falla de los sistemas eléctricos así como cálculos destinados a la operación del sistema eléctrico. Esta solución ofrece la ventaja de dar acceso a los ingenieros de análisis del COES-SEIN, de manera restringida, a la base de datos histórico del sistema eléctrico que maneja el Coordinador.

En cada red se ha dispuesto también un reloj sincronizado por satélite, tipo GPS, que deberá tener una aproximación mínima de 500 ns.

El equipamiento Mínimo Hardware debe contemplar lo siguiente:

- 2 REDES REDUNDANTES: una (01) red redundante para el centro de control principal y otra para el centro de control de reserva.
    - 3 Switchs, 2 para generar la red principal, y la tercera para el centro de control de reserva.
    - 3 Servidores SCADA redundantes. La implementación del protocolo ICCP debe estar embebido y/o funcionando en el mismo servidor del SCADA.
    - 2 Servidores para las Bases de Datos para la redundancia del histórico SCADA e información de los modelos y datos del EMS.
    - 2 Servidores redundantes para la Operación del EMS Implementado solamente en el centro de control principal
    - 3 Ruteadores : 2 para el centro de control principal y el tercero para el centro de control de reserva.
    - 1 Pantalla de tecnología DLP: para el centro de control principal

3.3 Requerimientos del Software

El software deberá soportar una arquitectura abierta que permita la interrelación de los programas, incluyendo programas de suministradores que se adquieran con posterioridad al suministro original.

Los siguientes paquetes deben estar comprendidos en el suministro del software:

3.3.1 Software SCADA

- Sistema operativo de alta disponibilidad.
- Administración de la base de datos en tiempo real.
- Adquisición, procesamiento e intercambio de datos.
- Manejo de alarmas y eventos.
- Reporte de generación de informes.
- Entrada de datos manuales.
- Programas de administración del sistema LAN.
- Generación de curvas y tendencias.
- Protocolos ICCP y X.25.
- Suministro de las siguientes herramientas: software de oficina, Lenguajes de programación.

3.3.2 Aplicativos EMS (ENERGY MANAGEMENT SYSTEM)

- Estimador de estado.- Determina el estado de la red, detecta y corrige medidas erradas.
- Flujo de Carga.- Permite simular cambios en la red.
- Análisis de Contingencias.- Permite simular salida de elementos de la red y establecer la severidad de la misma en el desempeño de la misma.
- Pronóstico de la demanda.
- Control automático de la generación (AGC).
- Programación de la generación.
- Programación de los intercambios de energía.
- Monitoreo de la reserva activa.
- Flujo óptimo de potencia.

3.4 Requerimientos Mínimos de las Funciones SCADA

3.4.1 Generalidades

- El sistema debería emplear una interfase de usuario gráfica como el "human-machine interface (HMI)". Esta interfase de usuario gráfica debe permitir al personal de operación desarrollar todas las funciones sin ningún conocimiento del sistema operativo a nivel de comandos de consola.
- La estación de operador debe correr en cualquier PC estándar comercial corriendo el Sistema Operativo MS Windows, el sistema también debería soportar la más reciente versión de dicho sistema operativo. Ninguna excepción debe ser permitida.
- La estación debe soportar un amplio rango de dispositivos de usuario, incluyendo un ratón, pantallas sensibles al tacto y teclado.
- El sistema debería ser configurado para poder ser restaurado en la eventualidad de perdida de energía, para lo cual el servidor automáticamente se reiniciará y comenzará su operación completa, sin la intervención del usuario.
- El sistema no debe requerir computadoras o servidores dedicados para la administración de la base de datos adquiridos y emitidos, administración de alarmas, administración de la seguridad, ejecución de llamadas o cualquier otro sistema usuario.
- Cada sistema servidor debe ser capaz de funcionar como un sistema cliente.
- Seguido a la finalización de la instalación, cualquier usuario del sistema con privilegios apropiados y con la capacitación de configuración del sistema, deben poder ser capaces de hacer cambios al HMI, sin requerir la asistencia del proveedor del producto.

3.4.2 Configuración del Sistema / Operaciones Diarias

- La configuración del sistema debe ser protegido de cambios no autorizados por sistema de seguridad con claves de acceso.
- Los manuales de usuario deben proveer suficiente asistencia a los operadores y personal administrativo con operaciones diarias y configuración del sistema después que haya completado la implementación del sistema.

- Para maximizar la disponibilidad del sistema SCADA, el software debe ser capaz de configuraciones en línea. Esto en cambios de pantallas de visualización de datos, seguridad, desarrollo de reportes y comunicaciones de Entrada y Salida (E/S) desde los centros de control remotos, deben poder realizarse sin parar o reiniciar la aplicación o las computadoras.
- El software debe utilizar una metodología de bloqueo para asegurar que 2 usuarios no puedan configurar la misma pantalla o variable simultáneamente.
- Una vez probado, el sistema desarrollado debe ser capaz de forzar los cambios de configuración a variables y pantallas todas las otras computadoras en el sistema sin requerir que se reinicie o se paren los programas.
- El sistema debe soportar las conexiones de los clientes vía LAN, WAN Internet, dial-in vía MODEM y conexiones handheld-device vía Wireless AplicationProtocol (WAP).

3.4.3 Redundancia del Sistema

- El sistema debe soportar múltiples servidores backup, cada uno capaz de proveer completa funcionalidad del sistema incluyendo reportes, almacenamiento histórico por excepción, visualización de datos históricos, comunicaciones de Entrada/Salida, comunicaciones de red, administración de alarmas, dial-out por teléfono. No debería haber límite en el número de servidores backup soportados.
- En el caso de una falla en el servidor primario, el sistema debería ser capaz de activar automáticamente el servidor backup. Este proceso debe continuar al segundo servidor backup en el caso que también este último fallara.
- Los servidores backup deben ser capaces de compartir la carga de varias operaciones del sistema (incluyendo comunicaciones, generación del histórico, administración de alarmas, administración de las comunicaciones de red, administración de la seguridad)
- El sistema debe soportar 2 conexiones físicas de red para cada servidor, para ser utilizado con una vía de comunicación redundante. En el caso que una conexión se pierda, las comunicaciones deben automáticamente pasar a la segunda conexión.
- La configuración dual de los servidores se propone como un requerimiento mínimo. Una redundancia adicional a lo señalado podrá ser aceptada siempre

que su costo resulte competitivo y que con esa propuesta se asegure una alta disponibilidad del sistema. La tecnología actual ofrece redundancias cuádruples, que pueden conseguirse mediante arreglos de software.

3.4.4 Comunicaciones

- Las herramientas del diagnóstico de las comunicaciones serán incluidas para ayudar en la visualización de comunicaciones apropiadas. Las herramientas incluirán los métodos para supervisar estadística de la comunicación, reportar errores y registrar comunicaciones de Entrada/Salida y de la red.
- El sistema será capaz de compartir comunicaciones de Entrada/Salida a través de varios servidores.
- Los protocolos de comunicaciones múltiples estarán disponibles sobre el mismo puerto de comunicaciones. Ningún controlador (driver) de las comunicaciones evitará explícitamente que otros protocolos usen el mismo puerto de comunicaciones. Los conductores de las comunicaciones serán capaces de compartir el equipo de comunicaciones, tal como una torre de radio (donde no hay diferencia en la radiofrecuencia) o un grupo de módems compartidos.
- En razón a que el protocolo designado por el coordinador es el ICCP, este debe ser capaz de conectarse con todos los servidores ICCP de fabricantes conocidos.
- Las conexiones para la adquisición de información deben configurarse en modo excepción (bloque 2 ICCP) con una máxima duración de 1 segundo y un máximo 5 minutos para barrido para guardar la integridad de los datos.
- Las licencias ICCP deben ser ilimitadas para asegurar que el número de integrantes del COES-SINAC puedan crecer sin restricciones.
- Los operadores podrán poner cualquier conexión en un estado de la rápido-interrogación. En este estado, las conexiones podrán aumentar la frecuencia más altamente que lo normal, permitiendo que los operadores y el personal de mantenimiento reciban más datos durante situaciones de alarma.
- El canal de comunicación principal, deberá enlazarse con la estación principal del Coordinador y el canal secundario, se enlazara con la estación de reserva del COES, ambos en protocolo ICCP.

3.4.5 Pantallas Gráficas de Sistema

- El sistema debe soportar objetos gráficos dinámicos y estáticos. Los objetos gráficos dinámicos proporcionarán la información en tiempo real del sistema al interfaz del usuario.
- Como mínimo una licencia del software estará para el desarrollo del sistema.
- Se deben crear pantallas representando procesos de sistema e instrumentación. Estas pantallas serán construidas con los elementos gráficos orientados al objeto.
- El sistema debe incluir un menú para navegar de una pantalla a otra. El menú debe ser configurable para permitir la agrupación lógica de pantallas donde sea necesario.
- Las pantallas deben usar capacidades del sistema de vídeo para mostrar visualmente los estados, valores y condiciones de alarma de los principales componentes del sistema. Así también cuando cambian los estados de los componentes del sistema, el color del símbolo mostrado para los componentes debe cambiar para denotar dichos cambios.
- Las Operadores con suficientes privilegios de seguridad deben tener acceso para modificar los setpoints y puntos de control sin parar o reiniciar el sistema.
- También debe proveerse al operador capacidad de imprimir pantallas gráficas.
- Los valores de entrada y salida E/S deben ser puestos a un estado "cuestionable" cuando se usan por primera vez, este estado debe ser removido por el operador cuando los valores hayan sido verificados por el operador contra los datos de campo.
- Debe ser posible determinar las propiedades de cualquier valor mostrado de E/S con solo seleccionarlo. Esto debe ser hecho en tiempo real y mostrar la siguiente información:

    - Nombre y descripción del Area (ubicación)
    - Unidades, etiqueta de tiempo y calidad del dato.
    - Propiedades de alarma.

- El sistema debe incluir editor de gráficos orientado a objetos y animación.

- EL software debe soportar imágenes por capas. Los objetos podrán ser colocados en fondos de pantalla u otras imágenes gráficas.
- El software debe soportar, importar formatos conocidos de archivos gráficos (JPEG, PNG, etc.) como son mapas para uso de fondos de pantalla.
- El software debe permitir encoger o ampliar para acomodar las pantallas como ventanas son redimensionadas.
- El software debe ser capaz de mostrar múltiples ventanas gráficas simultáneamente.
- No debe haber límite en el número de pantallas gráficas, el número de valores activos mostrados en una pantalla gráfica o el numero de E/S o estaciones remotas que el software sea capaz de manejar.

3.4.6 Visualización de la Información Histórica y de Tiempo Real

- La información histórica y de tiempo real debe estar disponible para todo monitoreo de variables en procesos digitales y análogos en la aplicación. Los valores históricos y de tiempo real deben ser mostrados en forma continua, ininterrumpida y desplazable. Estos deben ser mostrados en un estilo de gráfico continuo, el eje X con la unidad y el eje Y representando al tiempo. Cada pantalla debe ser escalado en las coordenadas apropiadas para la variable específica a ser monitoreada. El tiempo debe ser claramente marcado con etiquetas de tiempo.
- El sistema debe ser capaz de mostrar 10 variables análogas y 10 variables digitales en un solo cuadro. El color debe ser usado para diferenciar entre las variables. Esto significa que debe proveer una etiqueta y descripción para ubicar rápidamente cada variable mostrada.
- Debe proveerse las siguientes funcionalidades:
    - Generar tendencia y exploración de la información.
    - Hacer las ampliaciones (zoom).
    - Explorar los datos a lo largo del tiempo y poder seleccionar un día para mostrarlo.
    - Mover los gráficos de las variables análogas verticalmente.

- Mostrar información estadística, incluyendo promedios, mínimo y máximos, para cada gráfico.

- Capacidad de imprimir las tendencias Históricas y en tiempo real.
- Capacidad de adjuntar una nota del operador en un punto particular en el tiempo.
- Capacidad de exportar los datos en formato "comma separated value" (csv) (valores separados con coma o punto decimal) o directamente a una base de datos, para el use de algún software de análisis de datos de terceros.
- EL software debe ser capaz de guardar grupos de tendencias graficas para luego poder mostrarlas. Estos grupos deben guardar la última configuración de puntos de las tendencias de los valores. No debe haber límite en el numero de grupos.
- Debe ser posible almacenar información histórica mensual para luego poder ser restaurada y estar disponible para los Informes. Este proceso no debe requerir para o reiniciar la aplicación o computadora.

3.4.7 Administración de Alarmas

- Los eventos de alarmas deben incluir la etiqueta de tiempo (timestamp).
- Cuando ocurre una condición de alarma, la siguiente secuencia debe ser proveída:

  - Un tono audible anunciará en cada una de los servidores y clientes que tienen acceso a la alarma. Este tono audible debe repetirse hasta que la alarma sea reconocida por el operador.
  - La alarma debe ser añadida al log de eventos.
  - La alarma debe ser impresa en la impresora de log de eventos.
  - En el caso que la señal no ha sido reconocida por un tiempo configurado por el usuario el sistema comenzará a emitir mensajes por un medio externo (modem, mensajes a móviles, etc.). notificando esta alarma.

- Cada alarma análoga debe tener una configuración para la banda muerta y demora que puede ser modificada por el usuario.
- Todas las pantallas de usuario deben tener un botón o símbolo para que el usuario pueda cargar el módulo de administración de alarmas.

- Una alarma debe ser reconocida seleccionando en la lista de resumen alarmas y luego seleccionando un botón para ello. Las alarmas no deben ser reconocidas simplemente marcando en la lista de eventos. Estos dos pasos necesarios prevén la inadvertida acción de reconocimiento de la alarma.
- El reconocimiento de alarma debe propagarse inmediatamente a todas las pantallas.
- Los operadores deben ser capaces de ver las alarmas actuales, no reconocidas e históricas. Las alarmas deben poder ser filtradas por prioridad.
- La aplicación debe ser capaz de enviar mensajes por medios externos a la red SCADA, sea por conexión telefónica u otro medio efectivo.
- El software debe ser capaz de definir un número ilimitado de prioridades de alarma y este ser configurable.
- Los mensajes externos deben ser capaces de contactar grupos de usuarios del sistema de acuerdo al tipo de alarma. Debe poder configurar usuarios activos e inactivos, estos ser administrados por un usuario con privilegios de configuración. No debe requerir parar o reiniciar la computadora o aplicación. No debe haber límite en el número de usuarios activos e inactivos.

3.4.8 Sistema de generación de Reporte

- Un sistema de generación de reportes debe ser incluido para imprimir reportes estándares y configurados por el usuario. La generación de reporte puede ser invocada a necesidad del usuario, por un evento monitoreado, o automáticamente en el día, semana o mes.
- Debe ser posible configurar los reportes para cumplir las necesidades de administración y los requerimientos generales. Reportes deben ser impresos usando valores históricos o de tiempo real actuales o calculados.
- El sistema debe ser capaz de enlazar dinámicamente datos de tiempo real a hojas de calculo de terceros.
- El sistema de generación de reportes debe ser configurable, permitiendo a un operador crear, modificar y generar reportes y exportar datos para uso de paquetes de terceros. El sistema de reportes debe ser capaz de mostrar reportes por la pantalla o de exportar a archivos de los siguientes formatos:

- Archivos de Valores separados por coma (.cvs)
- Archivo de texto
- Directamente a base de datos (ODBC, OLEDB, DP, JDBC etc)
- Directamente a una hoja de calculo
- Directamente a hoja de calculo formateado como una plantilla de reporte.
- vía correo electrónico

- Los informes generados por un cliente Internet deben ser capaces de ser impresos en una impresora local.
- El sistema de generación de reportes debe tener predefinido por medio de un menú seleccionable considerando el periodo de tiempo para la cantidad de datos reportados. Los siguientes periodos deben ser proveídos:

  - Ultima hora
  - Ultimas 4 horas
  - Ultimas 12 horas
  - Ultimo día
  - Ultima semana
  - día previo
  - Semana previa
  - Mes previo
  - Trimestre previo
  - Configurado (el operador selecciona iniciar o parar días y horas)

- Los reportes deben ser capaces de mostrar cualquier dato analógico, digital o valores calculados.
- El Software debe ser capaz de guardar grupos de reportes para llamadas posteriores. No debe haber límite en el número de grupos a definir.

3.4.9 Base de datos

- El sistema debe mantener todas las configuraciones de los puntos en una base de datos relacional con características de consulta según el estándar SQL.
- El sistema debe mantener todas las configuraciones especificas de las estaciones de trabajo.

- El sistema debe guardar los valores históricos y de tiempo real, condiciones de alarma y eventos del sistema en una base de datos. El sistema debe guardar datos históricos por un periodo no menor a 5 años. El formato de datos histórico será tal que los cinco (5) años completos de datos pueden ser consultados sin requerir que los archivos sean restaurados. El hardware del servidor del sistema será dimensionado para almacenar dos veces el tamaño aproximado de esa cantidad de datos.
- La arquitectura del software asegurará que las bases de datos del sistema estén duplicadas en todos los servidores primarios y de reserva, y estas bases de datos deben estar sincronizadas siempre.
- En el evento de una falla del servidor primario, automáticamente entrara en función el servidor de reserva. Cuando el servidor primario se restaura otra vez, este sincronizará a las bases de datos en el servidor de reserva.

3.4.10 Diagnósticos Remotos

- El sistema debe permitir su acceso para propósitos de diagnostico, vía modem o medio externo. Cuando accesan al sistema de esta manera, el usuario asumirá el control total sobre el servidor al cual se enlazó.
- Todas las actividades de ingreso o salida del sistema deben ser grabados en el log de eventos del sistema.

3.4.11 Seguridad

- El sistema debe manejar la seguridad a través de claves de acceso, este debe permitir múltiples usuarios, cada usuario debe tener un juego de configuración de privilegios. Los privilegios para la configuración del sistema, visualización de datos, y actividades de operación pueden ser activados o no para cada usuario.
- La seguridad debe basarse en privilegio de usuario más que en roles, para permitir el máximo control de los accesos de los usuarios.
- Las cuentas de cada usuario deben permitir ser duplicadas para asignarlas a un nuevo usuario.
- Los password de los usuarios deben ser encriptados, de modo que no permitan la lectura en el lugar de almacenamiento.

- El sistema debe permitir la creación de privilegios de seguridad adicionales donde sea necesario. El sistema debe permitir la creación de no menos de 100 privilegios adicionales.
- Los cambios a los privilegios de acceso de los usuarios podrán efectuarse mientras la aplicación está siendo ejecutado y deberían ser afectados inmediatamente. Igualmente los usuarios conectados a la red deben ser afectados por los cambios inmediatamente sin necesidad de parar o reiniciar la aplicación.
- El sistema de seguridad debe ser multisesión. Esto validará simultáneamente y grabará las actividades de las sesiones concurrentes para todos los usuarios.

3.4.12 Pantalla tipo DLP

La tecnología DLP está basada en el semiconductor DMD (Digital Micromirror Device). La empresa Texas Instruments inventó este semiconductor. El DMD es un conmutador de rápida reflexión para la luz digital. Combinado con una fuente de luz, memoria, procesamiento de imágenes y elementos ópticos da lugar a un sistema DLP capaz de proyectar imágenes compensadas de gran brillo y colores de alto contraste con una fidelidad y cohesión en los colores sin precedentes. Sus dimensiones será de 2 x 3 m y su orientación se aplica a una presentación general de las pantallas de los operadores, pudiendo presentar los gráficos de cualquiera de ellas.

Ventajas de la técnica DLP respecto al LCD

- La tecnología DLP es especialmente efectiva a la hora de mostrar imágenes de vídeo. Un solo chip de DLP tiene una rejilla entera de píxeles y cada píxel de ese chip tiene su propio espejo reflector por separado que ayuda a amplificar la luz que se genera. Debido a que cada píxel tiene su propia fuente de luz amplificada, prácticamente no hay límite de tamaño de la imagen porque el brillo y el contraste siempre serán consistentes. Son pequeños, ligeros y muy fáciles de transportar.
- Mayor Luminosidad (Tecnología Reflexiva)
- Menos consumibles (mayor vida útil)
- Mayor estabilidad del sistema
- Menor consumo

- Mayor calidad y estabilidad en video.
- Mayor definición de colores.
- Mejor ajuste de colores.

En la tabla Nº 3.1 se presentan las diferencias entre las tecnologías DLP y LCD aplicados a las pantallas de visualización.

Tecnología DLP	Tecnología LCD
Mínimo 100 000 horas (12 años bajo trabajo continuo) de vida útil sin sacrificar la calidad de imagen ni el rendimiento del equipo.	30 000 horas (4 años bajo trabajo continuo).
No pierde sus propiedades físicas, por lo que la imagen se ve igual el primer día o 100,000 horas después de uso.	Después de cierto tiempo, la imagen empieza a verse opaca, borrosa, pierde contraste y uniformidad.
Mínimo efecto de las condiciones medio ambientales	Los paneles LCD se ven afectados por la luz ultravioleta, la temperatura y fluctuaciones eléctricas y con el uso se va decolorando la imagen, los blancos se ven amarillos, los colores originales se pierden.
Ninguna línea o mancha en la pantalla	Los paneles LCD suelen quemarse generando líneas, manchas o puntos en la pantalla. Estos paneles y su reparación son sumamente caros.

Tabla Nº 3.1: Diferencias tecnológicas entre Pantallas DLP y LCD

3.5 Requerimientos Software para Análisis (EMS)

3.5.1 Estimador de Estado.-

Determina el estado de la red detecta y corrige medidas erradas. Debe cumplir con:

- Ser un identificador de Telemetría Analógica Defectuosa. Antes de ejecutar la solución de estimación de estado, el programa debe validar todas las mediciones

para identificar aquellas que están fuera de límites, o aquellas que son inconsistentes con otras mediciones. Continuando con el proceso de solución, debe utilizar una técnica estadística y automática para identificar y eliminar aquellas mediciones que, por ser suficientemente imprecisas, pueden afectar la estimación de otros parámetros.

- Poseer Algoritmos Robustos de Solución Rápida que proporcionen fotos del sistema sobre las cuales otras secciones del programa pueden operar. El algoritmo de estimación de estado hace uso de las últimas técnicas de ordenación y esparsidad matricial para agilizar el proceso de solución. Debe ser particularmente robusto en la presencia de datos analógicos malos o de errores topológicos. Debe estimar las magnitudes y ángulos de los voltajes, así como las posiciones de ángulo de fase y derivadores de transformadores.
- Actuar como un procesador de observabilidad. Basado en datos de telemetría y configuraciones de medición, el Procesador de Observabilidad determinara qué partes de la red son observables y cuáles no son observables. En aquellas partes de la red que no son observables, el procesador debe insertar un número mínimo de seudo-mediciones de forma que esta parte de la red sea observable.

3.5.2 Análisis de Contingencias.-

Permite simular salida de elementos de la red y establecer su severidad en el desempeño de la misma. Partiendo del estado inicial del sistema, determinará qué contingencias de líneas, transformadores o generadores son más perjudiciales para la seguridad del sistema. Utilizando variadas técnicas analíticas y de modelaje. Deberá efectuar simulaciones precisas y detalladas de cualquier condición del sistema y luego efectuar un análisis preciso del comportamiento del sistema en esa situación. Debe poseer un flexible y optimizado sistema de recolección de datos y de presentación de resultados y ofrecerá al personal de operación un cuadro completo de todas las posibles amenazas para la seguridad del sistema.

3.5.3 Identificación de Errores de Topología.-

En esta sección el sistema debe actuar como un pre-procesador para corregir el status de los interruptores y cuchillas antes que el estimador de estado determine los voltajes de la red y la posición de los derivadores de los transformadores. Cuando el sistema software detecta un status incorrecto debe corregirlo y emitir una alarma.

3.5.4 Pronostico de la Demanda.-

El programa debe estar basado en un algoritmo probado que utilice la técnicas que permita predecir cargas horarias con proyección de hasta una semana. El programa debe incluir rutinas de largo y mediano plazo, así como condiciones de clima, incluyendo situaciones de demanda no corrientes.

3.5.5 Control Automático de la Generación.-

La función que debe llevar a cabo el control automático de generación AGC es determinar que cantidad de energía hay que generar para cubrir satisfactoriamente la demanda actual de carga, repartiendo esta generación entre las distintas unidades de producción, coordinando los requisitos de regulación con los puntos básicos de operación de cada unidad.

Este último requisito implica importantes conexiones del AGC con otras funciones propias del centro de control en las cuales se calculan esos puntos básicos de operación de esas unidades. Tradicionalmente esos puntos básicos los calcula la función del "despacho económico", aunque en algunas ocasiones otras funciones como el "análisis de la seguridad" o el "control de emergencias", pueden establecer esos puntos básicos de operación.

Para llevar a cabo esta función, se requiere que las unidades de generación cuenten con equipos apropiados para ejecutar las consignas emanadas por el Coordinador.

3.6 Disponibilidad del Sistema del Coordinador

El Sistema deberá tener una disponibilidad global del 99.95% para toda las funciones criticas. Esto significa que el tiempo de falla total anual acumulado de todas las funciones criticas no deberá exceder las 4 horas y 23 minutos y no ocurrirá mas de un total de 40 incidentes de falla, para cualquiera de las funciones criticas en el periodo de un año.

Todas las funciones son definidas como críticas, excepto las citadas a continuación:

- Generación y modificación de la base de datos.
- Generación y modificación de despliegues.
- Creación y modificación de reportes.
- Soporte para el desarrollo de software.

- Generación y configuración del software del Sistema.
- Eventos en la estación de Desarrollo e Ingeniería.

El valor de la disponibilidad mencionado no incluye a los centros de control remotos, sistemas de telecomunicaciones o fuentes de energía. Para los primeros, se recomienda definir una disponibilidad mayor a la anteriormente mencionada, de manera de no degradar la disponibilidad total del conjunto.

3.7 Infraestructura de Soporte

3.7.1 Alimentación Eléctrica

Para asegurar la continuidad de la alimentación del servicio eléctrico a los equipos de los centros de control principal y de reserva, es necesario suministrar alimentadores tipo UPS duplicados, conectados de manera tal que puedan conmutar la carga a la alimentación disponible. La autonomía del equipo debe garantizar un funcionamiento a plena carga de los equipos del Coordinador por un periodo mínimo de 4 horas.

3.7.2 Equipo de Aire Acondicionado

Para los ambientes de la sala de control así como la sala de los equipos informáticos se debe prever climatización en base a sistema de aire acondicionado que asegure una estabilidad de la temperatura de 20ºC y una humedad relativa que no exceda el 85%. El equipamiento del aire acondicionado debe preverse para los dos centros de control del COES-SINAC. La alimentación eléctrica para este sistema será efectuada desde el sistema eléctrico comercial

3.7.3 Equipo de Seguridad

En los dos centros de control se debe prever el sistema de seguridad mediante detectores de humo y fuego, así como una red de televisión de circuito cerrado (CCTV). Las imágenes centralizadas del sistema CCTV podrán ser observadas desde cualquiera de los dos Centros de Control, mediante los monitores dedicados a este servicio.

Se debe prever un control de acceso a personas autorizadas a los Centros de Control, mediante lectoras de tarjetas con códigos de barras u otro sistema superior.

Es conveniente que en la sala de control y en la sala de los equipos informáticos se instalen pisos antiestáticos de tal manera de prevenir mal funcionamientos por acumulación de cargas en los equipos.

Equipos extintores contra incendio, así como detectores de humo y fuego deben ser previstos en lugares críticos de las instalaciones del Coordinador.

3.7.4 Central Telefónica

Para la coordinación con los centros de control de los componentes del COES-SINAC, así como para las labores administrativas, se requiere una central telefónica digital de programa almacenado y de características no bloqueables. La central telefónica deberá prever como mínimo 12 circuitos de interconexión con la red publica y 50 abonados internos. Las restricciones para las llamadas locales, nacionales e internacionales, deberán ser previstas de modo de racionalizar el uso del servicio telefónico.

3.8 La Red ICCP del SEIN

La "Red ICCP del SEIN" (RIS) es una red de intercambio de datos operativos en tiempo real entre el Coordinador y las empresas integrantes del Sistema Eléctrico Interconectado Nacional (SEIN).

3.9 Estándares de calidad y confiabilidad de la RIS

La confiabilidad del canal de comunicación no debe ser inferior al 99.9%.

La calidad de los datos que llegan al Coordinador, influirá en el éxito de las funciones que debe asumir por lo que se impone asegurar una calidad mínima a los enlaces de comunicación que se enlazan con el Coordinador.

3.10 Transferencia de Información en Tiempo Real

Es importante establecer la manera y protocolos como los sistemas SCADA y EMS del Coordinador y los centros de control de los Integrantes del SEIN puedan intercambiar información. Se tomará en cuenta lo indicado en las Normas Internacionales y lo señalado en la NTOCTR. Así mismo, se ha tomado como referencia instalaciones similares de otros países, en especial de EEUU, donde el intercambio de información en tiempo real entre las áreas regionales se realiza utilizando el protocolo ICCP, a nivel de sistemas SCADA.

Para los enlaces de 64 kbps por cada empresa requeridos por el COES-SINAC.

El mantenimiento y el costo de los canales de comunicaciones que enlazan a los centros de control de los integrantes del SEIN con el Coordinador, están a cargo de cada uno de los integrantes del SEIN.

En la Tabla Nº 3.2 se muestra el total de puntos enviados por los integrantes del SEIN. Se estima que faltan todavía 4000 puntos entre medias, estados y alarmas.

EMPRESA	Total/Emp
CAHUA	116
CEM. NORTE PACASMAYO	23
EDE. CAÑETE	48
EDEGEL	492
EDELNOR	548
EEPSA	73
EGASA	223
EGEMSA	207
EGENOR	322
EGESUR	173
ELECTRO CENTRO	110
ELECTRO NOR OESTE	170
ELECTRO NORTE	74
ELECTRO SUR	71
ELECTROANDES	432
ELECTROPERU	76
ENERSUR	231
ETESELVA	88
ETEVENSA	34
HIDRANDINA	213
HUANCHOR	54
ISA PERU	161
LUZ DEL SUR	381
REDESUR	90
REP - SICN	1974
REP - SUR	545
SAN GABAN	149
SHOUGESA	69
TERMOSELVA	24
TRANSMANTARO	197
Total puntos:	**7368**

Tabla Nº 3.2: Cantidad de puntos remitidas en tiempo real por los integrantes del SEIN al Coordinador

CAPITULO IV

EQUIPAMIENTO E INGENIERÍA NECESARIA PARA IMPLEMENTAR EL SISTEMA SCADA DEL ORGANISMO REGULADOR DEL SECTOR ENERGÍA

4.1 Diagnóstico del tipo y volumen de información a procesar (tipo de Información que dispone el Coordinador del SEIN).

El COES-SINAC concentra toda la información de los SCADA's de las empresas eléctricas del SEIN, cada empresa presenta una realidad diferente en la implementación de protocolo ICCP para el envío de esta información.

Como parte de la implementación del SCADA del REGULADOR, se dispuso al COES-SINAC que reenviara esta información tal como lo recibe.

El COES-SINAC tiene la atribución de definir la manera como las empresas van a enviar la información de tiempo real, en su página Web en la opción SCADA define que los canales serán configurados de la siguiente manera:

- Analógicos serán del tipo RealQTimeTag este tipo de dato contiene la etiqueta de tiempo.
- Estados serán del tipo StateQTimeTag este tipo de dato contiene la etiqueta de tiempo.

Las empresas de acuerdo a su disponibilidad tecnológica y económica no han implementado los tipos tal como definió el COES-SINAC, muchos de ellos envían tipos RealQ y StateQ sin incluir la etiqueta del tiempo. El COES-SINAC como parte de su implementación SCADA asignan tiempos estimados a la etiqueta de tiempo de canales y en el que contemplan demoras promedio por empresa.

En el dimensionamiento del SMTR, se considerará la capacidad inicial y futura de soportar los equipos, los puntos físicos telemedidos en campo provenientes de todos los integrantes del SEIN, los puntos no telemedidos que corresponderán a valores ingresados manualmente o en forma automática y la capacidad de soportar puntos calculados.

En la Tabla 4.1 se indica el total de señales que el Coordinador recibe de los integrantes del SEIN, que será retransmitida al Sistema de Monitoreo en Tiempo Real (en adelante SMTR), el mismo que se incrementará por el ingreso de nuevas instalaciones eléctricas y/o ampliaciones de los existentes.

Analógicas	Estados	Alarmas	Total señales
4,358	3,801	2,859	11,018

Tabla Nº 4.1: Señales del SEIN

4.2 Equipamiento e ingeniería necesaria.

La ingeniería necesaria para implementar el SMTR del Regulador abarca:

- Ingeniería de detalle del SMTR.
- Pruebas de transmisión de datos desde el Centro de Control del Coordinador hasta el SMTR a ser instalado en OSINERG.
- Edición de despliegues del SCADA.
- Planos de disposición física de los equipos.
- Planos de canalizaciones por bandejas, tuberías y canaletas.

4.2.1 Configuración del SMTR

En la figura Nº 4.1 se muestra la configuración del SMTR. Los datos de campo provenientes de la empresas integrantes del SEIN, serán reenviados desde el Coordinador al SMTR a ser emplazado en las Oficinas del Regulador.

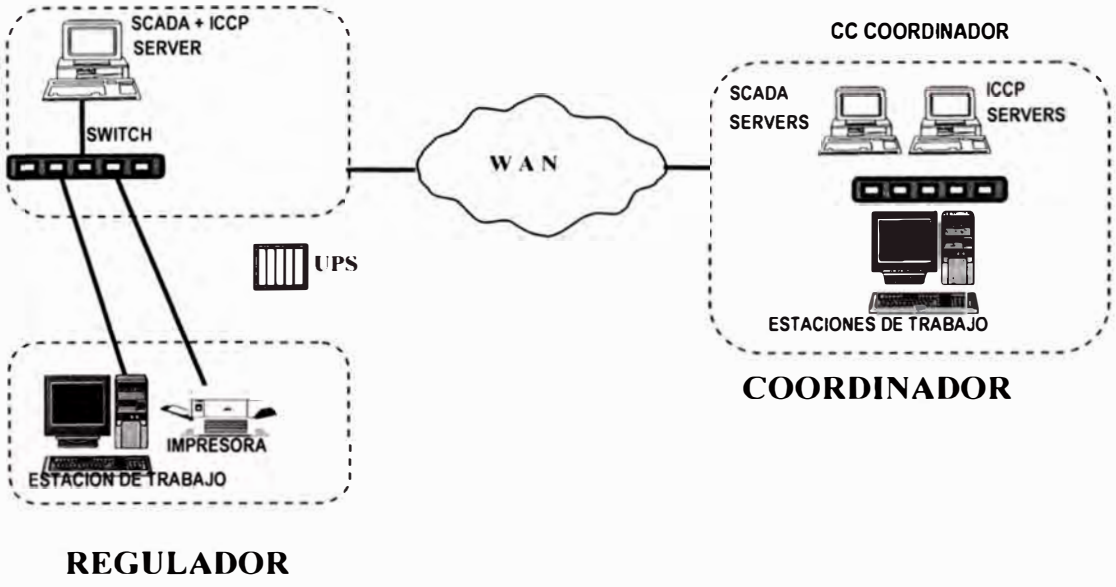


Figura Nº 4.1: Configuración del Sistema de Monitoreo en Tiempo Real

El medio de enlace entre los Centros de Control será mediante una línea dedicada de 256 kbps.

En lo que sigue se resaltan las características mínimas que los equipos y programas deben cumplir para que el SMTR cumpla con los objetivos propuestos.

4.2.2 Software del SMTR

Se precisan las características técnicas y funcionalidades que deben cumplir el software requerido para ser considerado como un producto de última tecnología y que son las siguientes:

a) Sistemas operativos y software de oficina

- El sistema operativo del servidor del SMTR será Microsoft Windows Server 2003 Standard Edition SP2.
- El sistema operativo de la estación de trabajo será Microsoft Windows XP Professional SP2 o en su versión más reciente.
- El software de Oficina para el servidor y la estación de trabajo será Microsoft Office 2003 Proffessional.
- Software administración, seguridad y diagnóstico
- Base de datos relacional SQL Server2000 o su versión superior (al menos 5 licencias para usuarios) compatible con el software SCADA.

b) Software SCADA

- El Software SCADA (Supervisory Control And Data Acquisition/Supervisión Control y Adquisición de Datos) basado en estándar OPC (OLE for Process Control/Object Linking and Embedding for Process Control) y protocolo Inter.-Control Center Communication Protocol (ICCP) embebido.
- Capacidad demostrada con catálogos para operar en diferentes arquitecturas como son sistemas de doble y múltiple redundancia.
- Capacidad de utilizar diversos medios de comunicación alámbrica e inalámbrica como son Wlan, fibra óptica, par trenzado, microondas, dial up, internet ADSL/DSL, tecnología celular GSM/GPRS/CDPD. En la definición de una línea de comunicación se incluirá nombre, protocolos, parámetros de línea y enlace, número de puertos y otros relevantes.

- Todos los subsistemas del sistema SCADA deberán estar desarrollados considerando los estándares abiertos especificados por la Fundación OPC (OLE for Process Control) como son el acceso de datos, alarmas y eventos, intercambio de datos, manejo de datos históricos, comandos, etc..
- Los programas y/o softwares a ser instalados en el servidor del SMTR serán modulares lo cual permitirá su fácil cambio a otras plataformas de cómputo y/o migrar a soluciones en software de versiones mas recientes.
- El subsistema Interfase Gráfica con el Usuario (GUI Graphic User Interfase) deberá ser totalmente gráfico (Full Graphics), con múltiples opciones de manejo de pantalla, capacidad de panning, decluttering y zooming continuos y con capacidad de introducir gráfico de tendencias, imágenes, acceder a registros de la base de datos y generar reportes utilizando procesadores de textos y hoja de cálculos.
- Disponer de una biblioteca de gráficos orientado a la industria eléctrica.
- Capacidad de construir gráficos estáticos y dinámicos que representen y simulen a las mediciones físicas obtenidas en campo.
- Capacidad de construir gráficos de tendencias.
- Capacidad de efectuar reportes tabulares.
- Presentación de reportes de datos históricos hasta con una antigüedad de 5 años.
- Facilidades para almacenar archivos históricos en formato DVD y en cinta magnética.
- El subsistema Administrador de Datos Históricos (HDM Historical Data Management) deberá permitir la administración de los reportes de acuerdo a las necesidades con el usuario con una periodicidad diaria, semanal, mensual, anual. Los datos podrán ser archivados en medios magnéticos a requerimiento del usuario o al cumplimiento de periodos preestablecidos.
- El subsistema de procesador de alarmas deberá detectar las condiciones anormales de operación con indicación de los siguientes mensajes:
    - Parpadeo de la alarma en la pantalla gráfica.

- Activación de una alarma sonora.
- Capacidad de envío de un mensaje de texto a celulares o notepads.

- La capacidad y la flexibilidad de expansión del sistema en etapas posteriores del proyecto serán aspectos importantes a ser analizados durante la evaluación de propuestas.
- El sistema SCADA se diseñará para manejar el dimensionamiento futuro de las señales de los puntos de estado, análogos, despliegues, base de datos, puntos integradores de energía y volumen de agua suministrada, etc.
- La actualización de las bases de datos y de los despliegues se efectuarán estando el sistema SCADA en servicio.
- El sistema SCADA será escalable en forma horizontal y vertical. En forma horizontal tendrá la capacidad ilimitada de aceptar las nuevas señales adicionales y en forma vertical aceptar sin mayores cambios nuevas plataformas de cómputo y nuevas versiones de software.
- La base de datos estará diseñado para soportar como mínimo de 150,000 puntos (estado + analógicos) y líneas de comunicación serán ilimitados.
- La base de datos histórica del SCADA será compatible con la base de datos relacionales como el SQL, Oracle y otros.
- Capacidad de manejar directamente protocolos de comunicación abiertos tales como ICCP, DNP 3, IEC y Modbus.

4.2.3 Hardware del SMTR

a) Plataforma de cómputo del servidor

El servidor, fuente principal de procesamiento y cálculo del SMTR, debe estar constituido por un servidor principal y será seleccionado de modelos recientes para ser instalados en rack, para lograr una operación eficiente y segura, como componentes de un sistema en tiempo real. Debe incorporar el soporte RAID 5 en su propia cabina y que esta a su vez tenga un consumo mínimo de electricidad y opere con un nivel de ruido permitido por normas. Los procesadores tendrán relojes de alta precisión y sincronizarán a equipos esclavos. Se mantendrá un registro de errores de los servidores para fines de diagnóstico.

Los servidores serán instalados en los ambientes de Informática del REGULADOR.

b) Estación de trabajo grafica

La estación de trabajo será de gran capacidad gráfica, de alta performance y perteneciente a plataformas de reconocido prestigio.

La estación de trabajo estará instalada en las oficinas del Regulador.

c) Red LAN

La Red de Area Local, será administrada por un switch de 8 puertos el cual deberá soportar una velocidad mínima de 100 Mbps.

La LAN del SMTR será altamente confiable y segura, y considerando que estos equipos tienen larga vida (20 años), el sistema de cableado estructurado considerará los estándares ANSI/EIA/TIA (American National Standards Institute / Electronic Industries Alliance / Telecommunications Industry Association) para integrar expansiones futuras, para lo cual emplearán armarios repartidores (racks) modulares. Todos los terminales serán identificados en concordancia a los planos de ingeniería de detalle.

d) Impresora laser

La impresora Láser a color será de una resolución de 1200dpi y capacidad de impresión en tamaño.

e) Linea dedicada de comunicación de datos

Con la finalidad de contar con un medio de comunicación dedicada entre el Centro de Control del Coordinador y el SMTR se requiere contratar una línea de comunicación de datos dedicada de 256kbps de ancho de banda.

4.2.4 Suministros complementarios

a) Cables, bandejas, tuberías

- **Cables**

Los cables de alimentación de energía eléctrica deben ser de un solo fabricante y su sección en mm2 deberá corresponder al tipo de carga y caída de tensión permitida. Los cables de conducción de energía eléctrica y los cables de comunicación deben ser instalados separadamente, debe evitarse en lo posible el cruce de los cables y el recorrido entre los dos puntos de unión de los cables será

lo mas corto posible y sin empalmes. Los conductores se fijarán con sujeta cables (cintillos de plástico transparente) si se colocan en colgadores, canastillas o canaletas.

El cableado interno de los tableros de control será de acuerdo a los planos de ingeniería aprobados y diferenciados por grupos de acuerdo al nivel de tensiones en VAC y VDC. En ambos extremos de cada cable se instalarán sistemas de numeración y letras permanentes.

- **Bandejas**

Las bandejas, canastillas o colgadores serán de PVC y del mismo color en todas las instalaciones, y serán los que conduzcan grupos de cables

- **Tuberías**

Se debe utilizar un tipo de tubería para interior, exterior y enterrado. Para las instalaciones interiores se utilizará tuberías PVC SAP. En las instalaciones exteriores se utilizará tuberías conduit metálico con sus acoples metálicos correspondientes. Todas las tuberías serán fijadas a cajas terminales selladas herméticamente.

b) Sistemas de puesta a tierra

Se utilizará el sistema de puesta a tierra del que utiliza el área informática del OSINERG el cual es menor o igual a 5 ohms.

c) Medio ambiente y estandares

- **Condiciones ambientales**

El lugar físico donde se instalará el SMTR está ubicado en la zona urbana de Lima Metropolitana el cual tiene una variación en la temperatura entre 10 y 30 ºC y una humedad relativa que alcanza a los 99%.

- **Estándares aplicables**

Todo el equipo y materiales serán seleccionados, diseñados y dimensionados para operar bajo condiciones severas de servicio y para mantener una alta tasa de disponibilidad operacional del sistema y de los equipos.

El sistema SCADA cumplirá con la versión actual de los estándares aceptados en la industria, pero no limitado, a los listados a continuación:

- NEC – Código Eléctrico Nacional (National Electric Code) – 1993

- ISA – Sociedad de Instrumentos de América (Instrument Society of America)

  S5.1 - Símbolos e identificación de instrumentación.

  S5.4 - Diagramas de lazo de instrumentos.

  S26 - Prueba de respuesta dinámica de la instrumentación de control del proceso.

  S50.1 - Compatibilidad de señales analógicas para instrumentos del proceso industrial electrónico.

  S51.1 - Terminología de la instrumentación del proceso.

  RP60.08 - Guía eléctrica para los Centros de Control.

- Guías IEEE para la Documentación del Software de Computadora para Tiempo Real y Sistemas Interactivos.
- IS/OSI - International Standard/Open System Interconected.
- OPC - OLE for Process Control.
- LAN Local Area Network.
- WAN Wide Area Network.

4.3 Pruebas del Sistema SCADA

Se requiere que se efectúen pruebas en fábrica y en campo. Los planes y procedimientos de pruebas serán diseñados de manera que el personal del REGULADOR pueda participar en la realización de las pruebas.

Para cada uno de las pruebas a ejecutar, el protocolo de pruebas incluirá lo siguiente:

Para la realización de las pruebas, se dispondrá con la información siguiente:

- Documentación completa (Manuales, Especificaciones Técnicas, etc.).
- Descripción del equipamiento a utilizar en cada prueba.
- Esquema de bloques de la configuración en prueba.

4.3.1 Definición de condición de operación del sistema

Se definen las condiciones de Operación Normal y de Emergencia con el fin de observar el desempeño del SMTR bajo diferentes niveles de actividad que se presentarán durante su operación.

a) Operación normal

Se considera condición normal de operación si un lapso de 30 minutos el SMTR mantiene su nivel de utilización del sistema y los tiempos de respuesta con el operador igual o por debajo de las condiciones establecidas a la simulación en las pruebas en fábrica y pruebas reales en durante las pruebas de aceptación en sitio.

Una condición normal de operación se define si durante 15 minutos se soporta un tráfico de 200 registros/segundo.

b) Operación en emergencia

El sistema se encuentra en operación de emergencia si el lapso de 15 minutos el SMTR mantiene su nivel de utilización del sistema, tiempos de respuesta con el operador y continúa barriendo debajo de los tiempos de respuesta establecidos considerando un tráfico de 500 registros/segundo.

4.3.2 Pruebas en fábrica

Antes del inicio de las pruebas en fábrica (FAT Factory Aceptante test), se debe disponer de todo el hardware y software perteneciente al proyecto, y se debe contar con el plan de pruebas respectivo. En la FAT no se podrán utilizar equipos o cables de reemplazo.

El sistema SCADA estará listo para su traslado e instalación en campo si los resultados de las pruebas en fábrica son satisfactorios. Los resultados de estas pruebas serán contrastadas con las pruebas en campo.

Durante las pruebas FAT se efectuará todas las pruebas que estarán basadas en el plan de pruebas, que demuestren que el sistema operativo, el software SCADA y cada módulo del software se encuentran completamente operativos de manera individual y conjunta en la plataforma de computo.

a) Prueba de utilización del sistema

Se efectuará la medición de Utilización del Sistema, para las condiciones de operación normal y emergencia, utilizando programas de diagnóstico apropiados y certificados. Los porcentajes de utilización no deben exceder en promedio lo establecido en la Tabla Nº 4.2, para un período de 15 minutos.

Nº	Descripción del entorno	Utilización	
		Normal	Emergencia
1	Utilización de la CPU del servidor	30%	45%
2	Utilización de la CPU de la estación de trabajo	30%	45%
3	Utilización de la memoria masiva	30%	45%
4	Utilización del enlace LAN	30%	45%

Tabla Nº 4.2: Utilización del sistema

b) PRUEBAS DE DESEMPEÑO DEL SISTEMA SCADA

Mediante estas pruebas (en lo que sea aplicable) se verificará los tiempos de respuesta del sistema SCADA, Tabla Nº 4.3.

Los tiempos de barrido para los diversos tipos de puntos, serán configurables por el operador y los cambios de estado considerados graves, serán tratados por excepción y presentadas al operador en menos de 3 segundos.

Los tiempos de la Tabla N° 4.3, no consideran los tiempos de retraso del sistema de comunicaciones.

Nº	Descripción de la acción	Tiempos máximos	
		Normal	Emergencia
1	Respuesta al llamado de despliegues	≤ 1.0 s	≤ 1.5 s
2	Respuesta a cambios de estado	≤ 3.0 s	≤ 3.5 s
3	Barrido general puntos de estado	≤ 10.0 s	≤ 20 s
4	Barrido general puntos análogos	≤ 10.0 s	≤ 20 s
5	Respuesta a telemando desde la consola del	≤ 2.0 s	≤ 2.50 s
6	Respuesta de subsistema de reportes	≤ 1.5 s	≤ 2.00 s
7	Panning suave en 1/8" de la pantalla	≤ 0.5 s	≤ 0.50 s
8	Paso en el zoom	≤ 0.5 s	≤ 0.50 s
9	Actualización en el drag and drop	≤ 0.5 s	≤ 0.50 s
10	Firma en consola por usuario	≤ 5.0 s	≤ 5.00 s
11	Despliegues de resumen de alarmas y eventos	≤ 2.0 s	≤ 3.00 s
12	Presentación de las curvas de tendencia	≤ 3.0 s	≤ 5.00 s

Tabla Nº 4.3: Tiempos de respuesta del sistema

c) Tiempos de recuperación del SMTR

La Prueba Tiempos de Recuperación del Sistema considera eventos razonables que se presentan en la operación del SMTR y verificar los tiempos de recuperación requeridos (ver Tabla Nº 4.4).

Nº	Descripción del evento	Tiempo
1	Arranque total en frío	≤ 300 s
2	Rearranque en caliente del servidor y estación de trabajo	≤ 240 s
3	Reingreso de la estación de trabajo (no incluye período de	≤ 240 s

Tabla Nº 4.4: Tiempos de recuperación

d) Tiempos de carga y mantenimiento del software

Los tiempos máximos de carga, actualización y mantenimiento que se requieren para tener completamente operativos los servidores SMTR, las estaciones de trabajo y actualización de la base de datos del sistema se muestran en la Tabla Nº 4.5

Nº	Descripción de la Acción	Tiempo
1	Regeneración completa de la base de datos (50,000	≤ 0.50 h
2	Carga completa del servidor	≤ 2.00 h
3	Carga completa de la estación de trabajo	≤ 1.50 h
4	Reconstrucción parcial del servidor	≤ 0.75 h
5	Reconstrucción parcial de la estación de gráfica	≤ 0.75 h
6	Integración de despliegues	≤ 0 25 h

Tabla Nº 4.5: Tiempos de carga y mantenimiento

4.3.3 Pruebas de aceptación en sitio (SAT)

Culminada la instalación de todo el equipamiento en campo, se iniciará las pruebas SAT, que se cumplirán en cuatro etapas: pruebas de instalación, integración, performance y 168 horas de operación continua.

Antes de empezar estas pruebas el proveedor deberá asegurarse que se han efectuado los cambios finales de ingeniería pendientes y se han ejecutado los trabajos a ser culminados para la etapa de prueba en el campo.

a) Prueba de instalación en campo

Durante esta etapa se efectuará las siguientes pruebas:

- Se efectuará la carga completa de un servidor del sistema SCADA, con la finalidad de comprobar la exigencia de tiempos indicado en la Tabla Nº 4.5.
- Deberá demostrarse que todo el equipamiento está operativo mediante la ejecución de diagnósticos en y fuera de línea.
- Se efectuará las pruebas de punto a punto para verificar las variables físicas provenientes del campo.

b) Prueba de integración en campo

Mediante esta prueba se demostrará que el nuevo sistema SCADA instalado en el REGULADOR, el sistema de comunicación instalado y todas señales se encuentran completamente integrados y operando en completa sintonía.

Durante esta etapa se completará aquellas pruebas que no pudieron ser probadas en fábrica y se ejecutarán nuevamente algunas pruebas FAT con la finalidad de validar los resultados.

c) Prueba de performance

Se desarrollara y programará parcialmente las pruebas de utilización del sistema (Tabla Nº 4.2), Pruebas de Desempeño (Tabla Nº 4.3), Tiempos de Recuperación (Tabla Nº 4.4) y Tiempos de Carga y Mantenimiento del Software (Tabla Nº 4.5) con la finalidad de comprobar la respuesta del SMTR en condiciones reales de operación.

d) Prueba de 168 horas de operación

Mediante estas pruebas se verificará que el software esta libre de errores y que el hardware opera sin fallas y armoniosamente con el software por un período continuo de 168 horas luego de haberse completado con éxito la prueba de Desempeño en el Campo. Esta prueba será calificada como exitosa si el sistema no pierde ninguna función crítica ni algún componente principal de hardware y si no se presentan reinicios automáticos del sistema. Las fallas calificadas como mayores en hardware y software (pérdida de una función) y luego del diagnostico respectivo, dará lugar a que se corrija la discrepancia para luego reiniciar una nueva prueba de 168 horas.

Esta prueba se realizará con todo el sistema en operación (SCADA y Comunicaciones) y se efectuarán simulaciones de condición de emergencia por lo menos una vez al día y a cualquier hora. El proveedor del SMTR deberá listar en su oferta las funciones y hardware que son críticos en el sistema que ofertan.

e) Prueba de disponibilidad del sistema

Esta prueba se efectuará luego de completarse satisfactoriamente la prueba de las 168 horas, y será por un periodo de 21 días calendarios; cuya finalidad es la

de comprobar la disponibilidad del sistema, así como verificar la confiabilidad del hardware y software.

El cálculo de disponibilidad se efectuará utilizando la siguiente ecuación:

$$\text{Disponibilidad (\%)} = \frac{(504 - \text{Tiempo Total de Parada})}{504} \times 100$$

Se considera Tiempo Total de Parada (TTP) a la suma de todos los tiempos en horas en las cuales ha estado indisponible alguna función crítica y/o equipo o el sistema completo.

La disponibilidad del sistema no deberá ser inferior al 99.9%

4.4 El SMTR del Regulador implementado

Siguiendo las pautas indicadas en los numerales anteriores del presente capitulo se implemento satisfactoriamente el SMTR del Regulador lográndose acceder a información operativa del Coordinador del SEIN para supervisar el estado operativo del SEIN a través de información transparente, para ello el Regulador se ha enlazado al COES-SINAC mediante una línea dedicada y se ha interconectado a la red ICCP del SEIN (RIS). De esta manera tiene información de las unidades de generación, de las instalaciones de transmisión y en cierto nivel instalaciones de distribución que forman parte del SEIN.

4.4.1 Alcances de los trabajos realizados como parte de la implementación del SMTR

Se ha efectuado el diseño, instalación, integración, pruebas y puesta en servicio del hardware y software del sistema de información de tiempo real y del sistema de comunicaciones necesarios a fin de disponer del **SMTR** que permite al Regulador disponer puntualmente la información en tiempo real del SEIN a partir de la información que maneja el Coordinador de la operación en tiempo real del SEIN (COES-SINAC).

4.4.2 Configuración del SMTR

Los datos de campo provenientes de las empresas integrantes del SEIN, son reenviados desde el Coordinador del SEIN al SMTR del OSINERG, tal como se muestra en la Figura Nº 4.1.

4.4.3 Trabajos efectuados

- **Línea dedicada**

El enlace dedicado entre el Regulador y el COES-SINAC es de 256 kbps de ancho de banda.

El tráfico observado por la línea dedicada en promedio es de 75 kbps es decir es inferior al 30% del ancho de banda. En ese sentido no se ha presentado congestión en la transferencia de datos.

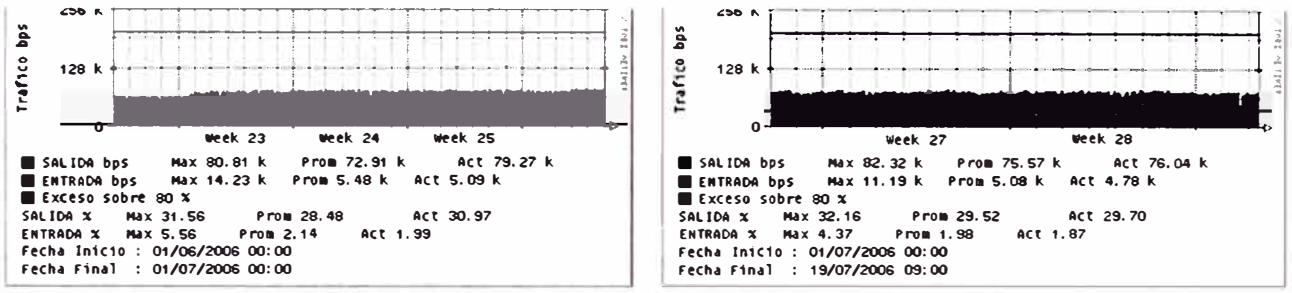


Figura Nº 4.2: Utilización del enlace dedicado Regulador –Coordinador

- **Estructura de la red SCADA**

La implementación del sistema de adquisición abarca el suministro de todo el software, hardware, servicios de ingeniería y demás recursos que permitan que el conjunto denominado SMTR cumpla con el objetivo de acceder y monitorear la información en tiempo real que utiliza el Coordinador.

- **Software SCADA**

  - El subsistema Interfase Gráfica del SMTR es totalmente gráfico (Full Graphics), con múltiples opciones de manejo de pantalla, capacidad de panning, decluttering y zooming continuos y con capacidad de introducir gráfico de tendencias, imágenes, acceder a registros de la base de datos.
  - Capacidad para operar en diferentes arquitecturas redundantes
  - Capacidad de utilizar diferentes medios de comunicación
  - Sistema SCADA modular
  - Interface gráfica versátil.
  - Procesamiento de alarmas

- Manejo de protocolos abiertos

- **Se han implementado 7350 puntos en la base de datos nativa del SCADA**
- **Se han efectuado pruebas en fábrica y pruebas de aceptación en sitio. Entre las pruebas de aceptación en sitio que se efectuaron son:**
  - Pruebas de instalación en campo
  - Pruebas de integración en campo
  - Pruebas de performance.
  - Prueba de 168 horas de operación.
  - Pruebas de Disponibilidad del Sistema.

Los resultados de las pruebas fueron satisfactorios y los resultados estuvieron dentro de las tolerancias que se indicaron en el presente capítulo en el numeral referido a las pruebas.

- **Interfaz grafica**

Posee una potente interfaz gráfica. Se ha implementado el diagrama unificar del SEIN, así como de un mapa georeferenciado.

Figura Nº 4.3: Interfaz Gráfica del SMTR

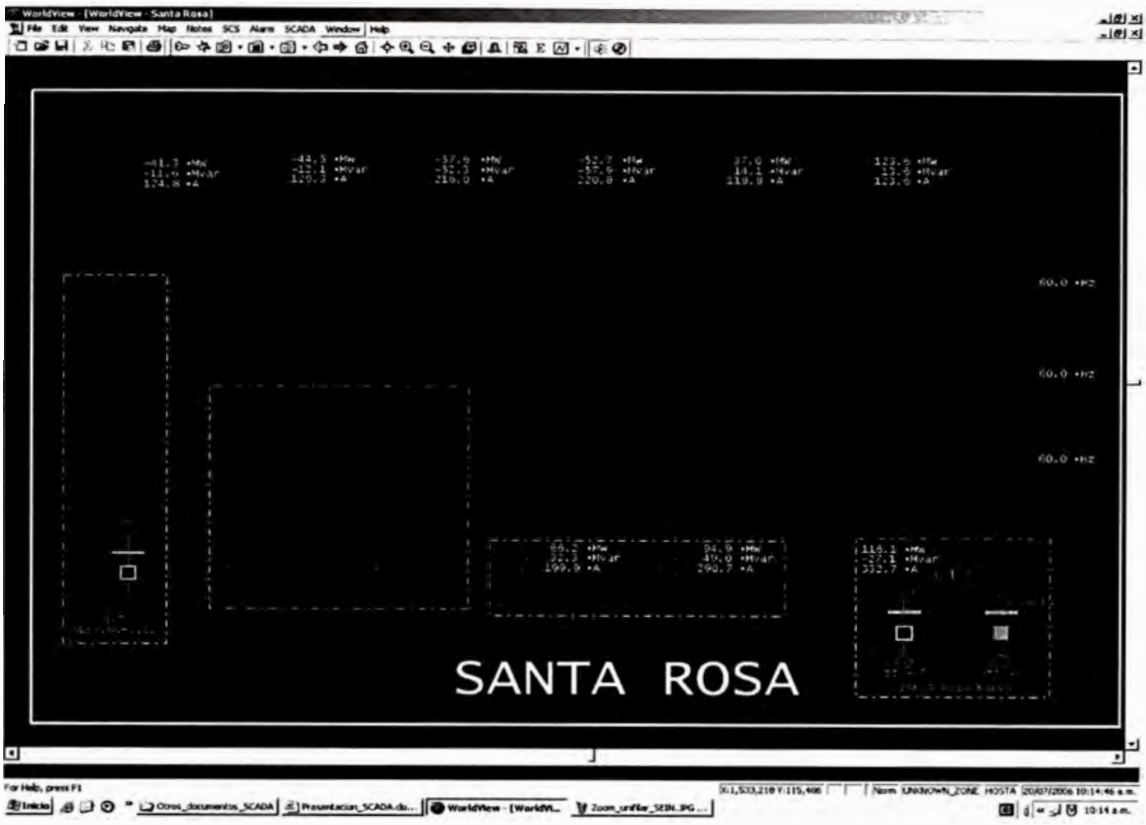


Figura Nº 4.4: Diagrama Unificar de la Subestación Santa Rosa

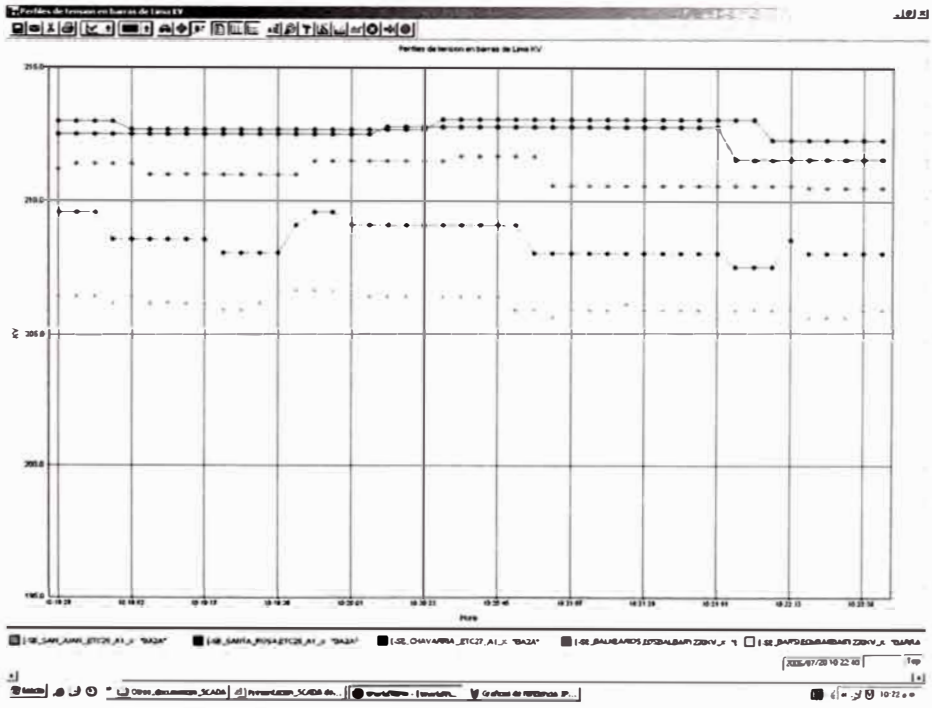


Figura Nº 4.5: Curvas de tendencias de los perfiles de tensión en las principales barras de 220 kV de Lima

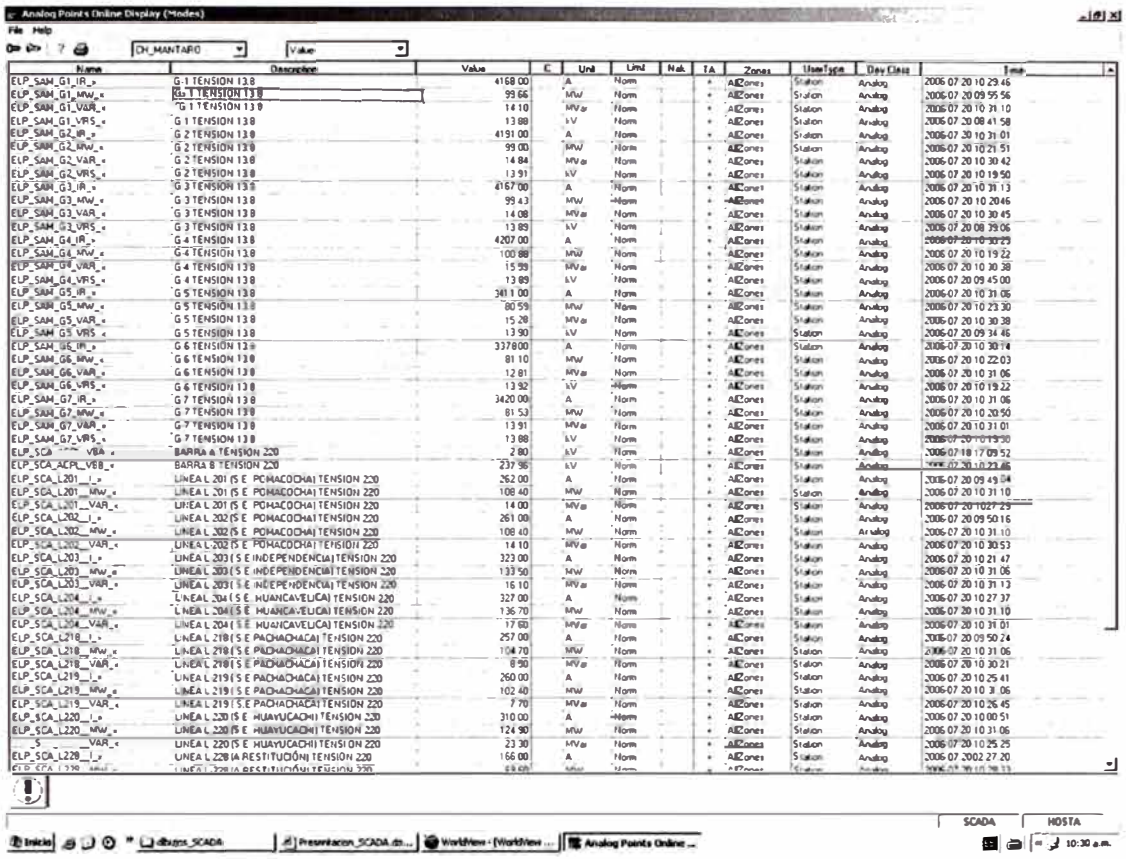


Figura Nº 4.5: Explorador del Sistema SCADA

4.4.4 Aplicaciones del Sistema de Monitoreo en Tiempo Real del Regulador

La implementación del Sistema de Monitoreo en Tiempo Real, permite al Regulador, contar con una herramienta muy importante para supervisar el estado operativo del SEIN utilizando información transparente y oportuna.

Entre otras aplicaciones se podrá efectuar lo siguiente:

- Diagnóstico de los niveles de sobrecarga de los transformadores del SEIN.
- Diagnóstico de las congestiones en la red de transmisión.
- Evaluación de los perfiles de tensión registrados en las principales barras del SEIN.
- Seguimiento a los niveles de reserva rotante programados y ejecutados.
- Registro de ocurrencia de eventos del SEIN.
- Verificación de la adecuada transferencia de información en tiempo real de los integrantes del SEIN al Coordinador.

En el **Anexo B** se adjunta información adicional respecto las aplicaciones del Sistema de Monitoreo en Tiempo Real del Regulador.

4.5 Base de Datos Histórica y Aplicativo para generar reportes

Luego de tener implementado el SMTR del Regulador se requiere efectuar el diseño de la base de datos histórica y el aplicativo para generar reportes. Se ha observado que se dispone de 2 niveles de almacenamiento de información de la base de datos de tiempo real:

- Base de datos propietaria para la información circular de tiempo real configurable por rangos de tiempo a periodos establecidos para mantener un tamaño de base de datos controlable, esta base de datos esta desarrollada por el mismo fabricante del software y optimizada para su propio fin, no pudiendo estar disponible para acceder libremente desde aplicaciones externas.

- Opción de almacenamiento a una Base de Datos externa para implementación de requerimientos propios, esta opción se realiza a través del modulo de trascripción. Este ultimo ha sido implementado en tablas no normalizadas no pudiendo se flexible el desarrollo de algún aplicativo de análisis de información.

- La propuesta de desarrollo seria la posibilidad de implementar el almacenamiento externo a través de Store Procedures (en adelante SP), en estructuras de tablas ordenadas que vendrían a tener una funcionalidad como de tablas circulares generadas por día, y a través de estas mismas SP, generar los índices necesarios.

  Debe contemplarse un modulo de importación de las tablas circulares.

En la implementación de SCADA's, Sistemas EMS (administracion de la Gestion de Energia) y demas Sistemas de Tiempo Real, generalmente las empresas proveedoras de estos software recomiendan como uso del Oracle y SQL Server como principales motores de Bases.

Los sistemas operativos que actualmente representan los entornos mas usados para la implementación de base de Datos son el Windows Server 2003

El Sistema operativo a utilizar seria el Windows Server 2003 por ser un sistema operativo que se administra fácilmente y tiene una alta confiabilidad, a diferencia del Linux que se tendría que tener continuamente un soporte de personal muy calificado con la consecuencia de un elevado costo de mantenimiento.

De los dos motores de bases de Datos mencionados el SQL Server 2005 se acondiciona mejor a la necesidad de la presente implementación ya que se dispone de mayor cantidad de personal calificado que permitirían un soporte adecuado a un tiempo y costo razonable, adicionalmente es el mejor base de datos sobre la plataforma Windows sobre el mismo tipo de Servidor hardware.

La base de datos y el aplicativo del Regulador debe de considerar las siguientes premisas.

- Ser una base de datos sólida, desarrollada por el mismo proveedor del Sistema Operativo que es el Windows Server 2003.
- Tiene una gran base instalada en el País, por lo que el soporte es más económico y existen mas empresas que lo utilizan.
- Soporta implementación nativa de aplicativos compilados para del Net Framework.

4.5.1 Lenguaje de programación a usar

Analizando los Sistemas de Supervisión y SCADA, se llega a la conclusión que las herramientas utilizadas para desarrollar este pueden ser agrupados en tres entornos:

- Modulo Central (Core) de administración de la adquisición de todos los canales (puntos de medición); que por necesidad de procesar datos a alta velocidad y volúmenes grandes de información se utiliza el lenguaje C++, como generalmente todos los sistemas operativos disponen de compiladotes de C++ para generar código binario que ejecuta directamente instrucciones para el hardware. Esto hace posible la implementación de la base de datos de tiempo real que viene a ser una base de datos jerarquerizada en memoria para administrar y procesar fácilmente la información del SCADA.
- Módulos de la Estaciones de trabajo de los usuarios; donde se visualizan la información a través de Human Machine Interface (HMI) para ver el estado de los canales de información en pantallas con diagramas con rico contenido visual y también pantallas de administración de la información de todo el SCADA. Estos módulos son desarrollados utilizando también el C++ y utilizando otros lenguajes y herramientas que permitan fácilmente la interacción y algunos módulos también requieran procesos que demanden altos volúmenes de datos.

- Módulos de acceso Web; que vienen a ser unas extensiones de los módulos de estaciones de trabajo pero estas utilizando un aplicativo cliente Web. Estos últimos referidos a modulo que no necesitan procesamiento que requiera volúmenes grandes de información o velocidades importante de procesamiento, que normalmente son reporte finales de consolidados que utilizan tablas intermedias procesadas previamente por módulos mas potentes. Estos módulos normalmente utilizan lenguajes mas difundidos de nivel de aplicación Web como el PHP, APS.NET, Servlet JSP ,etc , o utilizando implementaciones de J2EE o .NET a través de .conexiones directas de sockets, Web Services o Net Remoting.

  El lenguaje a usar para desarrollar este modulo depende:

  - Del ENTORNO donde este va a ser ejecutado, y
  - Del RECURSO HUMANO disponible que va ha desarrollarlo.

  De los lenguajes disponibles a utilizar se visto que desde el punto de vista de desarrollo SERIO, normalmente las empresas de desarrollo implementan sobre lenguajes basados en C++, dentro de mas extendidos podrían ser los lenguajes C# o el Java.

  Debe elegirse el Lenguaje que a todas luces debe conducir al objetivo primordial de lograr el éxito de la implementación a desarrollarse.

  Los entorno donde el aplicativo va ha interactuar son:

  - El Servidor de Base de Datos a usar es el SQL Server 2005.
  - Sistema Operativo Server Windows 2003.

  Debe tomarse en consideración sobre las implementaciones de accesos a datos disponibles para Windows (el aplicativo cliente correrá sobre el Windows) se tienen los estándares ODBC, JBC, OLE DB y los Data Provider de Net. Estos últimos son implementaciones nativas de los mismo fabricantes de los motores de bases de Datos para que las funcionalidades y velocidades de acceso sean las mas optimas sobre la Plataforma .Net.

  De ellos el Visual C# permite mayores ventajas de implementación sobre el SQL Server 2005, adicionalmente que es el mismo fabricante de ambos productos, esto pro que ya existe una compatibilidad nativa entre ellos.

El C# se implementa sobre la Plataforma .Net y como el SQL Server 2005 está totalmente integrado en .NET Framework y permite la creación de procedimientos almacenados, funciones y tipos y agregados definidos por el usuario mediante el lenguaje de programación .NET. Todas estas construcciones pueden aprovechar gran parte de la infraestructura de .NET Framework, la biblioteca de clases base y las bibliotecas administradas de terceros.

Respecto al uso del Lenguaje JAVA, en nuestro medio en la implementaciones de Sistemas de Supervisión / SCADA en el Sector Eléctrico no existe programas y tampoco experiencia de empresas en el desarrollo de este tipo de aplicación de Tiempo Real (Alta disponibilidad con altos volúmenes de información y procesamiento las 24 horas del día y los 365 días del año), en cambio si existen empresas como el del Coordinador COES, que tienen implementaciones desarrolladas en C#.

Acerca de los recursos humanos disponibles, existen pocas empresas que implementación soluciones en Java comparado con los disponibles en C#.

Adicionalmente que los que implementan las soluciones en JAVA están orientados mas Sistemas de Información con énfasis en procesos transaccionales y muy poco en Sistemas de Tiempo Real, disminuyendo la probabilidad de éxito utilizando este lenguaje.

De todo lo anterior tomando en cuenta el Entorno de ejecución de la aplicación y el mejor recurso humano disponible se recomienda para el desarrollo de esta aplicación el uso del Visual C#.

4.5.2 Modulo de Transcripción

El SMTR del REGULADOR recoge la información de todo el SEIN a través del Coordinador y este desde todas las empresas eléctricas utilizando el protocolo ICCP – TASE 2. (ver Figura Nº 4.6)

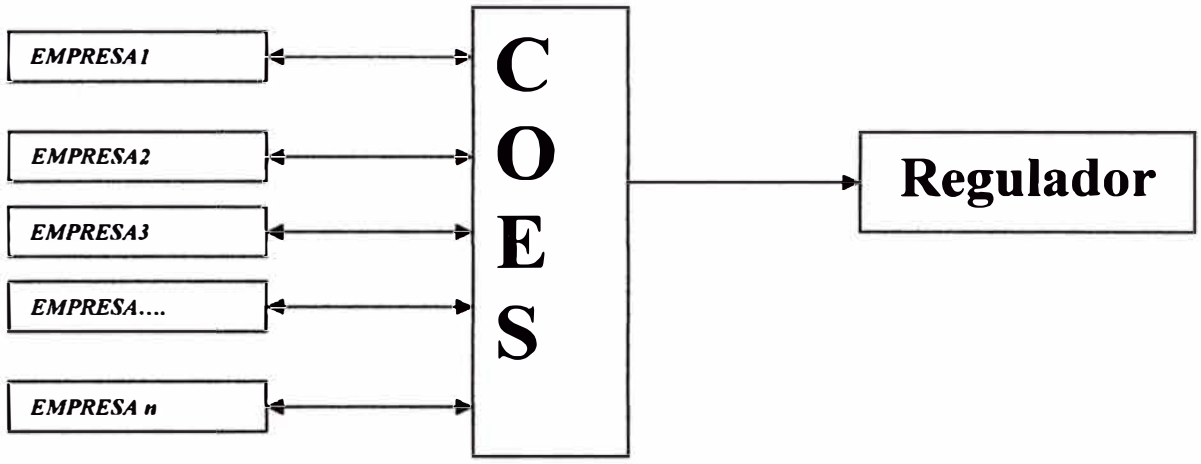


Figura Nº 4.6: Flujo de Transferencia de Información en Tiempo Real

El modulo de Transcripción del SCADA del Regulador, es implementada para generar a un repositorio externo de la información procesada en el SCADA este repositorio es una base da datos que es este caso seria el SQL Server 2005, esta información externa se puede configurar para la generación de históricos cada determinado tiempo o por eventos (ver Figura Nº 4.7).

Este modulo tiene varias maneras de enviar información a la base de datos:

- Valores Actuales - current data
- Datos Históricos - Historical Data
- Registro de operaciones - Operations logs.
- Datos de eventos – event data (including SOE).

Se debe realizar un estudio de cual de las anteriores formas es la más adecuada para la implementación de la solución de tiempo real.

Esta implementación deberá utilizar de manera optima el modulo de transcripción para:

- Limitar el espacio de la información generada por el módulo de transcripción, ya que este solo inserta información.
- Prever conflictos por concurrencia de transacciones en las mismas tablas de actualización.

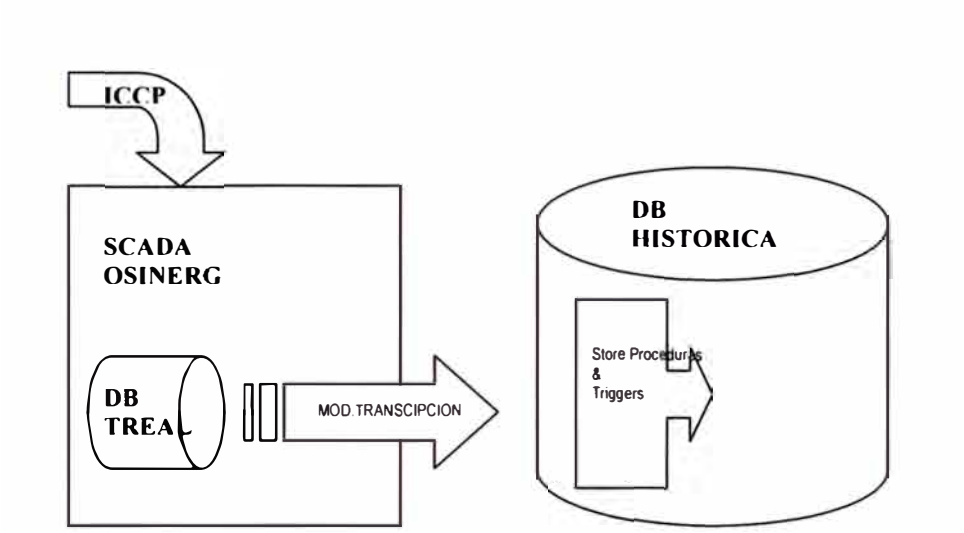


Figura Nº 4.7: Flujo de Transcripción de información

4.5.3 Modelo de base de datos para histórico SCADA y análisis de la información

La base de datos para el almacenamiento histórico debe estar diseñada de tal modo que se puedan realizar consultas, backups, y restauraciones de toda la información de tiempo real de una manera fácil.

Adicionalmente se debe realizar cálculos en tiempo real de índices que permitan los análisis del estado de todos los canales de datos recibidos en el SCADA.

La solución a desarrollar e implementar debe implementar básicamente:

- Generar las tablas ordenadas de la información de SCADA para que su mantenimiento y manipulación permitan el uso flexible por fechas.
- Adicionalmente debe implementarse el procesamiento de la información de la frecuencia a nivel de resolución que almacena el COES para el análisis de contingencias de eventos y de la NTCSE respecto a la frecuencia. (este no incluye el procesamiento a los índices de calidad de la frecuencia).
- La solución debe mantener el espacio del almacenamiento en forma de que no llegue a bloquearse por capacidad de disco, debe implementar mensajes/alarmas que prevengan al personal de mantenimiento de la base de datos realizar los backups.
- Prever formas de almacenamiento externo para que no se pierda información en caso deterioro de algún equipo Hardware
- Implementar código sobre la base de datos que permita en análisis en línea de las actualizaciones realizadas para mantener los índices por canal actualizados.

- Analizar la propuesta del COES para el cálculo de disponibilidad de información en tiempo real, de los mínimos técnicos que deben cumplir las empresas como parte de la NTCOTR para implementación de esta.
- Proponer índices que reflejen la calidad de la información que las empresas entregan al coordinador.
- Implementar un Aplicativo Windows para realizar la consultas de toda la información generada y reportes de estado de los canales y estado del envió de información por empresa.

CONCLUSIONES

1. La implementación de un Sistema de Monitoreo en Tiempo Real, permite al Regulador, contar con una herramienta muy importante para supervisar el estado operativo del SEIN utilizando información transparente y oportuna.

2. La evaluación y análisis efectuada en el presente trabajo ha conllevado a elegir el sistema de monitoreo en tiempo real a ser implementado por el Regulador. El cual consiste de un sistema SCADA autónomo escalable y flexible que se adecua a sus requerimientos.

3. La solución que sugiere que el Regulador tenga un sistema SCADA propio es la más adecuada en la medida que por un costo relativamente moderado cuenta con un sistema autónomo que pueda adecuarse a sus necesidades.

4. El Sistema de Monitoreo en Tiempo Real del Regulador es escalable pudiendo tener crecimiento vertical y horizontal, en ese sentido no solamente podrá tener una mayor cantidad de estaciones de trabajo conectadas al sistema o mayor manejo de información, sino también podrá tener mayores funcionalidades y redundancia.

5. El protocolo de comunicación ICCP es el adecuado para la transferencia de información en tiempo real entre centros de control.

ANEXO A

GUIA EPRI (ENERGY POWER RESERCH INSTITUTE – PROTOCOLO DE COMUNICACIÓN ICCP)

ABSTRACT

This Inter-Control Center Communications Protocol (ICCP) User Guide provides important information to ICCP users, both end users and developers. The background and reasoning behind the ICCP protocol (also known as the Telecontrol Application Service Element (TASE.2) are presented. The concepts of ICCP clients and servers, ICCP server and data objects, and other concepts fundamental to understanding ICCP are provided in a tutorial fashion. Help is provided in the use of the ICCP specifications, including many cross references from the guide to the specifications. Many issues facing developers and users of ICCP are also addressed, including most of the areas referred to as "local implementation issues" in the ICCP specifications. This guide is a supplement to rather than a replacement of the ICCP specifications.

Table of Contents

Exhibits

Appendix A Answers to Frequently Asked Questions about ICCP

1. Introduction to User Guide

1.1 Purpose

This User Guide is to provide guidance to users of the Inter-Control Center Communications Protocol (ICCP), otherwise known by its official name of Telecontrol Application Service Element.2 (TASE.2). Throughout this document, the name ICCP will normally be used, except where specific references are made to the IEC standards. In any case, it should be clear that there is only one protocol and set of specifications that may referred to as either ICCP or TASE.2

Although a Draft International Standard (DIS) for ICCP currently exists at the time of this writing, it is by necessity written in the style dictated by the International Electrotechnical Commission (IEC), the standards organization sponsoring the DIS. This style has been developed to specify international standards in a precise and unambiguous way so that all implementers will interpret the standard in the same way and thus ensure interoperability between different vendor's ICCP products.

However, the style of the ICCP DIS is not necessarily as readable for someone not intimately familiar with all the background leading up to the development of ICCP. Furthermore, certain types of information very useful to a user of ICCP but not necessary for specifying the protocol or services provided by ICCP have been omitted. Thus the need for this User Guide.

1.2 Intended Audience

The User Guide is intended for a broad audience of readers from an end user trying to decide if ICCP is appropriate for their data transfer needs to a vendor planning to implement ICCP, with the goal of offering an ICCP product. In particular, this guide should be helpful to the following:

- An end user, such as an electric utility, with the need to transfer real-time data to another utility or utilities or to another internal control center, who is trying to evaluate which protocol is most appropriate.
- An end user who already has decided to use ICCP and now needs guidance in how to procure ICCP.
- An end user who has procured ICCP and now is concerned about exactly how to map their actual data into ICCP data objects.
- An end user who is looking for conventions and answers to practical questions regarding configuring ICCP software and networks.
- A vendor with a project to implement the ICCP specification either as a project special or to offer a standard product.

1.3 Organization of Guide

This guide first introduces the background and concepts of ICCP to provide a framework for understanding the ICCP specification. Then the individual server and data objects comprising ICCP are described with cross references into the specification. At this point (i.e., Sections 1-8) the reader should have all the necessary foundation understanding to

intelligently use the ICCP specifications. The remainder of the guide (Sections 9-20) address practical issues that arise in connection with the use of ICCP. Appendix A is a collection of Frequently Asked Questions (FAQs) of interest primarily to developers of ICCP products which were originally collected into a preliminary Implementor's Guide.

1.4 ICCP Version Number

This version of the ICCP User guide applies to ICCP specifications IEC 870-6-503 and 870-6-802 Version 1996-08. This version of the ICCP specifications is also informally known as ICCP Version 6.1. See the References section 4 for more complete identification of the specifications to which this guide applies.

2. Definitions

For the purposes of this User's Guide, the following definitions apply. These definitions are also found in 870-6-503.

Action: An activity performed by the ICCP server under some defined circumstances.

Accounting Information: A set of information which describes an account for a utility. See IEC 870- 6-802 for more details.

Bilateral Agreement: An agreement between two control centers which identifies the data elements and objects that can be accessed and the level of access permitted.

Bilateral Table: The computer representation of the Bilateral Agreement. The representation used is a local matter.

Client: An ICCP user which request services or objects owned by another ICCP user acting as a server. The client is a communicating entity which makes use of the VCC for the lifetime of an association via one or more ICCP service requests.

Data Set: An object which provides services to group data values for singular operations by an ICCP client.

Data Value: An object which represents some alphanumeric quantity that is part of the Virtual Control Center (VCC) which is visible to an ICCP user. Data Values exist as part of the implementation of the control center and represent either real entities within the utility such as current, or derived values calculated in the control center. Data Value objects include services for accessing and managing them.

Instance: An implementation of ICCP executed in either the client or the server role.

Interchange Schedule: A set of information that specifies how energy is transferred from one system to another. See IEC 870-6-802 for more details.

Object: An abstract entity used to implement the ICCP protocol and represent data and optionally provide services for accessing that data within a VCC.

Object Model: An abstract representation that is used for real data, devices, operator stations, programs, event conditions, and event enrollments.

Operation: An activity which is performed by the ICCP server at the request of the ICCP client.

Server: An ICCP user that is the source of data and provides services for accessing that data. An ICCP server behaves as a VCC over the lifetime of an association.

Service: An activity which is either an ICCP action or operation.

Tagged: The term tagged is derived from the practice of putting a physical tag on a device as it is turned off for servicing or locked out from network access as a safety measure. The ICCP term tagged is used to signal such a condition to the ICCP user.

Time Series: A set of values of a given element that is taken at different times as specified by a single time interval. A time series is implemented through the transfer set mechanism as defined within this specification.

Transfer Account: A set of information that associates interchange scheduling information with either hourly or profile data.

Transfer Conditions: The events or circumstances under which an ICCP server reports the values of a data set, values in a time series, or all transfer account information.

Transfer Set: An object used to control data exchange by associating data values with transmission parameters such as time intervals, for example. There are four types of Transfer Sets: Data Set Transfer Sets, Time Series Transfer Sets, Transfer Account Transfer Sets, and information Message Transfer Sets.

User: An implementation of ICCP executed in either the client or the server role.

Virtual Control Center (VCC): An abstract representation of a real control center which describes a set of behavior with regards to communication and data management functionality and limitations. VCC is a concept taken from the underlying MMS services.

3. Abbreviations

ACSE	Association Control Service Element
API	Application Program Interface
BCD	Binary Coded Decimal
COV	Change Of Value
DIS	Draft International Standard
EPRI	Electric Power Research Institute
HLO	Hot line order
ICC	Inter-Control Center
IDEC	Inter-utility Data Exchange Consortium
IEC	International Electrotechnical Commission
IP	Internet Protocol
KQH	Kilovar hour readings
KWH	Kilowatt hour readings
LFC	Load Following
MMS	Manufacturing Messaging Specification
MOD	Motor operated disconnect
PDU	Protocol Data Unit
QOS:	Quality of Service
RBE	Report by Exception
ROSE	Remote Operations Service Element
TAL	Time Allowed to Live
TASE	Tele-control Application Service Element, IEC's designation of an international standard protocol for utility data exchange.
TASE.1	TASE based on the ELCOM-90 protocol.
TASE.2	TASE based on the ICCP protocol.
TCP	Transmission Control Protocol
TLE	Time Limit for Execution
TOD	Time of Day
UCA	Utility Communications Architecture
UCS	Utility Communications Standards working group
UDP	User Datagram Protocol

VCC	Virtual Control Center
VMD	Virtual Manufacturing Device
WSCC	Western System Coordinating Council
WEICG	WSCC Energy Management Systems Inter-utility Communications Guidelines

4. References

The following documents are recommended to the reader of this User's Guide. More technical documents are referenced in the ICCP standards themselves.

1. ISO/IEC DIS 870-6-503: TASE.2 Services and Protocol, Version 1996-08. This document is also referred to as ICCP Services and Protocol, Version 6.1, August 1996.
2. ISO/IEC 870-6-702: TASE.2 Application Profiles, Version 5.2, November, 1994. This document will be revised and submitted to the IEC in early 1997.
3. ISO/IEC DIS 870-6-802: TASE.2 Object Models, Version 6.1. This document is also referred to as ICCP Object Models, Version 6.1, August 1996
4. EPRI Inter-Operability Report: ICCP Interoperability Test Version 5.1, EPRI TR-105552, Project 3355-07, Final Report, September 1995.

5. ICCP Introduction

Inter-utility real-time data exchange has become critical to the operation of inter-connected systems within the electric power utility industry. The ability to exchange power system data with boundary control areas and beyond provides visibility for disturbance detection and reconstruction, improved modeling capability and enhanced operation through future security control centers or independent system operators.

Historically, utilities have relied on in-house or proprietary, non-ISO standard protocols such as WEIC, ELCOM and IDEC to exchange real-time data. ICCP began as an effort by power utilities, several major data exchange protocol support groups (WEICG, IDEC and ELCOM), EPRI, consultants and a number of SCADA/EMS vendors to develop a comprehensive, international standard for real-time data exchange within the electric power utilities industry.

By giving all interested parties an opportunity to provide requirements input and to participate in the protocol definition process, it was expected that the final product would both meet the needs of and be accepted by the electric power utility industry. To accomplish this goal, the Utility Communications Specification (UCS) Working Group was formed in September 1991 to:

1. develop the protocol specification
2. develop a prototype implementation to test the specification

3. to submit the specification for standardization
4. to perform inter-operability tests among the developing vendors.

UCS submitted ICCP to the IEC Technical Committee (TC) 57 Working Group (WG) 07 as a proposed protocol standard. Another proposed standard based on ELCOM-90 over ROSE was also being considered by WG-07. TC-57 decided on a multi-standard approach to allow (1) a quick implementation to meet European Common Market requirements by 1992 and (2) also allow long term development of a more comprehensive protocol. The first protocol was designated TASE.1 (Tele-control Application Service Element-1). The second protocol, based on ICCP over MMS, was designated TASE.2.

Successful first implementations of ICCP between SCADA/EMS control centers led to further expansion to allow communications between control centers and power plants. This expansion did not impact the basic services, but did lead to the development of specific power plant objects. These objects have now been incorporated into ICCP.

6. ICCP Overview

6.1 ICCP Concepts

6.1.1 Protocol Architecture

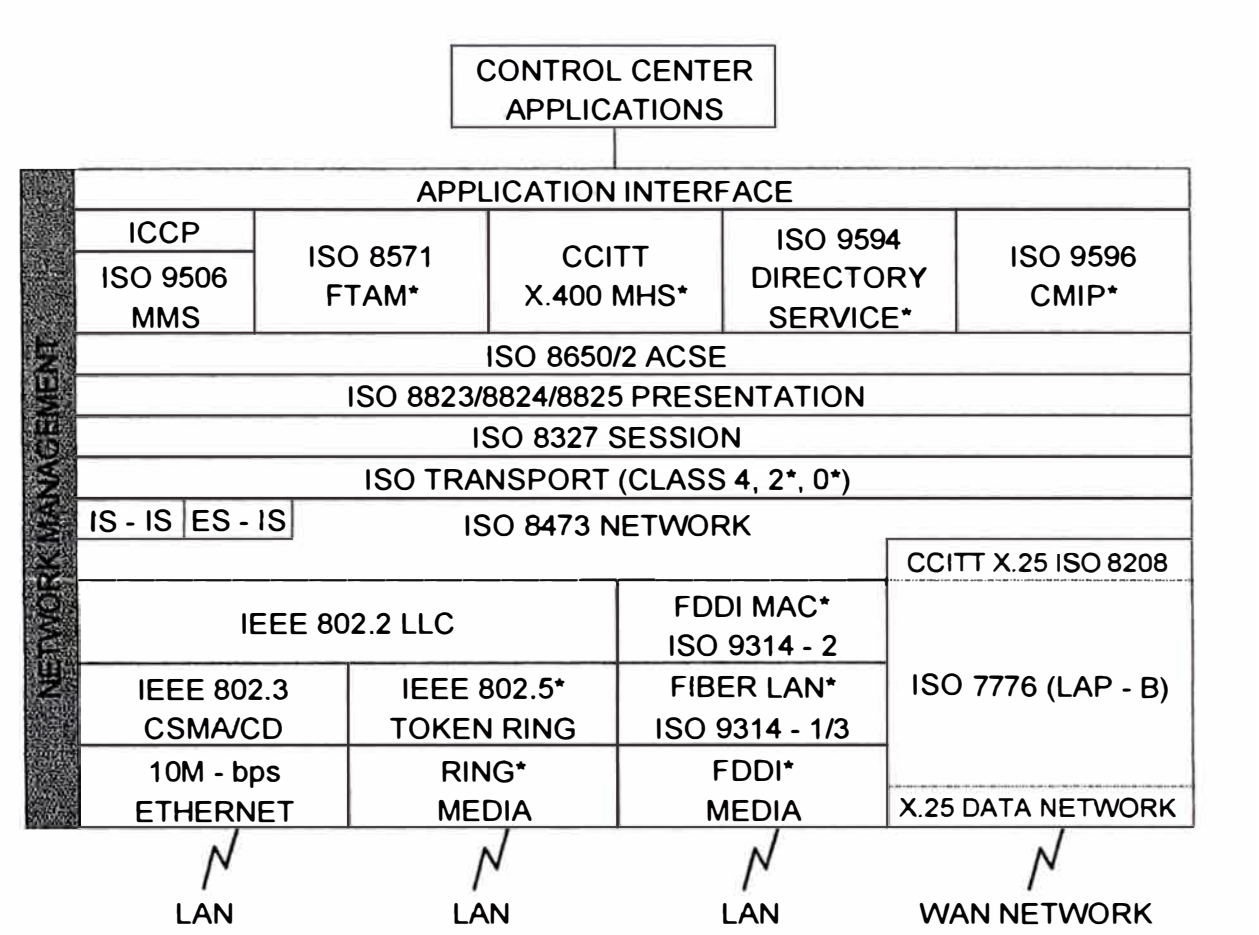
ICCP maximizes the use of existing standard protocols in all layers up to and including the lower layers of layer 7 in the OSI reference model. This has the benefit of requiring new protocol development for ICCP only in the upper sublayer of layer 7.

The protocol stack used by ICCP is the standard UCA Version 1.0 profile with control center applications at the top. ICCP specifies the use of the Manufacturing Messaging Specification (MMS) for the messaging services needed by ICCP in layer 7(see Exhibit 6.1.1-1). MMS specifies the mechanics of naming, listing, and addressing variables, and of message control and interpretation, while ICCP specifies such things as the control center object formats and methods for data requests and reporting. Applications at different control centers, possibly written by different vendors, but both conforming to these mechanics, formats, and methods, may interoperate to share data, control utility devices, output information messages, or define and execute remote programs via an Application Program Interface (API) to ICCP.

ICCP also utilizes the services of the Application Control Service Element (ACSE) in layer 7 to establish and manage logical associations or connections between sites. ICCP relies on the ISO Presentation Layer 6 and Session Layer 5 as well.

At the time this document was prepared, UCA Version 2.0 was in preparation. Early drafts of Version 2.0 include additional subnetwork types in layers 1-2, including Frame Relay, ATM, and ISDN. It also specifies the use of TCP/UDP as an alternative transport protocol (see Section 17 for more detail on transport profiles). Because of the protocol architecture, ICCP is independent of the lower layers, so that as new protocols evolve in the lower layers, ICCP will be able to operate over them with only configuration changes. Thus ICCP is able to operate over either an ISO-compliant transport layer or a TCP/IP transport service, as long as ISO layers 5-7 are maintained.

Exhibit 6.1.1-1, ICCP Protocol Architecture



* Indicates optional function

6.1.2 Application Program Interface (API)

Although an API is shown in Exhibit 6.1.1-1, the API is not specified in the ICCP specification - only the protocol and service definitions are specified and are the subject of standardization. Each vendor implementing ICCP is free to choose the API most suitable for their product or for their intended customers. Exhibit 6.1.2-1 illustrates this concept.

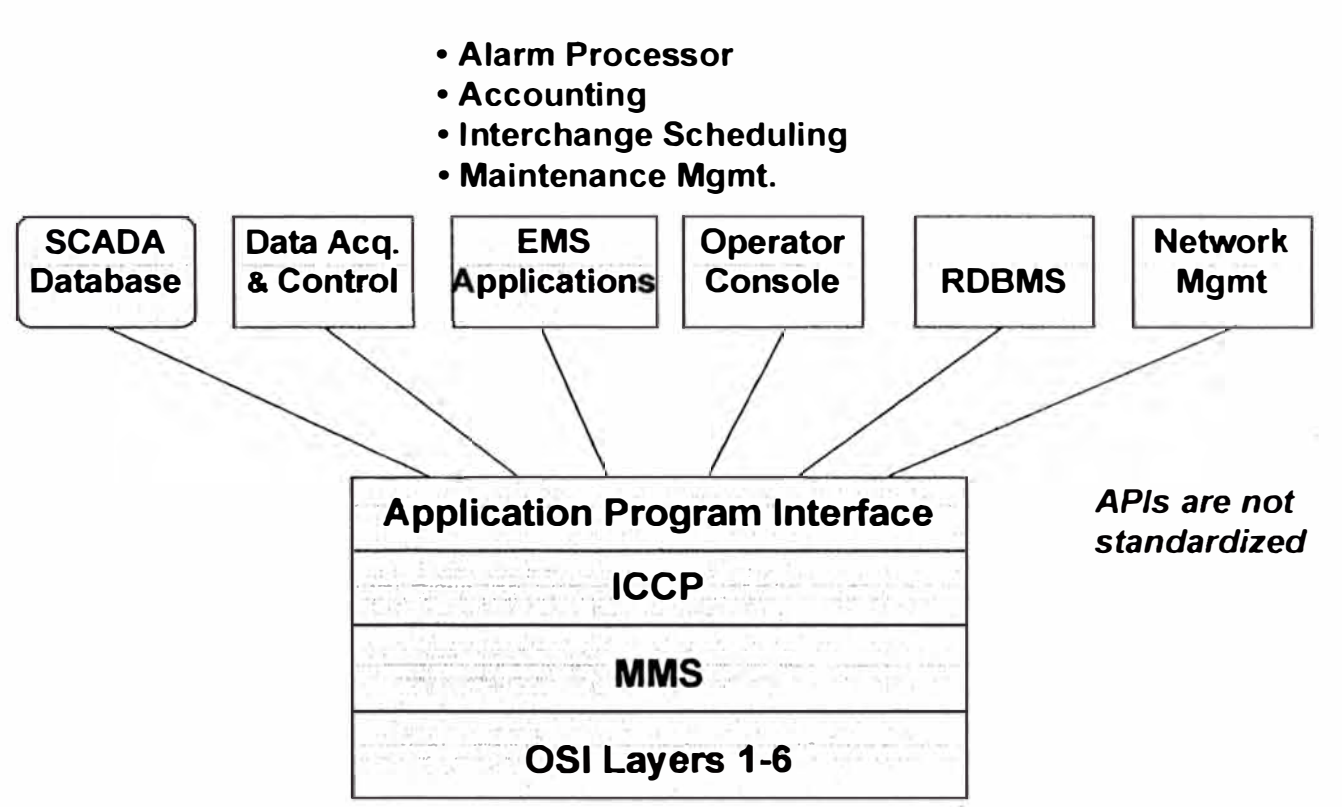
For example, an Energy Management System/Supervisory Control And Data Acquisition (EMS/SCADA) vendor may choose to provide an API optimized for interfacing with several different types of applications, such as:

- A proprietary real-time SCADA database for the storing and retrieving of real-time power system data, such as analogs, status, and accumulator values, on a periodic basis or when a value changes
- A Relational Data Base Management System (RDBMS) for the storing and retrieving of historical or other non-real time data
- Scheduling and accounting applications to send, for example, (1) C structures containing interchange schedules once an hour or once a day and (2) binary files containing accounting data spreadsheet files.

- Dispatcher console operator message application and/or alarm processor application to send ASCII text messages to be displayed on a dispatcher's console display at another control center

These are just a few examples of the types of APIs an EMS/SCADA vendor may provide for its ICCP product. How they are implemented is considered a "local implementation issue" in the ICCP specification. As long as the protocol services are implemented according to the specification, interoperability is assured between different ICCP vendor's products.

Exhibit 6.1.2-1, Application Program Interface (API)



6.1.3 Client/Server Model

ICCP is based on client/server concepts. All data transfers originate with a request from a control center (the client) to another control center which owns and manages the data (the server). For example, if a Control Center X application needs data from the Control Center Y SCADA database, the Control Center X application acting as the client may request Control Center Y acting as the server to send the data under conditions specified by the client.

There are various services provided in ICCP to accomplish data transfers, depending on the type of request. For example, if the client makes a one-shot request, the data will be returned as a *response* the request. However, if the client makes a request for the periodic transfer of data or the transfer of data only when it changes, then the client will first

establish the reporting mechanism with the server (i.e., specify reporting conditions such as periodicity for periodic transfers or other trigger conditions such as report-by-exception only), and the server will then send the data as an unsolicited *report* whenever the reporting conditions are satisfied.

A control center may function as both a client and a server.

6.1.4 Multiple Associations and Sites

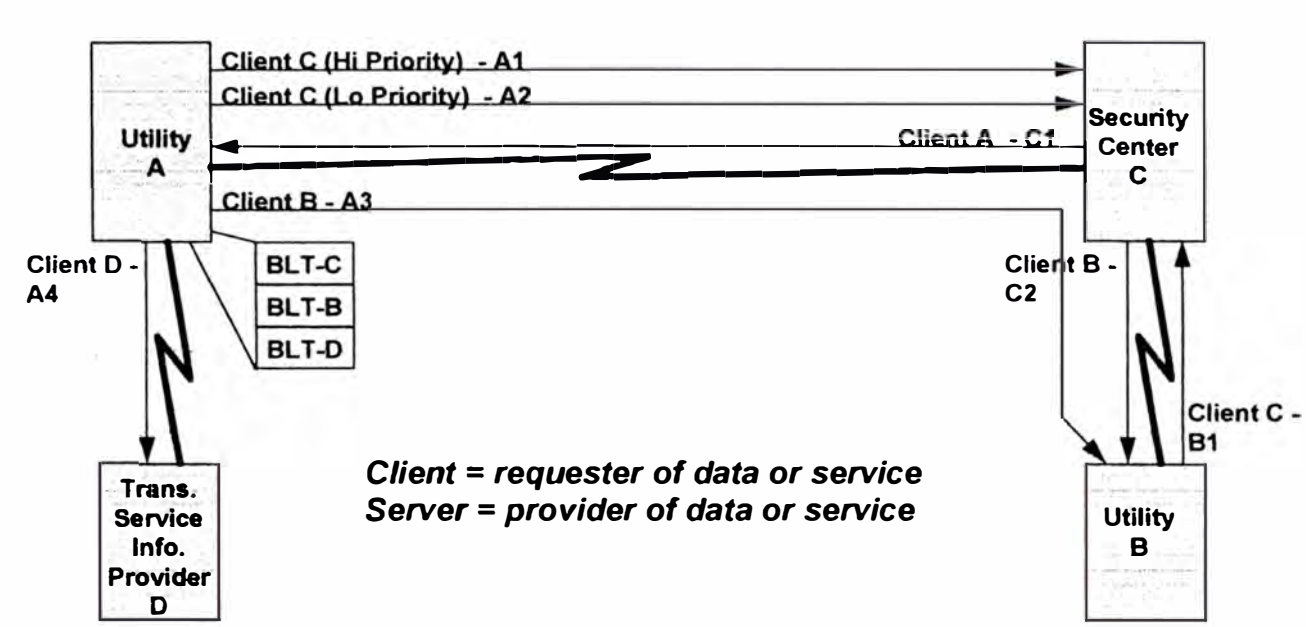
ICCP uses the ISO Association Control Service element (ACSE) to establish logical associations. Multiple associations may be established from a client to multiple, different control center servers. Although ICCP may be operated over a point-to-point link, it is envisioned that most installations will operate over a router-based Wide Area Network (WAN). As noted previously, ICCP is independent of the underlying transport network, so any combination of subnetworks may comprise the WAN, including the LANs within a site.

Multiple associations may also be established to the *same* control center for the purpose of providing associations with different Quality Of Service (QOS). An ICCP client then uses the association with the appropriate QOS for the operation to be performed. For example, to ensure real time data messages are not delayed by non-real data transfers, both a High and Low priority association may be established, with a separate message queue for each. ICCP will check the High priority message queue and service any messages queued before servicing the Low priority message queue. This permits a common data link to be shared for the transfer both high priority SCADA data and lower priority information message transfers.

Exhibit 6.1.4-1 illustrates an ICCP network serving four utilities. As shown, Utility A is a client to server C (Association C1) and a server for four associations: two to client C (Association A1 and A2), one to client B (Association A3), and one to client D (Association A4). The association to client B (A3) would presumably be accomplished via a router at utility C, but could follow any path available if a WAN is provided to interconnect all utilities. Each of the other utilities shown have similar associations established to meet their individual needs. Utility D functions only as a client. Utilities B and C function as both clients and servers. The point made by this diagram is that ICCP provides the capability for any type of interconnectivity needed via configuration of the ICCP software.

ICCP *permits* either a client or a server to initially establish an association. It further *permits* an established association to be used by either a client or server application at a site, independent of how the association was established. The PICs performance specifies how associations are used in any actual configuration of ICCP.

Exhibit 6.1.4-1, ICCP Client/Server Model with Multiple Associations



6.1.5 Access Control via Bilateral Tables

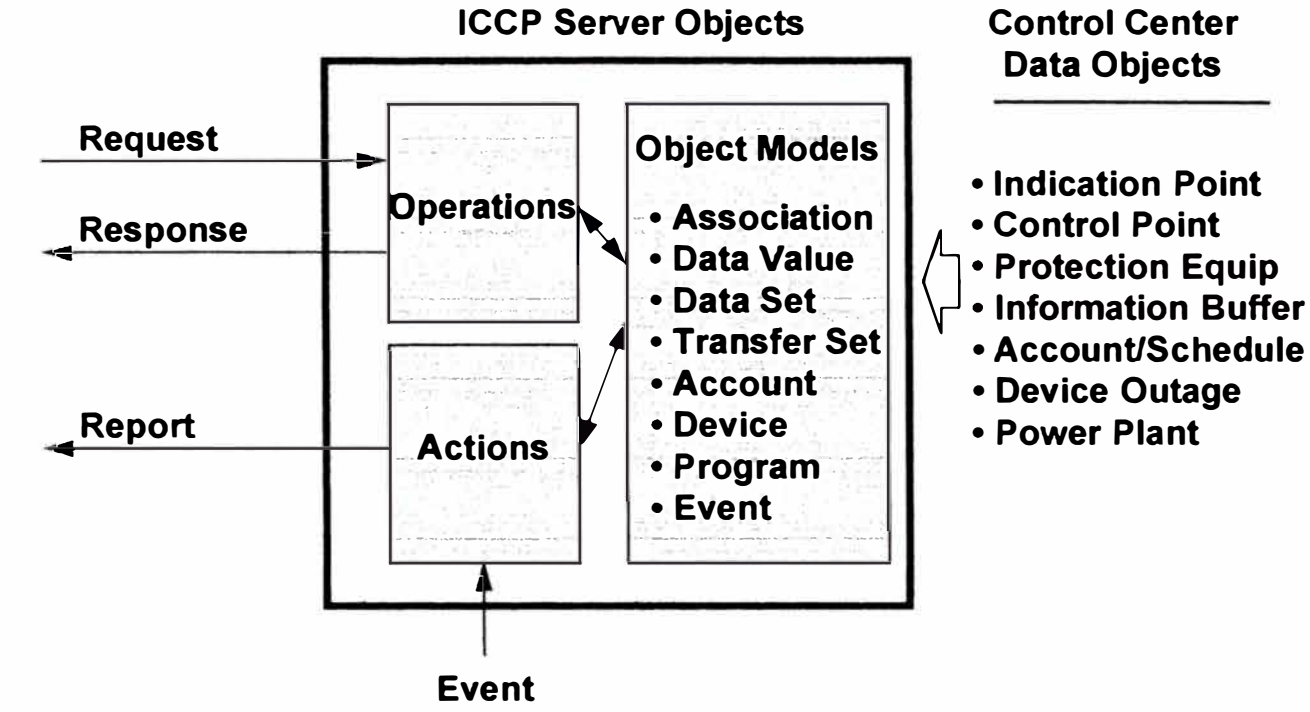
To provide access control, the server checks each client request to ensure that that particular client has access rights to the data or capability requested. Access control is provided through the use of Bilateral Tables (BLTs) defined for each client/server association. BLTs provide execute, read/write, read only, or no access for each item that can be requested by a client.

For example, as shown in Exhibit 6.1.4-1, Utility A maintains a separate BLT for each utility, permitting different access rights for the clients at each utility.

6.1.6 Use of Object Models

Object model concepts are used in two different ways in ICCP. Exhibit 6.1.6-1 illustrates these concepts.

Exhibit 6.1.6-1, ICCP Object Models



6.1.6.1 ICCP Server Objects

First, all ICCP services are provided via ICCP server objects which may be thought of as classical objects with data attributes and methods as defined in object-oriented design methodologies. There are two basic types of methods in ICCP called *operations* and *actions*. An *operation* is client-initiated via a *request* to a server, typically followed by a *response* from the server. An *action*, on the other hand, is a server-initiated function. An example of an *action* is the transfer of data via a *report* to a client in response to a timer expiring or some other external event at the server, such as a change in status of a breaker.

IEC 870-6-503 contains all the ICCP server object definitions. These objects are required to implement the ICCP protocol and are sometimes referred to as "internal" objects. Explanations of these objects is included in this guide in the ICCP Server Object Description section.

6.1.6.2 ICCP Data Objects

Second, all other data and control elements typically exchanged between control centers are defined as "data objects". These range from simple to complex data structures. In contrast to the "server objects", these objects are not required to implement the ICCP protocol, and so are sometimes referred to as "external" objects.

The standard Control Center Data Objects are defined in IEC 870-6-802. They are also described in this guide in the Conformance Block section. Supported data types include control messages, status, analogs, quality codes, schedules, text and simple files. Furthermore, additional data objects can be defined by ICCP users and transferred using

existing ICCP server objects with no change in the ICCP protocol software contained in IEC 870-6-503. The approach to defining new data objects is described in this guide in the section named Definition of New Data Objects.

6.1.6.3 Object Model Notation

The ICCP specification uses a formal method of describing objects. The first level is known as an Abstract Object Model. This model comprises a Name for the model, followed by a list of Attributes, headed by one Attribute known as a Key Attribute. In some cases an Attribute listed actually another object model inherited by the new object model. The meaning of each attribute is provided after the formal object model is presented.

Some object models, especially those used to describe control center data objects, contain Constraints, which provide alternative lists of Attributes within a single object model. These Constraints thus provide some flexibility in how the object can be used. All abstract models are described first in the specification.

Abstract object models then have to be mapped to concrete Structures with Components. Each Component is mapped to a data type. The services are mapped to MMS services. This must be specified to ensure that each implementer of ICCP uses the same data types and MMS services to implement the abstract models so that interoperabilty can be achieved with other vendor's ICCP products.

Section 7 describes in more detail the organization of the ICCP specification and the use of these models.

6.1.7 Conformance Blocks and Services

Conformance blocks are defined for ICCP for server objects in Section 9 of 870-6-503 as a way of grouping ICCP objects together to provide fundamental types of services. A vendor need not implement all defined conformance blocks (nine in all). However, any implementation claiming conformance to ICCP must fully support Block 1, as defined in Section 8 of this guide. Likewise, an ICCP end user need not procure all ICCP conformance blocks, only the ones actually needed to meet the user's data transfer requirements.

Conformance blocks are also defined in Section 9 of 870-6-802 for data objects as a way of specifying which server object services are needed to transfer each data object defined in 870-6-802.

6.2 ICCP Specification Organization

The ICCP specification organization is dictated by the rules and guidelines governing IEC/ISO standards documentation. The IEC numbers for the three parts of the specification were assigned by the IEC, basically by assigning the next sequential numbers available in the 870-6-500, -700, and -800 series of documents. The 500 series numbers are reserved for protocol standards and service specifications. The 700 series is reserved for Application profiles. The 800 series is reserved for Information Structure profiles, also known as Interchange Format and Representation profiles. This follows the classification scheme adopted for OSI functional profiles.

This section should explain how the IEC documents are organized and why (i.e., separation into parts 503, 702, and 802).

6.2.1 870-6-503

ICCP Part 503, known officially as IEC 870-6-503, TASE.2 Services and Protocol, defines the mechanism for exchanging time-critical data between control centers. The data exchange mechanism is defined in terms of ICCP server object models. It defines a standard way of using the ISO/IEC 9506 MMS services to implement the data exchanges.

A document that defines a standard way to use selected MMS services for exchanging electric utility data is known as an MMS Companion Standard for Electric Utility Data Exchange. And since MMS Companion Standards must follow a consistent format dictated by the MMS standards development groups, 870-6-503 is formatted as it is largely to conform to the guidelines established for MMS Companion Standards. This means that readability is sometimes sacrificed to follow these guidelines.

The ordering of the information presented in the document follows the "onion skin" analogy. That is, reading this document is like peeling off multiple layers of onion skins, with each new layer taking the reader to a deeper level of specification. This means that the same models are discussed at different levels several times throughout the specification. The order is as follows:

Layer 1

Section 5.1: Informal ICCP Model Description. The informal model of ICCP describes the various ICCP server objects in the context of the utility control center environment using plain English narrative.

Layer 2

Section 5.2: Formal ICCP Model Description. The formal model covers the same ground, only here more formality is introduced. Specifically, the entire control center with its software applications that are involved in data exchange are represented as a Virtual Control Center (VCC), comprising several object models. In this section, formal abstract models with attributes are introduced. Some models are represented as a hierarchy of object models, each of which is described. Each attribute for each object model is defined. Each operation and action is described again in more detail.

Layer 3

This layer covers three major sections:

Section 6: Mapping of ICCP Object Models onto MMS Object Models. In this section, the abstract object models are repeated, only this time each attribute is mapped directly to either a basic MMS attribute type or to a more complex ICCP data type defined in Section 8 , so that standard MMS protocols can be used for the actual transmission of data. For example, in Section 5.2 the Data Set Name attribute of the Data Set object model is defined as "the attribute that uniquely identifies the Data Set." In Section 6, the description for the Data Set Name attribute states that "this attribute shall be represented as the MMS Variable List Name attribute."

Section 7: Mapping of ICCP Operations and Action onto MMS Services. This section does for operations and actions what Section 6 does for attributes. It maps them onto MMS services, describing both the client and server roles in sufficient detail that a software vendor can implement each service in such a way that interoperability with other vendor's ICCP products is assured.

Section 8: Standardized Application-Specific Objects. This section specifies certain ICCP objects and complex data types used in Section 6 and maps them onto MMS standard objects and basic MMS data types. This section deals only with the objects required for ICCP internal use as distinguished from control center data objects, which are the subject of 870-6-802.

The last part of 870-6-503, Section 9, defines the Conformance Blocks, which are described elsewhere in this guide.

6.2.2 870-6-802

ICCP Part 802, known officially as IEC 870-6-802, TASE.2 Object Models, defines the control center data objects, which represent the control center data actually exchanged between control centers. This document is structured in a fashion somewhat similar to 870-6-503, but with only two layers:

Layer 1

Section 5: Object Models. This section defines the standard abstract object models for the data to be exchanged with ICCP. This uses the same notation that was used in 870-6-503 to describe the ICCP server object models, defining each attribute for each model. This is the section to browse or read to determine if there are appropriate standard objects available to meet a specific utility data exchange requirements. It is organized based on the classes of data typically exchanged between control centers. The order is Supervisory Control and Data Acquisition, Transfer Accounts, Device Outage, Information Buffer, and Power Plant objects.

Layer 2

This layer comprises two sections.

Section 6: MMS Types for Object Exchange. This section defines the data types to be used for exchanging the standard objects. This includes basic types, such as Data_Discrete, which is defined as an integer {width 32}. But it also includes complex data types based on the abstract models defined in Section 5. Each abstract model must be mapped to one or more concrete object types, which are defined in terms of structures with components. For example, an Indication Point object which contains an analog point value with quality and time tag (but not change - of - value counter) is mapped to the Data_DiscreteQTimeTag type, which is a complex type with a structure containing the components Value, TimeStamp, and Flags. Each component is also mapped to a data type, in this case Data_Discrete, Data_TimeStamp, and Data_Flags, respectively. In all cases, each type maps down to a supported MMS type for data exchange.

This section contains both the basic types and complex structure types, ordered the same as Section 5. The exception is the Matrix Data Type, which is used by several different objects, as described in Section 7.

Section 7: Mapping of Object Models to MMS Types. This sections defines the mapping of each object attribute from Section 5 to one or more of the ICCP types defined in Section 6.

Section 8, Use of Supervisory Control Objects, provides examples in the use of the Supervisory Control objects in order to introduce some conventions in assigning meaning to certain attributes which are generic in nature.

Section 9, Conformance, identifies the 870-6-503 Conformance Block required to provide the necessary services for exchanging each data object described in 870-6-802.

6.2.3 870-6-702

This specification defines the Application Profile (Layers 5-7) for use with ICCP. It is needed for vendors implementing protocol stacks that support the ICCP application layer. Most users of ICCP will not be concerned with this specification. Therefore this guide does not deal specifically with this 870-6-702 in the present version.

7. ICCP Server Objects

7.1 Association

Association objects are used to establish an association, or logical connection, between two ICCP instances. Such an association is typically long-running, staying in place as long as both ICCP instances are running and the underlying communications links are maintained.

Three operations are defined for Association objects:

1. Associate - used by a client to establish an association with a server.
2. Conclude - used by either a client or server to provide an orderly termination to an association (e.g., for some planned maintenance).
3. Abort - used by either client or server to terminate an association when there are failures in the underlying communications mechanisms.

There are no actions defined for Association objects.

7.2 Data Value

Data Value objects represent values of control center data elements, including SCADA points, such as analog measurements, digital status, and control points, or data structures. Any data element or object that is uniquely identified by a single MMS Named Variable (with persistence) can be represented via the Data Value object. Currently this includes Indication Point, Control Point, and Protection Event objects only.

There are four operations defined for Data Value objects:

1. Get Data Value - can be used to request the value of a single SCADA point.
2. Set Data Value - intended to permit a data value to be written or set at a local control center by a remote control center. In practice, few vendors or utilities are actually permitting the Set capability in an ICCP client because of the desire to keep the ability to change data with the owner of the data, which will be the ICCP server. Note that the Device object defined below is intended to permit remote supervisory control operations.
3. Get Data Value Names - allows client to obtain a list of the names of all the Data Value objects at a remote control center for which that client has permission (via the BLT). This operation can be used to determine which points can be viewed by the client as an aide in defining data sets or one shot requests for data, as described later.

4. Get Data Value Type - allows client to obtain the Type attribute for a Data Value object.

There are no actions defined for Data Value objects.

7.3 Data Set

Data Set objects are ordered lists of Data Value objects maintained by an ICCP server. This object enables a client to remotely define Data Sets via ICCP. The Data Set object can be used by a client, for example, to remotely define a list of SCADA points to be reported as a group. The establishment of the reporting criteria and the actual transfer of data vales is accomplished using the Transfer Set object, as described below.

There are six operations defined for Data Set objects:

1. Create Data Set - allows a client to create a Data Set object at a remote server. In addition to specifying the list of Data Value objects to be included in the Data Set, the client can also specify which of the following parameters will be included in a Transfer Report containing the actual data values:
   - Transfer Set name - identifies the Transfer Set object that generated the report
   - Data Set Conditions Detected - identifies the event that triggered the sending of the report. The list of possible trigger events is:
     - Interval time-out
     - Object change
     - Operator request
     - Integrity time-out
     - Other external event
   - Event Code Detected - identifies the event code if the trigger was Other External Event (see B. above)
   - Transfer Set Time Stamp - specifies the time the Transfer Report was generated at the server.
2. Delete Data Set - allows a client to delete a previously defined Data Set object.
3. Get Data Set Element Values - allows a client to obtain the value of each of the Data Value objects included in the referenced Data Set object. This operation permits a one-shot request of all values of for the list of Data Value objects included in the referenced Data Set.
4. Set Data Set Element Values - allows a client to set the value of each of each of the Data Value objects included in a Data Set. In practice, this is not usually permitted.
5. Get Data Set Names - allows a client to get the names of all the Data Set objects currently defined at a server.
6. Get Data Set Element Names - allows a client to obtain the list of names of all the Data Value objects currently included in a specific Data Set object at a server.

There are no actions defined for the Data Set object.

Typical Use

Transfer of SCADA data to and from a real-time SCADA database on an EMS/SCADA system.

7.4 Transfer Set

Transfer Set objects residing at an ICCP server are used by an ICCP client to establish the actual transfer of data values. While Data Value objects can be individually requested via a one-shot request, receiving the requested value in response, more complex data transfers require the use of a Transfer Set. As mentioned earlier, the transfer of groups of data defined in Data Set objects requires the use of a Transfer Set. The exchange of most all other data in ICCP requires a Transfer Set to be established first.

The Transfer Set object permits information to be exchanged on a periodic basis, on change of state or value, in response to a particular server event, or on operator request. The Transfer Set object provides the operations needed by a client to set up instances of Transfer Sets for each desired data exchange.

7.4.1 Four Transfer Set Object Models

Because of the unique requirements for transferring different types of data between control centers, ICCP provides four types of Transfer Set objects:

A. **Data Set Transfer Set** - used for establishing the transfer of Data Sets defined and created using the Data Set object.

B. **Time Series Transfer Set** - used for transferring the data values of a single Data Value object at different incremental times as specified by a delta time interval

C. **Transfer Account Transfer Set** - used for transferring many different types of data objects. In ICCP a Transfer Account is a generic term applied to a whole class of data objects used to represent information on schedules, accounts, device outages, curves, and other entities used by control centers which have only one thing in common - the use of complex data structures to represent data. Initially, the type of data envisioned was accounting or scheduling data, which represent an amount of energy transferred from one utility to another on a periodic basis, hence the name Account or Transfer Account.

As currently defined in the IEC standard, this transfer set is used to transfer any of the data objects defined as "Block 8 objects". This includes the following:

- **Transfer Account** - this is a container type of object which can be used for the exchange of any periodic or profile data for control center energy scheduling, accounting, or monitoring applications.
- **Device Outage** - this a data object designed to exchange information about device outages, either for scheduling outages or reporting actual outages. Devices can include almost any type of physical component in a power system that is routinely monitored for status today.
- **Availability Report** - this is the first of five data objects included in a class of data objects labeled Power Plant objects in IEC 870-6-802. It is intended for power plant control system or GCSs to report on predicted availability of generating units and/or to schedule outages. It is similar to the Device Outage object, but differs by having more attributes unique to generation units and

power plants and by not including actual status reports (this is handled by the next data object, Real Time Status).

- **Real Time Status** - this object is used by a power plant to report the actual operating status of generating units at the time of the report.
- **Forecast Schedule** - this object is intended for use by an EMS or GCS to deliver a forecasted usage of generating units at a power plant. Similar to the Transfer Account data object, this is another container object with user-defined matrix to specify the number and meaning of each column in the matrix. Rows are separated by a user-selected delta time increment.
- **Curve** - this object is intended for use by a power plant to report various types of curve data, such as heat rate, IO, incremental heat rate, MVAR capacity, opacity, SOX, NOX, and CO2 emission curves. The curve is represented as a sequence of curve segments, with each segment defined in terms of a polynomial.
- **Power System Dynamics** - this is a collection of data elements (rather than an actual object model) which need to be exchanged between a power plant and a GCS or EMS. These are scalar quantities and can be represented individually as Data Value objects.

These objects are described in detail in this guide under the Block 8 heading in the Conformance Blocks and Associated Objects section.

D. **Information Message Transfer Set** - used for transferring the Information Buffer data object defined in IEC 870-6-802. The Information Buffer is intended for sending unstructured ASCII text strings or binary data.

There are four operations defined for Transfer Set objects:

1. Start Transfer - permits a client to request a server to begin to transfer data under the conditions specified by the client in this operation. The capabilities provided differ in important ways for each type of transfer set:

   For Data Set Transfer Sets, the client provides the name of the Data Set object to use for grouping Data Values for transfer. A separate Transfer Set is used for each Data Set of interest, permitting different transfer conditions for each.

   For Time Series Transfer Sets, the client names the Data Value object of interest.

   For Transfer Account Transfer Sets, the client can only enable the transfer all Transfer Account objects defined in the Bilateral Table. That is all Block 8 objects get enabled at one time and under one set of conditions.

   For Information Message Transfer Sets, similar to Transfer Account Transfer Sets, the client can only enable all Information Messages under the same set of conditions.

2. Stop Transfer - used by a client to stop a data transfer operation (i.e., disable the transfer). A new Start Transfer operation is required to once again enable the transfer.
3. Get Next Data Set Transfer Set Value - used by the client as the first step in starting a Data Set data transfer. The server maintains a "pool" of available Data Set Transfer Sets for a client to use. The client must obtain the name of the next available Transfer Set, and then perform a Start Transfer operation using the name

of the that Transfer Set to actually start a transfer. Thus the Start Transfer operation may be thought of as the client "writing" a value of the Transfer Set variable to the server. A Stop Transfer operation actually releases the Transfer Set back into the pool of available Transfer Set names at the server.

4. Get Next Time Series Transfer Set Value - similar to the Get Next Data Set Transfer Set Value operation, only for this operation is used for starting the reporting of a series of values for the same Data Value object.

Note: There are no "Get Next Transfer Set Value" operations for Transfer Accounts (i.e., Block 8 objects) or Information Message objects, since the client can only start or stop transfers of all Block 8 objects or Information Message objects, respectively.

There are two actions for Transfer Sets:

1. Condition Monitoring - performed by the server for each Transfer as soon as that Set that is Enabled via a Start Transfer operation. Any and all conditions requested in the Start Transfer operation are monitored by the server until a Stop Transfer operation is performed by the client. Note that for Information Message Transfer Set objects, the conditions used are locally defined only and cannot be specified via the Start Transfer operation.
2. Transfer Report - a Transfer Report is generated whenever a condition specified by the client has occurred for an enabled Transfer Set. The Transfer Report is the action used to actually transfer data from the server to the client. The server formats and sends a report with the appropriate data for the type of Transfer Set.

Associated with the Transfer Report are four additional objects (with no operations or actions) to convey information about the Transfer Report generation process:

- Transfer Set Name - the name of the Transfer Set object which caused the Transfer Report
- Transfer Set Conditions - a bitstring indicating which Transfer Condition(s) triggered the transfer
- Transfer Set Time Stamp - the time of generation of the Transfer report
- Transfer Set Event Code - indicates the external event which caused the Transfer Report to be sent, if the Other External Event condition was being monitored.

7.5 Account

Transfer Account objects (i.e., Block 8 data objects) are usually transferred via the Transfer Account Transfer Set object. However, there is one special and very useful operation, the Query Operation, provided that permits a client to request a particular account object based on the account reference number and optionally start time and duration.

7.6 Device

Device objects represent actual physical devices in the field for the purpose of providing services for a client to control them remotely. Both interlocked (i.e., select-before-operate) and non-interlocked devices are represented.

There are four operations for Device objects:

1. Select - used by a client to request selection of an interlocked device only. If successful, the Device state is changed from IDLE to ARMED by the server.
2. Operate - used by a client to send a command to a Device object to execute a function. For interlocked devices, the Device state must be ARMED.
3. Set Tag - used by a client to set the Tag attribute of a Device object.
4. Get Tag Value - used by a client to retrieve the current state of the Tag attribute of a Device object.

There are four actions defined for Device objects:

1. Time-out - results from a time-out after a device has been set to ARMED via a Select operation but not yet operated. This action causes the device state to retum to IDLE.
2. Local Reset - causes a device state to be reset from ARMED to IDLE by a local action at the server. This may also cause the Tag attribute value to change.
3. Success - used to tell the client that a successful Operate operation has been completed.
4. Failure - used to tell the client that an Operate operation has failed.

7.7 Program

A Program object provides a client with remote operation of a program at a server site. The actual program being controlled can be any application program at the server site.

There are six operations defined for the Program object:

1. Start - starts an IDLE program
2. Stop - stops a RUNNING program
3. Resume - starts a STOPPED program
4. Reset - IDLEs a STOPPED program
5. Kill - makes a program UNRUNNABLE
6. Get Program Attributes - returns information on a RUNNING program

There are no actions defined for a Program object.

7.8 Event

An Event object represents a system event at a server site, such as a device changing state or the occurrence of a certain data error. Event objects provide a way for a client to be notified of system events at a server. There are actually two objects associated with events: Event Enrollment object and Event Condition object. There is only a minimal description of these objects in the ICCP specification, which map directly to MMS services with the same name.

7.8.1 Event Enrollment

Event Enrollment permits a client to express interest in being notified of particular event when it occurs at a server site. There are three operations associated with an Event Enrollment object:

1. Create Event Enrollment - creates an Event Enrollment object which specifies which event is of interest and which conditions should be reported. This is accomplished by specifying the name of an Event Condition object as a part of creating and Event Enrollment object.
2. Delete Event Enrollment - deletes an Event Enrollment object
3. Get Event Enrollment Attributes - gets existing Event Enrollment attributes

There are no actions defined.

7.8.2 Event Condition

Event Condition objects are predefined at a server for all system events that are to be available to clients for enrollment.

There is one action for an Event Enrollment object:

1. Event Notification - notifies all clients that have created Event Enrollment objects that specify the particular Event Condition object whenever the event occurs.

   It should be noted that the device state change events that are monitored by Event Condition objects may also be reported to a client via SCADA data point changes, so that the use of Event objects may not be needed. However, the Event objects provide a mechanism for certain events that may not otherwise be reported to a client.

There are no operations defined for the Event Condition object.

8. Conformance Blocks and Associated Objects

This section explains the intended use of each conformance block and object. The services and protocols associated with each conformance block and its associated objects are discussed in 870-6-503. The user objects themselves are described in 870-6-802. There are location references at the beginning of each block's description that point to discussions or descriptions in 870-6-503 and 870-6-802.

ICCP was designed from the beginning to be modular. Each conformance block represents a specific function or set of functions that a utility might wish to implement. A utility implementing ICCP for real-time data exchange is only required to purchase block 1. Additional blocks may be added independently. For example, a utility wishing to exchange power system data by exception and accounting data needs only to purchase blocks 1, 2 and 8.

Each block may have specific user objects associated with that block. This mapping of which objects are associated with which conformance blocks is found in 870-6-802, section 9. When a user decides to purchase a specific block, they should also specify which objects within that block must be supported by the vendor.

8.1 Block 1 (Periodic Power System Data)

8.1.1 Indication Point Object

Block 1 is slightly different from all the other blocks. Block 1 is the minimum that a developer can implement. It is also the minimum that a user can purchase. There are certain system services that must be supported. In particular, this block includes the following objects:

- Association
- Data Value
- Data Set
- Data Set Transfer Set

Once these objects and associated services are provided in Block 1, they will be utilized whether additional Conformance Blocks are added or not.

In addition to these special system services, Block 1 provides for the periodic transfer of power system data. Power system data is the database representation of field device status (i.e. breakers, MODs, HLO lamps, substation doors, etc.); analog values (i.e. megawatt, megavar, voltage, tap settings, phase shifter angles, etc.), and accumulator values (KWH, KQH). Each data item may also have associated with it a quality code that provides information about the reliability of the data item itself.

The data object transferred in Block 1 is the Indication Point Object. The Indication Point Object is used to transfer information about status points (referred to as STATE or DISCRETE) and analog points (referred to as REAL). A formal description of the object can be found in 870-6-802, Section 5.1.1.

An optional data object transferred in Block 1 is the Protection Event object, described here and in 870-6-802, Section 5.1.3.

8.1.1.1 Status Points

A description of the Status Points foundation types can be found in 870-6-802 section 6.1.1 as Data_State and Data_Discrete.

The user should decide whether to transfer status point information as STATE or DISCRETE. Using STATE will only allow up to a maximum of four states to be described for each device. Most power system devices are two or three state devices (open, closed, traveling). The choice of STATE allows for the most efficient transfer of status information. Two bits are used to encode the device state. The entire device state and quality are transferred in one octet.

There are, however, multi-state devices and pseudo status points in the SCADA/EMS database that have more than four states. To transfer these status points, the use of DISCRETE is required. Although less efficient, the use of DISCRETE allows the user to transfer a 32 bit integer where each value can represent a different state. Transferring status information using DISCRETE requires a 32 bit integer for the device states and an additional octet for the associated quality codes.

8.1.1.2 Analog Points

A description of the Analog Points foundation type can be found in 870-6-802 section 6.1.1 as Data_Real.

Analog point values are transferred as 32 bit IEEE format floating point values. Each analog value may have associated with it quality codes that provide information about the reliability of the value itself. Transferring analog information requires a 32 bit integer for the analog value and an additional octet for the associated quality codes.

8.1.1.3 Quality Codes

A qualitative description of the quality codes that ICCP provides to the user is found in 870-6-802 section 5.1.1 as Validity.

A description of the Quality Codes foundation type can be found in 870-6-802 section 6.1.1 as Data_Flags.

Quality codes are derived from the current SCADA/EMS computer system's ability to determine the reliability of a status, analog or accumulator point that has been stored in the SCADA/EMS database.

A telemetered value within reasonability limits that was updated to the SCADA/EMS database successfully on the last attempted scan has the highest quality. Its quality is derived from the fact that the value is both accurate and current. Quality is also considered high on data points that may not be current, but that have been manually entered by a dispatcher, operator or program. Because a "conscious" decision has been made to assign a point its particular value, it is considered "good" or of high quality.

ICCP transfers the quality codes associated with each data point, however, the assignment of local quality code bits in the receiver's SCADA/EMS database is a local implementation issue. Because each SCADA/EMS has its own symbols for displaying data quality, each user must determine their own hierarchy of processing and mapping to their own quality symbols.

8.1.1.4 Time Stamp

A description of the Time Stamp foundation type can be found in 870-6-802 section 6.1.1 as Data_TimeStamp.

The Timestamp attribute is used to assess the currency of the data value being transferred. Data can be "old" for a number of different reasons: delays in out going queues at the source SCADA/EMS, delays in transmission across the network, delays due to congestion and re-transmission within the network and delays in in-coming queues at the receiving SCADA/EMS. For all of these reasons, the data might need to be time stamped at the source SCADA/EMS at the earliest time following collection of that data from the field device. Values that are calculated from other values in the SCADA/EMS should be time stamped at the time the values is stored in the SCADA/EMS database.

8.1.1.5 Change of Value (COV) Counter

A description of the Change of Value foundation type can be found in 870-6-802 section 6.1.1 as COV_Counter.

A periodic information report transferring status and analog values will transfer only the current value of the data point. A receiving control center might want to know whether the point had changed and then changed back between information reports. For example, an auto-reclose operation might easily occur between information reports and not be recorded at the receiving site. A COV counter is incremented each time the owner sets a new value for the Indication Point.

8.1.1.6 Building Complex Data Types

The complex types are created by combining foundation data types. The choice of which complex data type to use is made by the implementer and is a balance between efficiency and the extent to which additional information about the value being transferred is required by the receiving site. For instance, if a client wants to receive status with quality codes and a time tag, the client would specify the use of the Data_StateQTimeTag complex type, described in 870-6-503, Section 6.1.1.

8.1.2 Protection Equipment Event Object

The protection equipment event object definition can be found in 870-6-802 Section 5.1.3.

When events occur at the substation, local relay actions may be taken to protect equipment. These events may be phase-to-phase, phase-to-ground, over current, over or under voltage, or other protective relaying schemes. In addition to the name of the event, protection equipment event object reports:

1. The quality of the information. An underline value indicates a yes answer to the question.

ElaspsedTimeValidity	Were the associated times correctly acquired?	VALID INVALID
Blocked	Is the information blocked against further updates until it has been transmitted or safe saved?	NOTBLOCKED BLOCKED
Substituted	Was the information manually entered or entered by an automated source?	NONSUBSTITUTED SUBSTITUTED
Topical	Was the last update of the information successfully completed?	NONTOPICAL TOPICAL
EventValidity	Were no abnormal conditions of the information source detected during the last update?	VALID INVALID

2. The type of event (SINGLE or PACKED)and information related to the event.

A SINGLE event has its EventState, EventDuration and EventTime reported.

A PACKED event reports either the cause and involved equipment (START) , or the actions taken (TRIP).

START events includes the following information: An underlined value indicates a yes answer to the question.

StartGeneral	Was this a general start?	START NOSTART
StartPhase1	Was phase 1 involved in the event?	START NOSTART
StartPhase2	Was phase 2 involved in the event?	START NOSTART
StartPhase3	Was phase 3 involved in the event?	START NOSTART
StartEarth	Was ground current involved in the event?	START NOSTART
StartReverse	Was reverse current involved in the event?	START NOSTART
DurationTime	Event duration in milliseconds	
StartTime	Protection equipment operation start time	

TRIP events includes the following information: An underline value indicates a yes answer to the question.

TripGeneral	Was this a general trip operation?	TRIP NOTRIP
TripPhase1	Was a control operation issued to trip phase 1?	TRIP NOTRIP
TripPhase2	Was a control operation issued to trip phase 2?	TRIP NOTRIP
TripPhase3	Was a control operation issued to trip phase 3?	TRIP NOTRIP
OperatingTime	Time in milliseconds from the start of the operation until the first command was issued to an output control circuit	
TripTime	Time of the start of the operation	

8.2 Block 2 (Extended Data Set Condition Monitoring)

A description of Data Set condition monitoring can be found in 870-6-503 section 5.2.9.1.1 and 5.2.9.1.2.

Block 2 is used to provide the capability to transfer power system data in more ways than periodic reports. A periodic report (block 1) is simple and easy to set up, but it has the

drawback that because it reports every value to the client every time the report is generated, it is not very bandwidth efficient. Block 2 is also referred to as report-by-exception, or RBE.

Report by exception allows the client to specify that power system objects will be reported only when a change is detected or when an integrity check is performed. ICCP does this by having the server monitor a number of conditions and when one or more of those conditions occurs, the data that has changed is sent to the client. The client sets the conditions to be monitored in the transfer set at the server.

The conditions that can be monitored are:

- The normal reporting period is due (IntervalTimeOut). This is the same condition that is monitored in block 1.
- The value, state or quality code of a value has changed (ObjectChange).
- The operator at the server site has requested that the value be sent to the client (OperatorRequest).
- A periodic report of all values is sent to the client to ensure that the two databases are still synchronized and that no changes have been lost since the last integrity check (IntegrityTimeOut).
- Other, unspecified conditions can be monitored (OtherExternalEvents).

Once the server has determined that a report by exception information report is required, it must then determined whether the client has requested that the report be generated as normal MMS named variables, or as blocked data (see next section).

8.3 Block 3 (Block Data Transfer)

A description of the rules for encoding block data can be found in 870-6-503 section 7.1.4.4.2.

Block data with report by exception is a very efficient transfer mechanism under certain conditions. It provides the possibility for an ICCP server to send power system data to a client with fewer bytes than required for sending with full ASN.1 encoding, as required in Blocks 1 and 2. Blocking may be useful where bandwidth is at a premium due either to low data rates or short periodicities (i.e., high frequency) of the data reports. However, the consequence of blocking is that the information needed to properly decode the data in a transfer report is not all contained in the report itself.

There are two mechanisms used by Block 3 to achieve efficiency. The first is the dropping of the tag and length fields for each data value reported. The second is the creation of an index-based tagging scheme to replace variable names with a one or two byte number. Block 3 provides three rules for encoding. The choice of the proper rule depends on whether the data is all sent periodically or as report-by-exception, and on how many values are sent. These mechanisms and rules are described below.

8.3.1 Use of an Octet String MMS Variable

Instead of sending a tag and length along with each data value, as required by the ASN.1 Basic Encoding Rules used in Layer 6, the ICCP server instead utilizes a single long octet-string MMS variable to transfer all the data values. This requires that all primitive data

types (and any aggregates based on them) be encoded using the full length permitted by that type in order to avoid putting in the length fields. Therefore, variable length fields must be padded out to their maximum length. In order for the client to receive and utilize the data, the client must have prior independent knowledge of the location and type of each value in the octet-string. Client knowledge of the type field is required to permit the dropping of the tag fields.

Then, if the data is sent as provided in Block 1 (i.e., not Report By Exception), the data is encoded into the octet-string according to rule 0, described below:

Rule 0: [rule#, total length, $value_i$ ...]

This can result in fewer bytes being transferred because the tag and length fields for each variable are not transferred. This works best for variables with short data types that require only one byte for the value. However, for longer types, there are cases where this will not result in any savings. For example, transferring an Integer32 variable that happens to equal 0 in value will result in a MMS PDU encoding using BER of 3 bytes (tag, length, and value each one byte) whereas blocking would have to expand the integer out to four bytes, actually wasting one byte. Therefore, the type of data to be transferred should be considered before automatically assuming fewer bytes will result just from dropping the tag and length fields.

8.3.2 Index-Based Tagging

Block data and report-by-exception can be combined to yield a more efficient transfer of data. If block data and report by exception are specified, the server has two rules available for constructing the message that will be sent to the client. In each case the database point is identified by an index into the named variable list, followed by the current value of the point. This has the effect of replacing variable names, typically many bytes in length, with a one or two byte index number.

Utilizing rule 1, the header consists of the rule number [1], followed by the total message length in octets. The body of the message consists of a one octet index (the relative position of the identifier in the named variable list), followed by the value of the identifier. This pairing of index and value is continued to the end of the message.

Rule 1: [rule#, total length, $index_i$(1-octet), $value_i$ ...]

Rule two is similar to rule 1 except that it utilizes a two octet index for messages that have more that 255 index-value pairs.

Rule 2: [rule#, total length, $index_i$(2-octets), $value_i$ ...]

Blocking when combined with report-by-exception thus provides guaranteed efficiency for transmission by sacrificing inclusion of the information needed to decode the data contained in a message, creating a data maintenance task. If message formats seldom change, this may be a good tradeoff. However, if bandwidth is not a primary concern or report-by-exception is not used, and more flexibility is desired by a client to change the content of messages using ICCP protocol mechanisms without operator involvement at the server, then blocking should probably not be used.

8.4 Block 4 (Information Messages)

Block 4 provides a general message transfer mechanism that also includes the ability (by agreement of the two parties) to transfer simple text or binary files. Block 4 adds the Information Message Transfer Set server object with the associated Information Buffer data object.

One use of this service might be for a utility to notify other utilities within its inter-connection that an event more complex than that represented by simple power system data values, has occurred. For example:

- notification of a decision to implement an inter-connection wide time error correction action.
- notification of the boundaries of identified electrical islands during a disturbance.
- request for emergency use of pool reserves.

These messages might be simple formatted ASCII text messages with data from the SCADA/EMS incorporated into the body of the message. These could be used as alarm text or text reports for display on a receiving operator console or for logging.

The InformationBuffer object provides a unique identifier (InfoReference) and a local identifier (LocalReference). The MessageId identifies the particular instance of a message. The Size attribute is the length in octets of the actual data being transferred.

This object also provides a mechanism for simple, small, binary file transfer. These transfers are limited in size by MMS to 8k octets. The InfoReference and LocalReference attributes could be used to identify a process that would receive the binary information buffer and store it in a local file. The information stored could, by agreement, be an Excel or Word Perfect file that would later be accessed by the client or server. Individual instances of this file being transferred (the June, July or August instances) would be distinguished by the MessageID attribute.

An informal description of the Information Message can be found in 870-6-503 Section 5.1.6 and a formal description can be found in Section 5.2.8. The Information Buffer object is described in 870-6-802 Section 5.4, the type descriptions in Section 6.4 and the mappings to MMS in Section 7.4.

8.5 Block 5 (Device Control)

Block 5 adds the Device server object and associated Control Point data object.

Block 5 provides a mechanism for transferring a 'request to operate a device' from one ICCP implementation to another. ICCP does not directly control the device, rather it communicates a client's request to operate a device to the server.

ICCP retains some of the important characteristics of RTU device control. Specifically, the select and validate before operation for interlocked devices and the armed-for-execution mode for a selected device.

The ControlPoint object is used to transfer the request. It distinguishes between a device operation (COMMAND) and the transfer of a numeric value (SETPOINT), either floating point (SetpointRealValue) or integer (SetpointDiscreteValue).

A control request can be for non-interlocked (NONINTERLOCKED) or interlocked devices (INTERLOCKED). Both command and setpoint operations can be inter-locked or non-interlocked. Non-interlocked controls are control operations that do not require select-before-operate confirmation. These might include transformer tap changes, raise/lower operations and digital value setpoint type operations. Interlocked controls on the other hand, require select-before-operate confirmation for critical operations such as breaker trip/close, recloser on/off and HLO lamp on/off.

For interlocked control operations, the client sends a request to operate a specified device to the server. After checking for the existence of the device object, checking access control in the Bilateral Table, the server then performs a local verification that the device is available for operation. The verification checks that the server actually performs are a local implementation issue. The device is SELECTED and a previously agreed to CheckBackName is provided to the client to confirm that the correct device has been selected. A Time-out period is reported to the client giving the length of time that the device will remain selected by the server.

ICCP does provide a mechanism for the server to report to the client whether the desired control point is tagged. The server reports:

0 if the device is not tagged
1 if the device is tagged open and close inhibit
2 if the device is tagged close only inhibit

The client, having received a verification of device operability and a validation of device selected, then sends a final request to have the device operated by the server or to cancel the requested operation.

The server completes the requested control operation and notifies the client of success or failure. Provision are made so that at any time during this process the client or the server can terminate the operation for a valid reason.

An informal description of device control can be found in 870-6-503 section 5.1.10 and a formal description can be found in section 5.2.11. The device object model mapping can be found in section 6.15. Device operations and action mapping to MMS including a sequence of device control diagram can be found in section 7.1.6.1. The control point object is described in 870-6-802 section 5.1.2, the type descriptions in section 6.1.2 and the mappings to MMS in section 7.1.2.

8.6 Block 6 (Program Control)

Block 6 adds the Program server object and associated services.

Block 6 provides a mechanism for an ICCP client to perform program control at a server ICCP implementation site. Program control is only available by prior agreement between any two ICCP sites.

Implementation of program control is made very straight forward by the fact that MMS provides program invocation and control as part of its basic services. ICCP can then utilize these services with proper interfaces to the SCADA/EMS system to perform remote program control. There are no user objects associated with program control.

An informal description of program control can be found in 870-6-503 section 5.1.11 and a formal description can be found in section 5.2.12. The program control object model mapping can be found in section 6.16. Program operations and action mapping to MMS can be found in section 7.1.7.

8.7 Block 7 (Event Reporting)

Block 7 adds the Event Enrollment and Event Condition objects. Block 7 is not required for any of the other blocks, but instead provides extended reporting of system events occurring at a remote site (i.e., ICCP server).

Block 7 provides two functions to the ICCP client.

1. It allows the ICCP client to enroll in two types of events:
    a) Specific error condition reporting from the server
        i) Time-out conditions
        ii) Failure conditions
        iii) Local reset actions
        iv) Success conditions
    b) Device state changes at the server
2. It allows the ICCP client to receive information about the events that the client has enrolled in and has enabled.

An example of how a utility might utilize event enrollment is a situation where a utility is required during non-working hours to monitor specific security events at a substation or power plant. During working hours, monitoring and control is performed locally at the site. The enrollment and receipt of the security information could be enabled only for the non-working hours.

An informal description of event reporting and event conditions can be found in 870-6-503 section 5.1.12 and 5.1.13, and a formal description can be found in section 5.2.13 and 5.2.14. The event enrollment and event conditions object model mapping can be found in section 6.17, and 6.18. Event enrollment operations mapping and event conditions action mapping to MMS can be found in section 7.1.8, and 7.1.9

8.8 Block 8 (Additional User Objects)

Block 8 adds the Transfer Account Transfer Set server object for transferring Block 8 data objects. An informal description of Transfer Account Transfer Set objects and services can be found in 870-6-503 section 5.1.7 and a formal description can be found in section 5.2.9.3. The Transfer Account Transfer Set object model mapping is found in section 6.9.3. Transfer Account Transfer Set operations and action mapping to MMS can be found in section 7.1.4.

Block 8 also adds the Account server object for requesting Block 8 data objects. Using the Query operation supported by this server object, an ICCP client can specify the following:

- The Transfer Account Reference number for the account for which information is to be returned
- Start time for the data

- Duration of the data in seconds since the start time
- A RequestID, which is echoed back by the server to permit the client to match incoming data with a specific request
- TAConditions to identify the type of data requested.

An informal description of account objects and services can be found in 870-6-503 section 5.1.5 and a formal description can be found in section 5.2.7. The account object model mapping is found in section 6.7. Account operations and action mapping to MMS can be found in section 7.1.5. However, the details of the attributes included in the Query operation are contained in 870-6-802 section 5.2.4.

Block 8 provides a utility with a number of additional *data objects* related to transferring scheduling and accounting information, device outage information, and power plant information. A vendor might offer support for one or more of the data objects in Block 8. Information on these objects can be found in the ICCP specification at the following locations in 870-6-802:

	Object Model	MMS Types	Object mapping to MMS
Scheduling & Accounting			
Transfer accounts	5.2.1	6.2.1	7.2.1
Transmission segment	5.2.2	6.2.2	7.2.2
Profile value	5.2.3	6.2.3	7.2.3
Account request	5.2.4	6.2.4	7.2.4
Device outage	5.3	6.3	7.3
Power plant			
Availability	5.5.1	6.5.1	7.5.1
Real-time status	5.5.2	6.5.2	7.5.2
Forecast schedule	5.5.3	6.5.3	7.5.3
Curve mapping	5.5.4	6.5.4	7.5.4

The following subsections describe the ICCP data objects in more detail.

8.8.1 Transfer Account Data Object

The ability to transfer scheduling and accounting information between ICCP implementations is a key feature of ICCP. With it, an ICCP client can set up a transfer set that will allow the server to send pre-schedules, next hour schedules, mid-hour changes, after-the-hour-actuals and historical information. ICCP generalizes this transfer capability to allow any data that is collected on an hourly (or other period) basis, including such data as generator schedules, interchange schedules, forebay and afterbay elevations, average hourly TOT limits and actual flows, pricing information, delivery point loads, etc. This is transfer capability is accomplished via the Transfer Account data object.

The flexibility of this object is achieved through the use of a matrix data type with the number of rows and columns defined by the user for each type of desired transfer. In addition the meaning of the column headings are also user-defined, so this standard data object can be used to transfer many different types of schedules and accounts.

An important feature of ICCP is the ability of the client scheduler or dispatcher to specify the time frame for the data to be retrieved and have the server return the specified information corresponding to that time frame. The client specifies this via the TAConditions object described below.

The transfer account object definitions can be found in 870-6-802 section 6.2. A transfer account example is provided in informative annex A of 870-6-802.

8.8.1.1 The Meaning of TA Conditions and How to Use Them

TAConditions (Transfer Accounts Conditions) are used to allow the client to set up condition monitoring of specific accounts in the server. Within the electric power utility business, the transfer of scheduling and accounting information is very time dependent. To illustrate this time dependency, a utility might have the following scheduling and accounting time frame requirements:

- Pre-schedules must be completed by 16:00 the day before they are used.
- Next hour schedules must be completed by 20 minutes prior to the hour in which they will be used.
- Mid-hour changes can occur anytime within the current, already scheduled, hour.
- After-the-hour-actuals are due by 10 minutes past the just completed, previous hour.
- All 24 hours of historical forebay elevations for the previous day need to be transferred at 10 minutes past midnight of the current day.

The client can instruct the server to monitor specified accounts for specific TAConditions and have the server automatically generate and transfer the account information when the condition is met. The actual time frames used are a local implementation issue. Since the exact formatting of the Transfer Account data object is user defined, it is possible to have a different format for data corresponding to each TACondition. The Transfer Account Reference number can be used to further identify the format of the report being transferred.

8.8.1.2 Transfer Account Structure

Scheduling and accounting data is stored by utilities in what is essentially a matrix structure. ICCP carries forward the matrix concept, but generalizes it to allow the user to define the meaning of the columns. Both floating point and integer matrixes can be transferred. This allows the ICCP client and server to exchange virtually any type of matrix format data in addition to scheduling and accounting data.

Generally speaking, the actual Transfer Report used to transfer a Transfer Account Data Object identifies the account to be transferred, the transfer account condition (TACondition), the sending and receiving utilities, the start time (referenced by hour ending, if hourly scheduling and accounting information is being transferred), and the time span of the period used (typically one hour). The message then specifies whether or not

this is a wheeling transaction, and if so, the number of wheeling segments is identified. For each segment, the number of floating (or integer) values and the number of periods (the values that will form the matrix of information) are identified.

In the event that a matrix of information is being transferred that has specific meaning to the client, a list of local references can be identified which will provide the client system with the column heading information for the matrix.

8.8.1.3 Examples

Exhibit 8.8.1.3-1 illustrates the structure of this object. Up to one floating point matrix and one integer matrix can be sent in one Transfer Account object. Exhibit 8.8.1.3-2 shows the use of this object to send two matrices of data for a time period covering one hour with a period resolution of 15 minutes.

A more detailed example of the use of the Transfer Account object is provided in the informative annex A of 870-6-802.

Exhibit 8.8.1.3-1, Transfer Account Data Object Model Structure

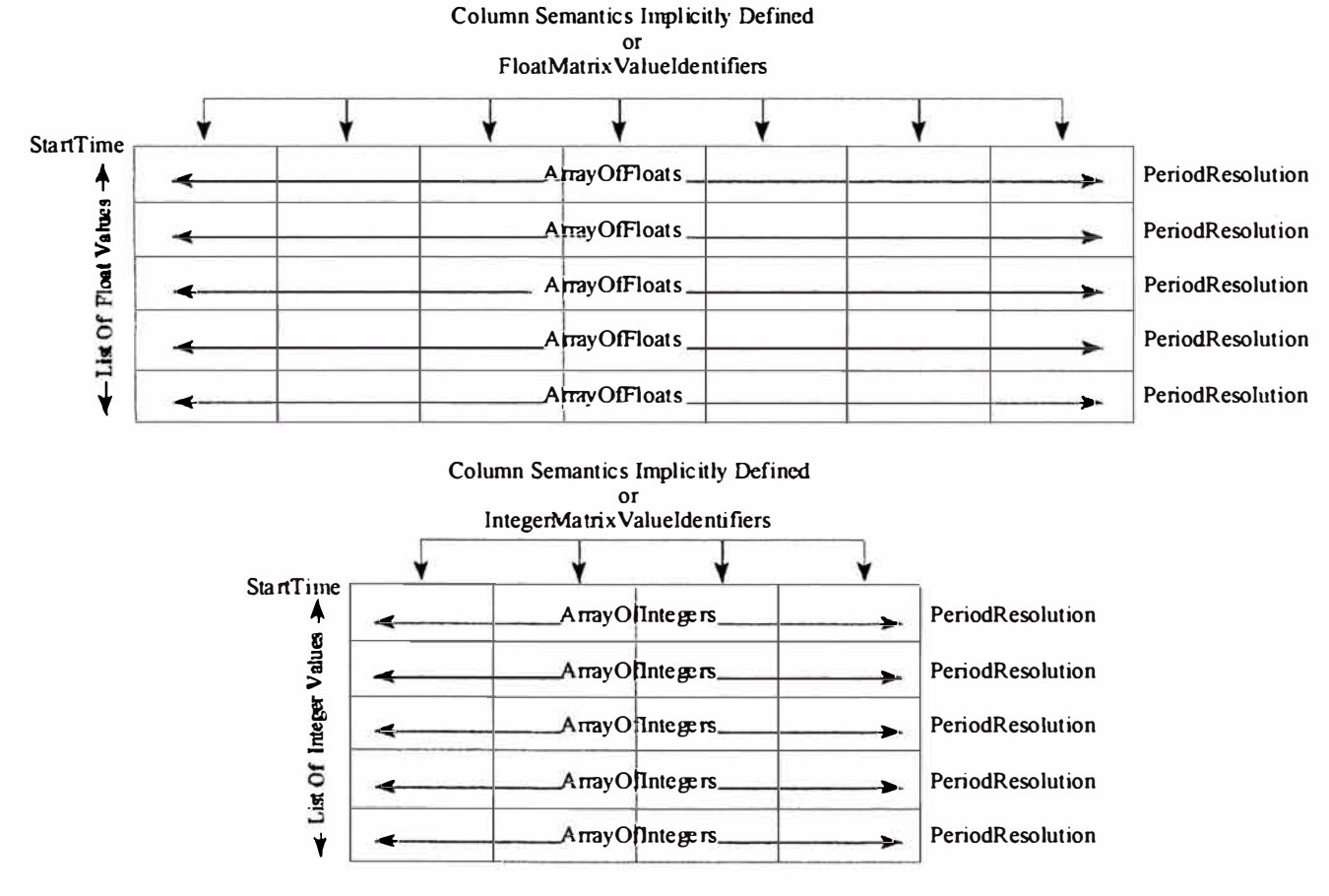


Exhibit 8.8.1.3-2, Example of Transfer Account Data Object Use

StartTime: 10:00 AM

Period Resolution: 00:00:00:15:00

Column Semantics: Implied by TransferAccountReference

Floating Point Matrix

	Seller Cost	Buyer Cost	Emergency Cost	Tariff Value	Tariff Incurred	Tariff Avoided	Savings
10:00 AM							
10:15 AM							
10:30 AM							
10:45 AM							

Integer Matrix

	MWH	Emergency MWH	Area Load
10:00 AM			
10:15 AM			
10:30 AM			
10:45 AM			

8.8.2 Device Outage

Utilities deal with two types of equipment outages, planned and unplanned. Planned outages of generators, transmission lines and line devices for maintenance and unplanned outages due to system disturbances which result in no, partial or full curtailments of power transfers. ICCP provides an object for the transfer of outage information.

The DeviceOutage object identifies the location of the device (StationName), the device (DeviceType) and provides information about the device (DeviceName, DeviceType and DeviceRating). If the outage is planned, then the object information can be used to set up a new outage or revise an existing planned outage. In either case, the out of service and return to service date and times are provided. The outage type can be categorized and if

it is an outage resulting in a partial curtailment, new upper and lower operating limits can be specified.

If the outage is an Actual outage as a result of unplanned operation of devices in the electrical system that resulted in a loss of load, the type of action is categorized and the amount of load that was being carried at the time of the service interruption is provided.

The device outage object definition can be found in 870-6-802 section 5.3.

8.8.3 Power Plant Objects

ICCP has been extended to include communications between the SCADA/EMS and power plants. Power plants have specific requirements that result in specialized objects. These objects take advantage of the existing underlying ICCP services available such as report-by-exception and condition monitoring.

8.8.3.1 Power Plant Availability Report Object

The power plant availability object is used to allow a generation station to inform the control center of the known or scheduled availability of a unit at that site. The object can also be used to schedule a unit outage or curtailment. If it is reporting a unit curtailment, new operating constraints can be reported for the period of the curtailment.

The object identifies the generation station location and the specific unit referenced in the report. It also identifies the start and stop time as well as the duration of the proposed change of status of the unit, either AVAILABLE or UNAVAILABLE. A curtailment is treated as AVAILABLE with a change of operating constraints.

If the unit is AVAILABLE, the report allows the generation station to specify for the duration of the availability:

- A new price
- New maximum ramp rates both up and down
- New gross maximum and minimum capacities
- New net maximum and minimum capacities
- Whether the unit is in standby or on-line mode

  If the unit is on-line, whether it is available for load following

  If the unit is on-line, but not available for load following, the reason (STARTUP, UNSTABLE)
- If the unit is UNAVAILABLE, the reason it is unavailable (FORCED, SCHEDULED, TESTING).

The reporting generation station can also report whether the unit is providing reserves, and up to 256 characters of user comments.

The power plant availability report object definition can be found in 870-6-802 section 5.5.1.

8.8.3.2 Power Plant Real Time Status Object

The power plant status object is used to allow a generation station to inform the control center of the current status of the plant and each unit at that site.

If the plant is AVAILABLE, the report allows the generation station to report the current operating characteristics of each unit.

- The maximum ramp rates both up and down
- The gross maximum and minimum capacities
- The net maximum and minimum capacities
- Whether the unit is in standby or on-line mode

  If the unit is on-line, whether it is available for load following

  If the unit is on-line, but not available for load following, the reason (STARTUP, UNSTABLE)
- Whether the unit is externally blocked high or not
- Whether the unit is externally blocked low or not
- If the unit is UNAVAILABLE, the reason it is unavailable (FORCED, SCHEDULED, TESTING,EQUIPMENT).

The power plant real time status object definition can be found in 870-6-802 section 5.5.2.

8.8.3.3 Power Plant Forecast Schedule Object

Some power plants and units are operated with pre-scheduled base points. These units are either not used for load following or have pre-defined load following periods. This object allows base points and operating modes to be transferred to the generation stations. Modes of operation can be user defined in the event that load following or not load following does not adequately describe the required modes.

The scheduled period for which a megawatt base point value applies can be specified in the object. Normally, one hour (hour ending) would be used, but the user can define other scheduled period durations. The only constraint is that all the referenced periods have to be of equal duration.

The power plant forecast schedule object definition can be found in 870-6-802 section 5.5.3.

8.8.3.4 Power Plant Curve Object

The power plant may wish to transfer data in the form of two dimensional curves. These curves could be incremental heat rate, hydro head dependent efficiency curves, cost curves or other power plant related curves.

The curve is defined as an nth order polynomial. All the segments in the curve are of the same order. Each segment of the curve is represented by a start of segment and an end of segment, and mathematically by the nth order polynomial: $A_0 + A_1x + A_2x^2 \ldots A_nX^n$. In representing each segment's polynomial, only the coefficients, $A_0 + A_1 \ldots A_n$ are

transferred. Knowing the order of the polynomials and these coefficients, the client can reconstruct the curve.

The power plant curve object definition can be found in 870-6-802 section 5.5.4.

8.9 Block 9 (Time Series Data)

Block 9 adds the Time Series Transfer Set server object.

Block 9 provides an ICCP client with the ability to receive time series data. Time series data might be data that has a required sampling time too fast to conveniently transfer it continuously between ICCP implementations and is not needed at the client site in real time. Examples of this type of data might be 200 millisecond sample on key analog values on the backbone transmission system during a disturbance. The values once collected might then be transferred as historical data to a disturbance analysis center. Real-time trending of values with longer reporting periods for more efficient use of communications bandwidth is another potential time series data application.

In setting up a time series data transfer, the client establishes the begin time and the end time. Both begin time and end time may be in the past, in which case the server immediately generates a report of historical values based on the time frame specified. If the begin time is the current time or 0, the server begins to immediately collect values until the end time occurs. At the designated end time, the server stops collecting values and generates a report for the client. If the end time is the current time or 0, the server assumes current time and stops collecting values and generates the report. For a planned collection of values in the future, the client can specify both a future begin and end time.

Two intervals are specified to make the collect and transfer of information as efficient as possible. The sample interval specifies the collection rate at the server. The reporting interval specifies the time between reports.

Several option exist to fine tune the reporting functions of the server. Since the end time may not fall exactly on one of the reporting period boundaries, the server can be instructed to generate a report at the specified end time. Similarly, the server can be instructed to generate a report at the initial enabling of the transfer set and at each reporting period. The server can also be instructed to allow an operator at the server system to initiate on demand a transfer of the time series data collected since the last reporting period

The time series transfer set object model can be found in 870-6-503 in section 5.2.9.2 and the time series transfer set object model mapping can be found in section 6.9.2.

9. Mapping Utility Data to Conformance Blocks and Control Center Data Objects

A utility planning to use ICCP must perform several tasks before knowing exactly which Conformance Blocks are required to meet its needs. The following issues will need to be addressed:

a) The data to be transferred needs to be identified and performance requirements established. This will uncover which ICCP services are needed, and hence which ICCP server objects and Conformance Blocks are needed. For instance, if SCADA data, schedule/accounting data, and

text reports are to be transferred, then Conformance Blocks 1,2,4, and 8 will be required.

b) Analyzing data to be transferred will also identify which data objects are needed. For instance, if in addition to scheduling/accounting data, outage information for scheduling and reporting outages is needed, then either the Device Outage object or a combination of the Availability and Real-Time Status objects will probably be required.

c) Each data element will need to be mapped to an ICCP object attribute. This mapping will need to be documented. Every attempt should be made to map to existing standard objects specified in the ICCP specifications, since this will ensure interoperability with other ICCP vendor products without additional software development.

d) Some types of data reports will not map 1:1 to standard ICCP objects. The choice will then be one of the following:

   i) "Force fit" a data element to an attribute with a different meaning. This eliminates any ICCP software changes, but creates the opportunity for misunderstandings of meanings of attributes.

   ii) Add a new attribute to a standard object, thus customizing it. If no new data types are introduced, this will result in minimal change, but will ensure there is no misunderstanding. Eventually common usage may result in a modification of the standard object.

   iii) Create a whole new data object. Sometimes, this is the only choice. This process is described in the next section.

e) All the choices made will need to be documented. A Network Interface Control Document (NICD) is commonly used for this purpose. This document is not defined anywhere since it goes beyond what is specified in the ICCP specifications, but by common practice it includes the mappings, the common conventions decided on for assigning numbers or codes to reference numbers, the definition of any new data objects, etc. For data objects that use the Matrix data type, the meanings of column headings and the number of rows for different uses of this object will also be documented here.

10. Definition of New Data Objects

The designers of ICCP expected that new objects would be needed from time to time. Not all possible uses of ICCP could be envisioned during the creation of the initial revision of the specification. If the process of mapping actual data requirements to ICCP objects described in the previous section requires a new object, then the process described in this section should be followed.

The process for creating a new data object is as follows:

A. Develop an abstract data model, creating a name for the object and deciding which attributes are needed along with a definition of each attribute. The object model definitions in the ICCP specification provide examples of how this is done. This can be done by end users with little or no knowledge of MMS.

B. The abstract model then needs to be mapped to concrete structures with components. Part of this process is assigning data types to each attribute. The goal is to reuse the data types already defined in the ICCP specification, thus minimizing the implementation effort for the new object.

11. Using the PICS

Section 9.2 of 870-6-503 contains a Protocol Interface Conformance Specification (PICS) table which lists all the conformance requirements (i.e., model definitions and attributes, operations, and actions) that have been defined for ICCP. The requirements fall into two categories: Mandatory and Optional. The requirements are grouped according to the ICCP server objects. A vendor must implement all Mandatory features for an object and may implement the Optional features.

An end user needs to specify which Optional features are desired when procuring or implementing an ICCP instance. Typically this would be specified in detail in a software Functional Specification for ICCP.

12. Bilateral Table Issues

ICCP specifies access control through the use of Bilateral Tables. The functionality required is clearly presented in 870-6-503. The type of access for each ICCP data object is defined via these tables. However, implementation is left as a "local implementation issue." This includes the management and maintenance of these tables. As a result, each vendor is free to choose how to implement the functionality for Bilateral Tables, including what type of operator interface to provide. This means that an actual physical table is not necessarily required, as long as the functionality is implemented according to the ICCP specification.

A common request from end users is to have a capability for an ICCP client to view the Bilateral Table at an ICCP server to determine which objects it has access to and to be notified whenever that table is updated. The ICCP specifications do not specify a way to accomplish this, although there is a Data Value operation, Get Data Value Names, which an ICCP client can use to obtain a list of all the Data Value objects accessible to that client. A "browser" capability could be quite useful for a user acting as an ICCP client, which would let a client view the objects it has access to, and then simply point and click which objects it wants to receive. Part of the functionality could include creating data sets by pointing and clicking. This would minimize the potential for operator error on entering data values.

Some users may not desire to use the security mechanisms provided through Bilateral Tables, for instance, where ICCP is used between two regional control centers within the same utility. One way to handle this is just to provide the same access to all control canter objects in the VCC to any client. However, the protocol operations and actions specified in the ICCP specifications still must be implemented to ensure interoperability.

13. User Interface Issues

The ICCP specifications do not specify a user interface for managing and maintaining ICCP. This is left as another "local implementation issue." Each vendor is free to choose an appropriate interface.

The following areas may need a user interface:

- Displaying ICCP performance data, such as status of each association and data link, last error detected, throughput statistics, etc.
- Control of data link associations, data sets, or other ICCP objects to enable or disable selected capabilities
- Creation and editing of Bilateral Tables
- Creation and editing of Data Sets
- Setting up and managing broadcast groups for information messages when Conformance Block 4 is implemented. Since ICCP does not provide a broadcast capability, it may be desirable to have the ability to create broadcast groups that would specify groups of destinations (i.e., other ICCP sites or operator consoles) to receive information messages.

14. Other Local Implementation Issues

ICCP is a standard real-time data exchange protocol. It provides numerous features for the delivery of data, monitoring of values, program control and device control. All the protocol specifics needed to ensure interoperability between different vendor's ICCP products have been included in the specifications.

The ICCP specifications, however, do not attempt to specify other areas that will need to be implemented in an ICCP software product but that do not affect interoperability. These areas are referred to as "local implementation issues" in the specification. ICCP implementers have the freedom to handle these in different ways and can therefore differentiate their products by the way handle these issues. For example, one vendor may have a graphic-oriented user interface permitting point and click operations for creating data sets or controlling ICCP data links, while another may provide only programmer's editing tools to accomplish these tasks.

Local implementation issues in the specification include but are not limited to the following:

- The API through which local applications interface to ICCP to send or receive data
- A user interface to ICCP for user management of ICCP data links
- Management functions for controlling and monitoring ICCP data links
- Failover schemes where redundant ICCP servers are required to meet stringent availability requirements, such as those typically experienced in an EMS/SCADA system environment
- How data, programs or devices will be controlled or managed in the local SCADA/EMS to respond to requests received via an ICCP data link

These responsibilities fall to the SCADA/EMS vendor and the implementing utility. This section will attempt to address some of the areas that have been specially identified as local implementation issues in the ICCP specifications that have not been covered elsewhere in this guide.

14.1 Client Server Association Management.

The client always initiates the association establishment procedure with a ICCP server. A single ICCP site can act as both client and server to one or more ICCP sites. It can also

simultaneously be just a client or just a server to other sites. In the case where it is both client and server with another site, the use of the associations between the two sites is a local implementation issue. The simpler method to implement is where each client uses a different association with its server. However, it is possible to utilize the same association for the client-server pairs in both directions. This implementation is more complex, but is also more resource efficient. If a site that can utilize one association for both client-server directions (dual use) attempts to establish an association with a site that does not support dual use, it is the responsibility of the dual use site to fall back to single use associations. It is a local implementation issue whether or not to support dual use associations.

14.2 Local Implementation Setup Issues.

When a utility implementing ICCP joins an existing network or begins communicating with another ICCP implementation, there are a number of issues that should be decided among the data exchange members.

1. Pre-defined Data Set object names must be published to appropriate data exchange partners.
2. The maximum number of associations that will be allowed
3. The maximum exchange frequency of data should be agreed to in order to avoid overloading a SCADA/EMS with data request
4. Which data types can be specified as critical data
5. The use and specification of retry counters
6. The assignment of values to the Information Reference Number used by most data objects.

14.3 Specific Conformance Block Issues.

Individual conformance blocks in ICCP have specific user considerations. Some of these issues are local to the utility and some are issues that should be discussed with the ICCP and SCADA/EMS vendors prior to procuring an ICCP implementation.

14.3.1 Block 1 (Data Set Definition Management)

A concern among ICCP users is how to ensure synchronization of data set definitions at both the client and server sites.

14.3.1.1 Data Set Definition

The approach assumed by ICCP is for the client to create all data sets each time the association for transferring the data defined in data sets is established with another ICCP server. This would ensure data set definitions are synchronized at least each time an association is restored after being brought down for whatever reason. This means that the ICCP server would not retain any data set definitions after an association with a remote client is brought down. The main drawback for sites with large amounts of data seems to be the time required to create all data sets before any data is actually transferred, but this approach must be used if interoperability is to be guaranteed.

A second approach is for the server to always retain data set definitions whether or not associations exist with a ICCP client. Then it would be up to the client to periodically or on request to verify the definitions at the server, perhaps using the Get Data Set Names and Get Data Set Element Names operations to compare the lists of Data Value object at the server with the lists known at the client. However, this requires that both the client and server expect to operate in this fashion ahead of time.

14.3.1.2 Data Set Updates

How does an ICCP client know when a server site changes the list of available Data Value objects? ICCP does not provide a mechanism for data base management that would alert a client of such changes. Therefore some scheme needs to be defined outside ICCP. The simplest approach is to have an ICCP server site operator agree to email, phone, or FAX notices of any changes affecting a client (i.e., addition, deletion, or modification of a point). Perhaps changes could be sent as low priority alarms. The optimum approach would be to have the client poll the server periodically using the ICCP Get Data Value Names operation and then locally display and highlight any changes.

14.3.2 Block 2 (Extended Data Set Condition Monitoring).

When using report-by-exception, there is always a small chance that due to either the client or the server system being down, or due to communications problems, that the two databases will not be identical. The integrity scan (analogous to an RTU integrity scan) is used by ICCP to resynchronize databases. The use and frequency of integrity scans should be decided by data exchange members who have implemented Block 2.

When using report-by-exception for analog values, the use and specification of deadbands that reduce unnecessary transmission of minor changes should be decided by data exchange members.

An issue for discussion between the ICCP implementers and the utility is where the deadbands for analog and database state for status points will be monitored. Is this a SCADA/EMS or an ICCP implementation responsibility?

14.3.3 Block 4 (Information Messages)

14.3.3.1 Operator Messages

Block 4 can be used to send operator messages. After an ICCP implementation has received an operator message, it must be passed to the SCADA/EMS for presentation to the dispatchers or operators. How will the SCADA/EMS display, save, retrieve and purge the resulting message files?

14.3.3.2 Binary File Transfers

Block 4 allows for the transfer of small, binary files. These files will need to be stored in SCADA/EMS directories and the end user notified that they have been received. Will existing files automatically be overwritten? Will the local SCADA/EMS utilize the version information to automatically create new copies of the file? How will end users be notified? What convention will be used to identify the binary files as EXCEL, MS-Word, Word Perfect, etc.?

14.3.3.3 Requesting an Information Message Object

ICCP does not support the request of a specific information message or object. Some utilities have solved this problem through establishing a convention for the use of the Information Reference number, which is a 32 bit integer. This number can be broken down into 9 bytes or fields. Each byte (or combination of 2 or more bytes) can be assigned a meaning. One byte can be reserved for indicating whether the information message is a request for a specific information message object or whether it is the actual object. For example, byte 4 could be encoded as follows:

1. Information Message data object
2. Request for the Information Message object identified by the rest of the Information Reference number.

The rest of the Information Reference number would remain unchanged. The Info Stream attribute would be empty for the request.

14.3.3.4 Segmenting Long Information Messages

Information messages must fit within the maximum length MMS PDU, which is 8000 bytes. If messages longer than this need to be transferred, an application above ICCP in the protocol stack needs to perform this function at both the client and server end of the association. Data fields provided by the ICCP information object can be used to convey to the receiving site the information necessary to reassemble multiple segments, but ICCP simply forwards this data without interpreting it.

One solution adopted by a power pool is to use the LocalReference or MessageId field in the InformationBuffer object described in 870-6-802 section 6.4 to indicate if the message is completely contained in the PDU or if it is segmented into two or more segments. If more than one, a value is assigned corresponding to the order of the segment in the total sequence and whether or not it is the last segment.

14.3.4 Block 5 (Device Control).

During a device control operation the server provides a CheckBackName to the client to allow the client to verify that the server has selected the expected device. The content of the CheckBackName is by agreement of the two sites.

After receiving the select request from the client, the server is required to make local checks to verify that the device is operational. The checks that will be performed (for example: communications to the device available, status of the device is current, device is free of blocks or inhibiting tags, etc.) are determined by the server implementation.

14.3.5 Block 6 (Program Control).

The invocation of programs requested by an ICCP client will use other SCADA/EMS services to initiate and control the programs. Local implementation issues include program scheduling, execution monitoring of scheduled programs, priority of execution, which processor the program will be assigned to, and exception and abort processing.

14.3.6 Block 8 (Transfer Accounts).

14.3.6.1 Meaning of TAConditions

The TAConditions refer to general periods of time before, during, and after a schedule is in effect. All parties sharing schedules and account data need to agree to specific time periods to associate with each TACondition and also agree to the format of the data reported under each condition. An alternative used by some utilities is to make all transfers occur as a result of Object Change or Operator Request only. The types of reports to be sent are agreed to and assigned unique Transfer Account Reference numbers. Then as the data becomes available (or changes) for each report type, it is sent with the appropriate number so that the client can interpret the data contained.

14.3.6.2 Complex Scheduling Transactions

For many utilities a transfer of a schedule is just one step in a more complex transaction. For instance, a member company in a power pool may submit a proposed schedule to the power pool operator, who first acknowledges receipt, then reviews and either accepts or rejects. If rejected, the member company then needs to submit a revised schedule. If accepted, the member company then needs to confirm. ICCP itself contains no provisions for maintaining a "memory" of each step of the transaction. Such "memory" needs to be implemented in an application above the ICCP API.

Some utilities have solved this problem through establishing a convention for the use of the Transfer Reference Number, which is a 32 bit integer. This number can be broken down into 9 bytes or fields. Each byte (or combination of 2 or more bytes) can be assigned a meaning. One byte can be reserved for indicating the status of a schedule in the approval process. For example, byte 4 could be encoded as follows:

1. Original submittal
2. Received (acknowledged)
3. Approved
4. Rejected
5. Revised
6. Confirmed

The rest of the Transfer Account Reference number would remain unchanged, and the entire data object would be retransmitted each time with any needed revisions to attribute values.

Note that this approach could also be used to provide just a simple acknowledgment that any Block 8 object was successfully received by a client. ICCP does not provide an application-level acknowledgment. It instead relies on the Transport layer to deliver an error-free message or retransmit it transparently to ICCP in the Application layer. If it is unable, the Transport layer would take down the connection, thus notifying both the ICCP client and server of a problem. Otherwise, ICCP assumes the message is received error free. The application above ICCP implementing this capability could then also maintain records of all messages sent to ensure no data is lost.

14.3.7 Block 9 (Time Series Data).

A request may be made for time series data to be collected for a specific point at a specific sampling interval. The reporting request may then expire or be terminated. A subsequent request for data from the same point may specify a different sampling interval with a begin time that includes historical data with the first sampling time. The historical data must then be extrapolated such that the new sampling interval is identical for all reported data. How the server will extrapolate that historical data (linear, best fit, etc.) is an implementation issue for the server system.

15. Network Configuration

One of the first issues to be addressed by a potential user of ICCP is whether the ICCP communications processor should be integrated into the SCADA/EMS LAN or function as a stand-alone gateway processor. Legacy systems are the most likely candidates for standalone processors. Both implementation configurations have advantages and disadvantages.

In the case of an integrated processor, the access to the SCADA database is direct, without any intervening protocol. It is easier to implement the functionality provided in ICCP if the ICCP client or server has direct access to the SCADA database and operating system. Functions such as program initiation, monitoring of database points for report by exception, control operations and operator messages are all simplified with direct access. Security, however, becomes more of a concern where the processor that communicates with outside the controlled environment of the SCADA/EMS system provides a potential path of access. Firewalls and other security may be needed where the connections are to other entities whose systems may be open to the Internet or other outside networks.

Users considering the use of ICCP need to decide how to acquire the ICCP software. ICCP products available commercially from vendors are typically packaged in one of three ways:

A. **As a protocol native to the EMS/SCADA system**. This type of ICCP product is typically offered by EMS/SCADA vendors as a standard product associated with their standard EMS/SCADA system (hence the use of the term "native"). The software will run on one of the standard hardware/software platforms used for other EMS/SCADA applications, and thus may be considered to be closely integrated into the SCADA/EMS operating environment. Typically the ICCP software features the same API as other EMS/SCADA applications. This approach is sometimes referred to as an integrated processor approach.

Not all EMS/SCADA system vendors that offer ICCP actually use this approach. Some provide only a stand alone gateway processor (described below).

The advantages of this approach are:

- All EMS/SCADA applications have direct access to the ICCP API, providing full functionality to them and possibly better performance. Operator messaging and device control may be simpler to implement with this approach.
- SCADA can be retrieved from (and deposited into) the real-time SCADA data base directly. Monitoring and notification of SCADA data changes is direct.

- A separate relational data base is not required to buffer data - the relational data base associated with the EMS/SCADA system can be used directly.
- System administration and maintenance is accomplished using the standard EMS/SCADA system/network administration tools.
- User interfaces will have the same look and feel as for other EMS/SCADA user interfaces.
- Since the platform is the same as for other SCADA/EMS applications, common servers can be shared between ICCP and other applications. This also helps the spares and maintenance problem.

The disadvantages are:

- This approach may not be available for legacy systems
- If a proprietary API is used, it may prevent open access to other possible users of ICCP outside the EMS/SDADA environment
- Security may be a concern where the processor that communicates with systems outside the controlled environment of the SCADA/EMS system provides a potential path of access. Routers, firewalls and other security may be needed where the connections are to other entities whose systems may be open to the Internet or other outside networks.

B. **As a tool kit from a third part supplier.** This approach typically provides ICCP software on a stand alone platform (i.e., Windows NT on a PC), but provides an API with full functionality for an EMS/SCADA system or other control center computer that has TCP/IP, NETBIOS, DDE, SQL, or other industry standard communications networking capabilities.

The advantages of this approach are:

- Provide the same (or nearly the same) capability as a native ICCP implementation for an EMS/SCADA system whose vendor does not offer a native ICCP implementation
- May provide a more open API to enable open access to the ICCP messaging services by other control center users
- Should be low cost solution

The disadvantages are:

- May have a different look and feel for the user interface
- May not use same network administration tools as EMS/SCADA system
- May require custom development work to interface to the EMS/SCADA system

C. **As a Standalone Gateway Processor or Communications Node Processor (CNP).** This approach is for providing ICCP capability to a legacy system with limited communication networking capability. Typical offerings permit connection over either a serial line or a LAN, using TCP/IP as the transport protocol. Some typical messaging protocols offered include the following:

- IDEC Host-to-CNP protocol, developed for the same application for a CNP implementing the IDEC protocol. This is a simple block transfer protocol that

has been implemented by several vendors. This requires that the legacy EMS/SCADA system have software running that also talks the Host-to-CNP protocol

- FTP. This requires that data to be transferred be formatted as flat files. Custom parsing software is required at both the host processor and the ICCP gateway processor. If only limited SCADA data (i.e., analogs and status) are to be sent at low periodicities, this may be an acceptable approach
- Emulation of a legacy system protocol, such as WSCC or some existing proprietary protocol. This would have no impact on the host system, but would required custom emulation software in the ICCP gateway. However, some vendors already provide WSCC and IDEC emulation. Others provide ICCP gateways that emulate one of their existing proprietary EMS data link protocols for their own legacy systems
- New custom protocol between the gateway and the legacy system. This may be acceptable for limited uses of ICCP, but would probably require excessive development to utilize all the features of ICCP.

The advantages of this approach are:

- May be only way to implement ICCP for a legacy system
- May have minimal impact on legacy host computer
- May provide additional security

The disadvantages are:

- A second protocol is required between the gateway processor and the host computer
- Limited functionality of ICCP via the restricted host-to-gateway protocol and serial connection. Implementing object transfers, control operations, accounting information transfers and operator messages across an intervening protocol requires that two databases be maintained and that additional applications be implemented to carry the ICCP functionality all the way to the SCADA/EMS.
- Separate database required on the ICCP gateway processor to store and buffer ICCP data, which may be different from that used on the EMS/SCADA system, creating training and maintenance issues
- May be different operating system and processor hardware, requiring different system/network administration, additional licenses and spares.
- Lower performance and throughput with greater time delays in transferring data are likely

16. Security

ICCP provides access control via the Associate operations to establish an association. The client must identify itself to the server. The server must have a Bilateral Table in place for that client and the Bilateral Table version numbers must match. Otherwise, the server

must Conclude the association. As previously described, the Bilateral Table identifies all objects the client is authorized to access and the level of access permitted for each object.

ICCP does not provide mechanisms for authorization or for encryption. These would normally be provided by lower layer protocols.

17. Profiles

17.1 OSI

As stated earlier, ICCP was originally designed for operation of OSI/ISO-compliant protocols, specifically the protocols identified in UCA Version 1.0. This has been the norm for vendor implementations up to the current time. The current effort to standardize ICCP also assumes a fully-compliant OSI protocol stack.

17.2 TCP/IP

Depending on the vendor providing ICCP, it may be possible to operate ICCP over TCP/IP. There are two possibilities proposed for UCA Version 2.0 to accomplish this:

A. OSI Layers 5-7 including ICCP directly over TCP/IP. This approach replaces ISO TP4/CLNS in Layers 3-4 with TP0 over TCP/IP. This approach is specified in RFC 1006 and is the most widely supported by protocol vendors. However, TP0 over TCP/IP does not have the same capability as TP4 regarding QOS parameters and the automatic checking via "keep alive" messages to ascertain that a data link has not gone down. To provide an equivalent capability, the Application layer using ICCP would need to generate periodic test messages. In practice, this may not be a problem since most ICCP links are expected to support the transfer of periodic SCADA data at rates as often as every 4 seconds, and any attempt to send data over a failed link would get reported immediately.

An unresolved issue identified is the reporting of error messages from the transport layer. It is not clear if MMS maps error messages from TCP and TP4 to the same error codes for reporting to ICCP. If not, the transport layer will not be truly transparent to ICCP and the handling of different error codes would become a local implementation issue.

B. OSI layers 3-7 encapsulated in UDP/IP messages. This approach uses RFC 1070. It retains the QOS and automatic detection of outages, but does require the maintenance of two address spaces (i.e., the ISO CLNS network layer addresses and the TCP IP layer addresses).

The consensus regarding ICCP and MMS is that the transport layer should be mostly transparent, so that either TP4/CLNS or TP0/TCP/IP can be used. The idea of TCP use is that if a utility already uses TCP/IP, then it is probably preferable to use ICCP over TCP rather than introducing a full OSI stack just for ICCP. However, there is nothing to prevent a utility from running both stacks in parallel. The vendor used by the utility should be consulted to determine the actual choices available.

18. Procurement of ICCP

Because of the acceptance of ICCP by the utility industry, there are a number of ICCP products on the market. These can be obtained from either EMS or SCADA vendors as

well as third party suppliers on a variety of hardware platforms and operating systems. As a result there should no need for a user of ICCP to have to develop new software to implement the protocol. Because of the extensive interoperability testing either accomplished or planned in the near future, interoperability of these products is not a high risk area, although data link testing is obviously required as part of acceptance testing.

However, there are a number of areas identified throughout the ICCP specifications and this guide which are referred to as "local implementation issues" that a vendor is free to handle in a variety of ways. There are also other system considerations and configuration issues that need to be clearly specified. As a result, it is recommended that a procurement specification be prepared to capture any requirements in these areas.

The purpose of this section is to help guide a prospective user in preparing such a procurement specification.

18.1 Preparing a Procurement Specification

A procurement specification should address the following areas:

a) Network diagram showing all networking requirements between ICCP nodes

b) System configuration at each ICCP node to identify all computer system interfaces from SCADA databases, RDBMS, power applications, or operator consoles to each ICCP server. This would require a choice of integrated processor or standalone gateway implementation of ICCP.

c) System requirements, such as sizing, performance, availability, backup and recovery (including whether redundant ICCP servers are needed and failover schemes required), and the use of certain corporate standards.

d) Functional requirements, such as which ICCP Conformance Blocks are needed, specific ICCP data objects needed, definition of any new data objects to handle the required data transfers, API needs, security required, number of associations and intended use of each, user interface (such as for Bilateral Table creation and editing, Data Set creation and editing, and network management).

e) Hardware requirements, such as the use of specific platforms, routers, LAN hub technologies, etc.

f) Support software requirements, such as standards to be followed, operating system, programming languages, editor and program development support tools, etc.

g) Project implementation requirements, such as project deliverables, customer and vendor responsibilities, project management guidelines, quality assurance provisions, testing, commissioning, warranty, maintenance support, documentation, and training.

18.2 Network Interface Control Document

In addition to a procurement specification, which serves to document all specific requirements for the ICCP vendor, there is usually a need for a document often referred to as a Network Interface Control Document (NICD). The NICD is needed to document agreements and conventions about such issues as

a) Mapping of specific data to ICCP objects and attributes

b) Variable naming, as for SCADA point names

c) Definition of the key attributes used to uniquely identify instances of ICCP objects, such as the Information Reference Number for Information Messages or the Transaction Reference Number for Transfer Account objects

d) Definition of requirements for any special applications developed to handle unique messaging needs beyond the ICCP specifications, such as complex transactions involving several ICCP message transfers, segmenting of Information Messages longer than 8000 bytes, or creation of any new data objects

e) Any other agreements between multiple parties all connected to the same ICCP network

19. Management of an ICCP Network

There is very little in the IEC specification dealing with management of an ICCP network. This section attempts to address common issues a user will be faced with in using ICCP. Actual capabilities provided with an ICCP software product will be vendor-dependent.

19.1 Configuration Management

19.1.1 Naming of Data Value Objects

Naming of Data Value Objects is a local matter. The names chosen should have meaning to all ICCP clients and servers wherever they are located. If ICCP is used internal to a single utility between control centers, then it may be that all sites use the same names locally. These names could be maintained for naming ICCP objects as well

If, however, ICCP is used in a power pool setting, for example, then one utility's names will not necessarily be used by another utility, even for the same substation (for instance, where a substation is between two utilities and therefore has many points monitored by both utilities). In this case, there are two choices:

A. A global network name for each point could be defined and used by all parties. Each utility would then map that name into a local name. This is the most common approach and probably the easiest to maintain.

B. The name used by the owner (source/server) of the data could be used by all, with a mapping done at the client from the server name to the client name, if necessary. This approach has the disadvantage that any local name changes by the owner/server of the data would require a change at every client location.

19.1.2 Creation of Data Sets

The creation of data sets is described as a client function in IEC 870-6-503. However, that document does not specify how they are to be created or what tools should be provided. This is a local implementation matter and will depend on the ICCP vendor. Special requirements should be specified in a procurement specification.

As a minimum, the vendor should provide an editor capability to permit an operator to define the contents of each data set and name it. It would be helpful if the operator could browse a list of Data Value objects a server site permits the client to see and access. This list can be obtained via the Get Data Value Names operation. This may require custom development beyond an ICCP vendor's standard offering.

An altemative approach is to automatically define and name data sets based on the same list of Data Value objects desired by the client for each ICCP server.

19.1.3 Association Management

ICCP assumes that associations will be brought up as part of an initialization procedure implemented in the ICCP software. However, the particular method used is a local implementation issue. Furthermore, ICCP assumes that associations are long lasting and once up will remain up until a data link is lost.

Therefore, any operator capabilities to control associations and/or data links (i.e., to enable/disable an association or data link) are defined by the vendor. If specific capabilities are required, they should be included in an ICCP procurement specification.

19.2 Performance Management

The ICCP specifications do not address monitoring of ICCP data link performance. Any features an ICCP user requires must be specified separately.

19.3 Fault Management

ICCP assumes an error-free transport mechanism is available via for transferring data unless an error message is received from a lower layer protocol. Therefore there are no test capabilities or fault management capabilities specified for ICCP.

As a result, any maintenance of error statistics or lost connections as well as an operator display of these features is considered a local implementation issue and will be up to the vendor to decide what capabilities, if any, to include with its standard ICCP product. If specific capabilities are needed, they should be included in the procurement specification.

20. Inter-Operability

A key feature of any successful protocol is its ability to quickly and easily inter-operate between different manufacturer's implementations. This inter-operability must also extend to later releases. ICCP has been designed from the beginning to be inter-operable. Keys to achieving inter-operability included:

- Early identification of utility requirements
- Involvement of key vendors on the design and test teams
- Early involvement of the Intemational Standards Organization
- Parallel development of the ICCP specification and vendor developed implementation of the ICCP protocol
- Encouragement of informal connectivity tests between four early ICCP developing vendors
- Performance of a formal set of inter-operability tests between four ICCP vendors

- Planned performance of a second formal set of inter-operability tests between up to eight ICCP vendors

The best practical test of real interoperability is to bring together the developers and in a controlled environment subject all possible pairs of vendor implementations to a comprehensive set of well defined inter-operability tests monitored by an impartial protocol expert.

In February of 1995, the UCSWG (Utility Communications Standards Work Group) held a series of inter-operability tests between four vendors: Harris, Siemens, ESCA and NSR. The results of these tests are available from EPRI as the ICCP Inter-Operability Test Report (see Reference 4). A summary of these tests is presented in the next subsection. A second interoperability test involving as many as nine separate ICCP vendors is planned for late 1996.

20.1 Summary of Interoperability Tests

In order to test ICCP inter-operability, four levels of interaction between all possible pairs of ICCP implementers were established. As each pair successfully achieved a given level as both client and server they proceeded to the next level until all participants had achieved level four. The four levels were:

Level-1	Network connectivity	Physical connection to the network
Level-2	MMS Association	Establishment of an MMS association
Level-3	ICCP Association	Establishment of an ICCP association including: exchange of Bilateral Table Ids exchange of ICCP version numbers exchange of ICCP negotiated features
Level-4	Block-1 Exchange	Periodic exchange of power system data

In all, thirty-two tests were performed between each pair of testers in turn, with each ICCP implementation acting as client or as server, and then changing roles. In some tests, outcomes were different depending on whether the system was acting in the client or the server role.

The results of the test clearly demonstrated that ICCP has achieved its primary goal of inter-operability across multiple vendor platforms. A second important goal was to strengthen the ICCP specification that was to go to IEC for international standardization. This goal was also achieved by the identification of several areas of potential miss-interpretation or different interpretation.

20.2 Version Compatibility

Version control is discussed in 870-6-503 section 7.1.1.1.1, where the client role in association operation and action is described. The version control object definition can be found in 8.1.9 as TASE2Version Type.

ICCP will continue to evolve as new objects are added and as new services are required. ICCP anticipates this requirement and provides for an orderly evolution of the protocol.

After verifying that the Bilateral Table ids are valid, an ICCP implementation client must retrieve the TASE2_Version object from the server and compare with the local version number. If a mismatch is found, the association is immediately terminated via the Conclude operation. No further association establishment requests are permitted until the conflict is resolved. However, the vendor may have implemented emulation software for previous versions and may be able to execute as if it were an earlier release of ICCP for compatibility reasons.

20.3 User Object Compatibility

ICCP consists of system objects (found in 870-6-503) and user objects found in 870-6-802. The user objects have been segregated into a separate document to enable that document to evolve independently from the less fluid services document.

The distribution of ICCP user objects found in 870-6-802 among the different implementation blocks is shown in section 9.

A company purchasing a particular implementation block should make sure that the objects related to those functions that they require as a business have been implemented by prospective vendors. The services required for any particular implementation block may be implemented without necessarily also providing the user with all the objects within that block.

ANEXO B

APLICACIONES ADICIONALES DEL SISTEMA DE MONITOREO EN TIEMPO REAL DEL REGULADOR

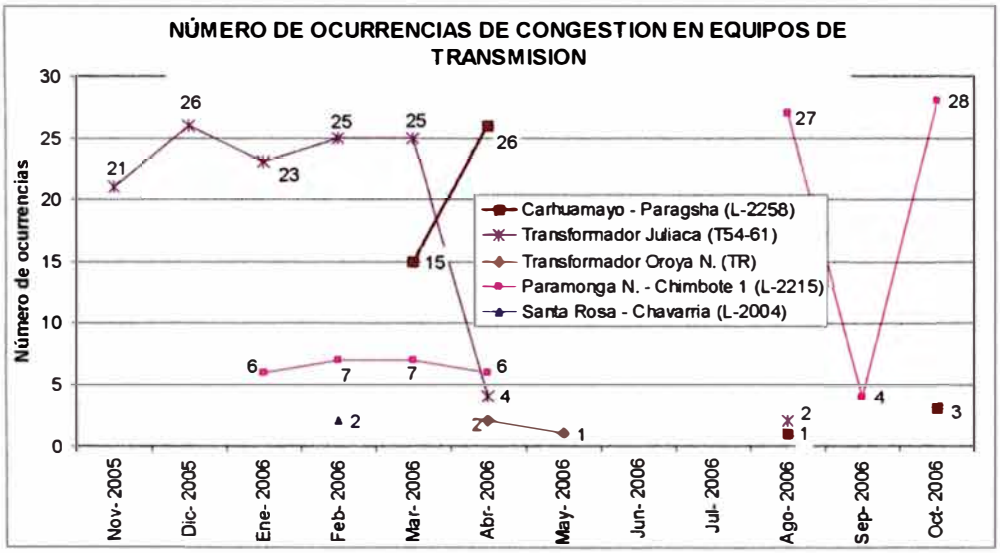
Con el Sistema de Monitoreo en Tiempo Real se podrá hacer un seguimiento a las variables que maneja el Coordinador para operar el SEIN de manera segura.

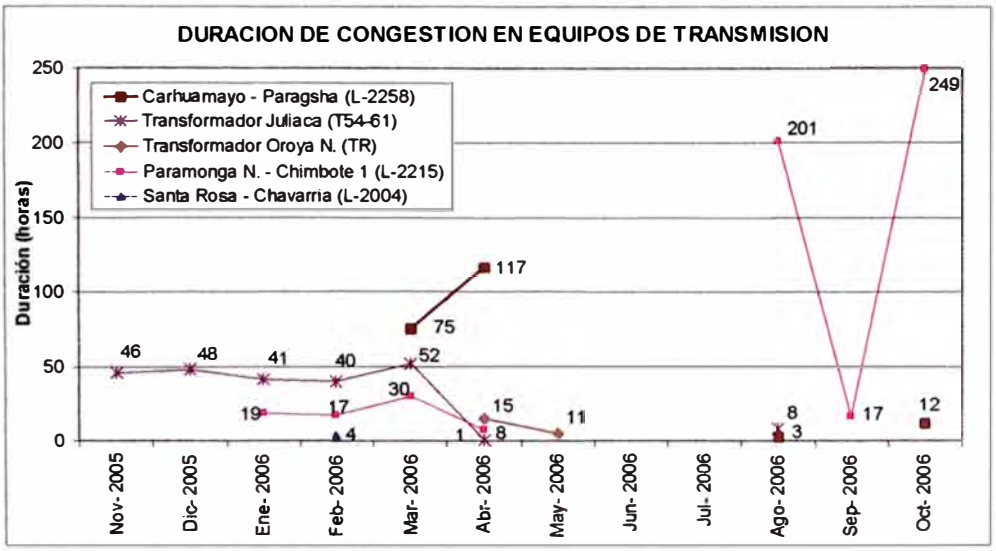
Como ejemplo se muestra el seguimiento a las congestiones en las instalaciones de transmisión.

CONGESTIONES DE EQUIPOS CONSIDERADOS EN LAS TRANSFERENCIAS DE ENERGÍA

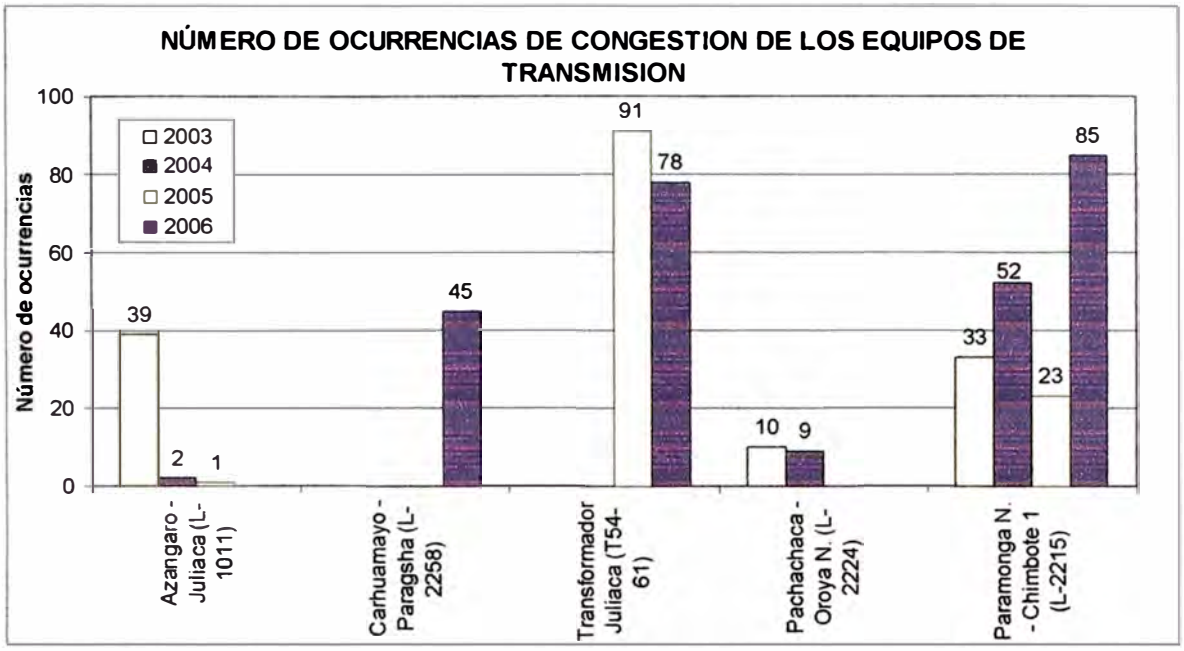
En el mes de octubre DE 2006 se produjeron treinta y dos (32) eventos que ocasionaran congestión en elementos del sistema de transmisión del SEIN.

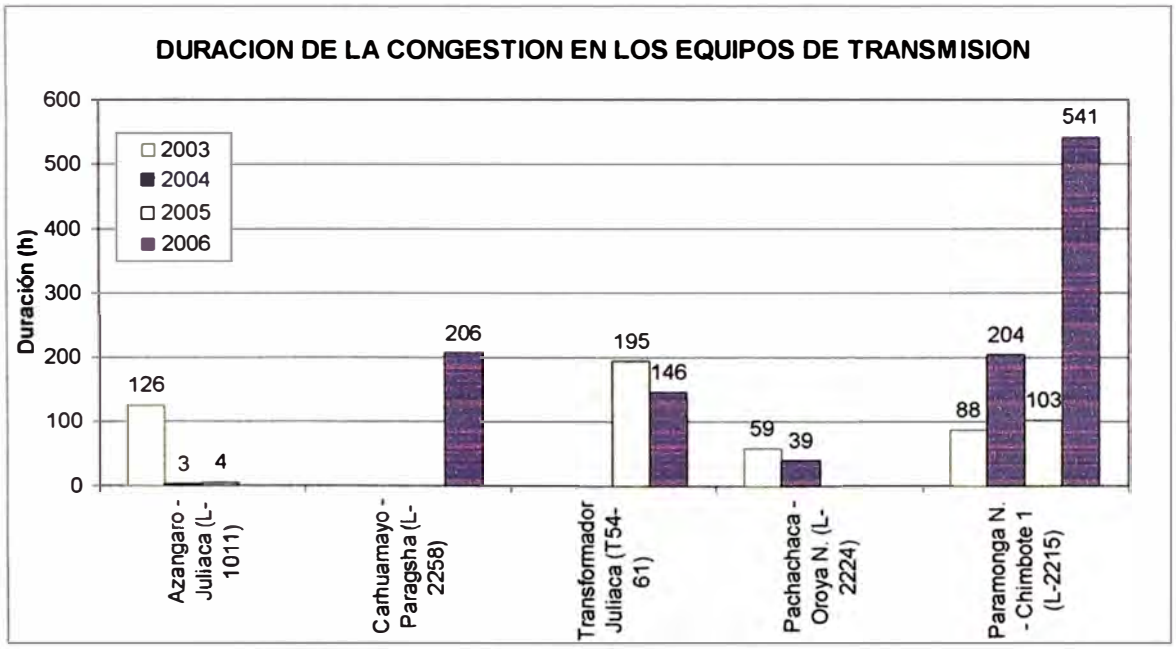
En los siguientes gráficos se aprecian los casos más relevantes de congestión y su evolución, tanto en número de ocurrencias (primer gráfico), como en duración (segundo gráfico).





Se resume a continuación la evolución del número de congestiones en los equipos más congestionados en los últimos tres años.

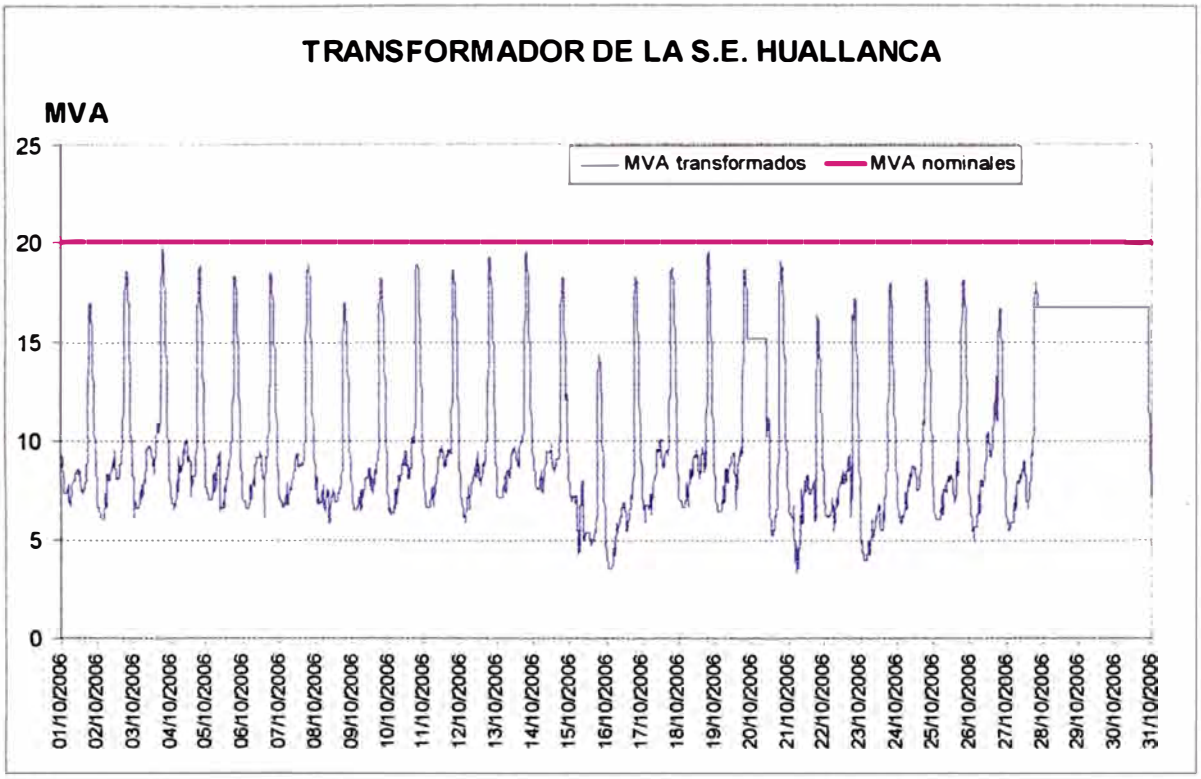




MONITOREO DE CONGESTIONES EN TIEMPO REAL

De la información obtenida de registros de Bases de Datos de Tiempo Real, se muestra en los siguientes gráficos los elementos del sistema de transmisión (en este caso transformadores), cuyo estado de operación se encuentra próximo a su máxima capacidad.

Se aprecia que el transformador de la SE Huallanca continúa con en hora punta con los valores llegando al nominal.



BIBLIOGRAFIA

[1] Manual del sistema SCADA SURVALENT

[2] Norma Técnica para la Coordinación de la Operación en Tiempo Real

[3] Ley de Concesiones Eléctricas

[4] Reglamento de la Ley de Concesiones Eléctricas

[5] Manual para el intercambio de información entre el coordinador y los Integrantes del Sistema Eléctrico Interconectado Nacional (SEIN)

[6] Términos de referencia para la adquisición del sistema de monitoreo en tiempo real del Regulador

[7] Guía de usuario del protocolo de comunicación ICCP (Inter-control Center Communications Protocol – ICCP TASE.2) (IEC 870-6-802).