

**UNIVERSIDAD NACIONAL DE INGENIERÍA**

**FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA**



**PROTOCOLO DNP3 Y SU APLICACIÓN EN SISTEMAS SCADA**

**INFORME DE SUFICIENCIA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**INGENIERO ELECTRONICO**

**PRESENTADO POR:**

**HUBERT MOISES TORRES CONDOR**

**PROMOCIÓN  
2001 – II**

**LIMA – PERÚ  
2007**

## **PROTOCOLO DNP3 Y SU APLICACIÓN EN SISTEMAS SCADA**

*Dedico este trabajo a:*  
*Mi Madre, inspiración plena de lucha y*  
*sacrificio,*  
*Mis Hermanos, por el apoyo incondicional en*  
*mi carrera,*  
*Y mis sobrinos esperanza de superación.*

## SUMARIO

El presente trabajo realiza un análisis de las características funcionales y estructura del protocolo DNP3 (Distribution Network Protocol) y su aplicación en sistemas SCADA, así mismo se realiza el análisis de otros protocolos de comunicaciones utilizados sistemas SCADA, para lo cual, se han considerando aspectos de arquitectura de capas, funcionalidad y performace.

Como resultado de análisis se determina que el DNP3 es el protocolo más confiable y avanzado en aplicaciones SCADA y flexible a diversos sistemas de comunicaciones.

En el capítulo I se ofrece una visión general de los sistemas SCADA y de los estándares, en ella se describe una reseña histórica de la evolución de los Sistemas SCADA, así como la definición de estándares para la interoperatividad entre sistemas.

El capítulo II se realiza el análisis de la arquitectura de los típicos sistemas SCADA, es decir una descripción general de la funcionalidad de los sub-sistemas de que lo conforman, y algunas especificaciones técnicas para la implementación.

El capítulo III trata de un sistema importante en la adquisición de datos que es el sistema de comunicaciones, para los cuales se describe los protocolos abiertos más importantes utilizados en la adquisición de datos y control.

El capítulo IV describe las características funcionales y se realiza un análisis de la arquitectura del protocolo DNP3, también se describe las recomendaciones y reglas que los fabricantes deben seguir para la implementación del DNP3.

El capítulo V se presenta la aplicación del DNP3 en un Sistema SCADA para el sistema de distribución de Agua potable en dos distritos de Lima, para lo cual se utiliza como plataforma de comunicaciones el sistema Celular GPRS.

## INDICE

<b>PROLOGO</b>	<b>1</b>
<b>CAPITULO I</b>	
<b>DESCRIPCIÓN GENERAL DE SISTEMAS SCADA</b>	<b>2</b>
<b>1.1 Introducción</b>	<b>2</b>
<b>1.2 Definición de Scada</b>	<b>2</b>
<b>1.3 Estándares Aplicables.</b>	<b>3</b>
<b>1.3.1 Desarrollo de Estándares DNP3.0 y IEC 60870</b>	<b>4</b>
<b>1.3.2 Introducción del Estándar IEC 60870-5</b>	<b>6</b>
<b>1.3.3 Estructura General del Estándar IEC 60870-5</b>	<b>6</b>
<b>CAPITULO II</b>	
<b>ANÁLISIS Y EVALUACIÓN DE LA ARQUITECTURA DE SISTEMAS SCADA</b>	<b>9</b>
<b>2.1 Descripción de Arquitectura Scada</b>	<b>9</b>
<b>2.2 Elementos de Sistemas Scada</b>	<b>10</b>
<b>2.2.1 Funciones y Arquitectura de la Estación Master MTU</b>	<b>11</b>
<b>2.2.2 Funciones y Arquitectura de la Estación Remota (Subestación)</b>	<b>12</b>
<b>2.3 Especificaciones y Recomendaciones Básicas para la Implementación de Sistemas Scada</b>	<b>15</b>
<b>2.3.1 Requerimientos de Seguridad</b>	<b>16</b>
<b>2.3.2 Selección de Protocolos</b>	<b>17</b>

## CAPITULO III

<b>ANÁLISIS DE SISTEMAS DE COMUNICACIONES PARA APLICACIONES SCADA</b>	<b>19</b>
<b>3.1 Descripción de la Filosofía de Comunicación</b>	<b>19</b>
<b>3.2 Arquitectura de Comunicaciones</b>	<b>20</b>
<b>3.2.1 Arquitectura Punto-Punto</b>	<b>20</b>
<b>3.2.2 Arquitectura Punto-Multipunto</b>	<b>21</b>
<b>3.2.3 Arquitectura Estación Relay (Repetidora)</b>	<b>21</b>
<b>3.3 Métodos de Comunicación</b>	<b>22</b>
<b>3.3.1 Polled (Master – Esclavos)</b>	<b>22</b>
<b>3.3.2 Contención (Peer to Peer)</b>	<b>23</b>
<b>3.4 Alcances Generales de los Protocolos mas Utilizados.</b>	<b>24</b>
<b>3.4.1 Protocolo Modbus</b>	<b>25</b>
<b>3.4.2 Protocolos DNP3 y IEC 60870-5</b>	<b>26</b>
<b>3.4.3 FieldBus</b>	<b>28</b>
<b>3.4.3.1 Protocolo Profibus</b>	<b>28</b>
<b>3.4.3.2 Modelo de Comunicación Profibus</b>	<b>29</b>
<b>3.5 Introducción a la Arquitectura UCA (Utility Communication Architecture)</b>	<b>31</b>
<b>3.5.1 Tecnología UCA</b>	<b>33</b>
<b>3.5.2 Interface de Aplicación</b>	<b>34</b>
<b>3.5.3 Modelo de Datos</b>	<b>34</b>

## CAPITULO IV

<b>DISTRIBUCIÓN NETWORK PROTOCOL DNP3.0</b>	<b>38</b>
<b>4.1 Introducción</b>	<b>38</b>
<b>4.2 Características del Protocolo DNP3</b>	<b>39</b>
<b>4.3 Beneficios del DNP3</b>	<b>39</b>

<b>4.4</b>	<b>Método de Comunicación</b>	<b>39</b>
<b>4.5</b>	<b>Análisis de la Arquitectura del DNP3</b>	<b>42</b>
<b>4.5.1</b>	<b>Capa física</b>	<b>44</b>
<b>4.5.2</b>	<b>Capa de enlace.</b>	<b>44</b>
<b>4.5.3</b>	<b>Capa de Transporte</b>	<b>48</b>
<b>4.5.4</b>	<b>Capa de aplicación</b>	<b>50</b>
<b>4.6</b>	<b>Niveles de Sub Sets</b>	<b>70</b>
<b>4.6.1</b>	<b>Definición de Subset Nivel 1</b>	<b>70</b>
<b>4.6.2</b>	<b>Definición de Sub-Set Nivel 2</b>	<b>71</b>
<b>4.6.3</b>	<b>Definición de Sub-Set Nivel 3</b>	<b>71</b>
<b>4.7</b>	<b>Recomendaciones y Reglas de Implementación</b>	<b>72</b>
<b>4.7.1</b>	<b>Eventos y clases de datos</b>	<b>72</b>
<b>4.7.2</b>	<b>Operación de Salidas Binarias</b>	<b>73</b>
<b>4.8</b>	<b>Pruebas de Conformidad</b>	<b>73</b>
<b>4.9</b>	<b>Sincronización de Tiempo</b>	<b>74</b>
<b>4.10</b>	<b>DNP3 sobre TCP/IP</b>	<b>75</b>
 <b>CAPITULO V</b>		
<b>COMUNICACIÓN DNP 3.0 A TRAVÉS DE UNA RED GPRS PARA UN SISTEMA DE DISTRIBUCION DE AGUA POTABLE</b>		<b>76</b>
<b>5.1</b>	<b>Introducción</b>	<b>76</b>
<b>5.2</b>	<b>Antecedentes</b>	<b>76</b>
<b>5.3</b>	<b>Descripción y Justificación del Sistema Implementado</b>	<b>79</b>
<b>5.4</b>	<b>Descripción del Sistema de Comunicación GPRS y Protocolo DNP 3</b>	<b>81</b>
<b>5.5</b>	<b>Arquitectura del Sistema de Comunicaciones</b>	<b>83</b>
<b>5.5.1</b>	<b>Resultados del Cálculo del Volumen de Datos por la Red GPRS.</b>	<b>86</b>
<b>5.6</b>	<b>Beneficios y Facilidades del Sistema</b>	<b>87</b>
<b>CONCLUSIONES</b>		<b>89</b>

**ANEXOS**

**90**

**BIBLIOGRAFÍA**

**115**

## PRÓLOGO

Una de los mayores de problemas que tienen las Empresas de Servicios públicos de Electricidad Agua Gas es la búsqueda de la eficacia en la supervisión y control de sus sistemas de Generación, transmisión, y distribución. En tal sentido, con la finalidad de ofrecer una buena calidad del servicio y reducir costos operativos, muchas empresas implementan sistemas potentes de adquisición de datos así como sistemas de comunicaciones para transportar la información desde Estaciones Remotas hacia un centro de operaciones. Sin embargo muchas de ellas probablemente no tengan un desempeño óptimo debido a las características de los equipos de adquisición de datos, arquitecturas de los protocolos de comunicaciones que utilizan para comunicarse con sus estaciones remotas u otras razones.

El presente trabajo realiza un análisis detallado de uno de los protocolos mas utilizados en diferentes ámbitos de la industria el DNP3; como resultado se demuestra características importantes que hacen que información sea confiable y detallada de los equipos. Además se describen las reglas y recomendaciones de los estándares para su implementación por fabricantes de dispositivos electrónicos y sistemas de adquisición de datos. También se realiza un análisis de otros protocolos de comunicaciones usados en la industria de la automatización y nuevas arquitecturas emergentes como el UCA.

Para la realización de este trabajo se han desarrollado cinco capítulos. En el Capítulo I se realiza una breve revisión de los sistemas SCADA y estándares aplicables. EL Capítulo II se realiza un análisis de la arquitectura típica de los sistemas SCADA y así como las especificaciones de acuerdo a los estándares aplicables para la implementación de estos sistemas. En el Capítulo III se realiza una descripción de los sistemas de comunicaciones y protocolos de los sistemas de automatización. El Capítulo IV se realiza el análisis del la arquitectura de capas del protocolo DNP3. El Capítulo V demuestra la flexibilidad del protocolo DNP para adaptarse en un sistema SCADA implementado sobre las nuevas tendencias en tecnología en comunicaciones, así como las ventajas ofrecidas frente a otros sistemas de comunicaciones tradicionales.

# **CAPITULO I**

## **DESCRIPCIÓN GENERAL DE SISTEMAS SCADA**

### **1.1 Introducción**

Los Primeros sistemas SCADA ofrecían funcionalidades muy básicas de monitoreo sin proporcionar funciones de aplicación, proporcionaban reportes periódicos de las señales de medida y/o condiciones de estado de dispositivos ubicados en las estaciones remotas. Los dispositivos electromecánicos y contadores numéricos fueron utilizados para el control y supervisión de la producción en plantas. Conforme la tecnología se desarrollaba, los ordenadores fueron encargándose de la recolección de datos, disponiendo comandos de control, proporcionaban funciones de presentación de la información en paneles basados en tecnología digital, y agregaron capacidades de programar el sistema para realizar funciones de control complejas.

Actualmente, la mayoría de sistemas SCADA instalados se han convirtiendo en parte integral de la estructura gerencial de la información corporativa. Estos Sistemas además de utilizarse como herramientas operacional sirven como recurso importante de información para los sistemas corporativos externos al centro de operaciones que dependen de información oportuna en la cual basan decisiones relacionadas con la producción y calidad de servicio.

Los fabricantes de Sistemas SCADA han reconocido esta tendencia, y están desarrollando métodos eficientes para disponer la información de manera segura sin afectar la operación del sistema SCADA.

### **1.2 Definición de Scada**

SCADA proviene de las siglas Control y Adquisición de Datos de Supervisión- (Supervisory Control and Data Acquisition). Estos sistemas permiten desde Estaciones Centrales realizar funciones de control y supervisión de procesos ampliamente distribuidos

a través de interfaces amigables presentadas en pantallas para la interacción entre el operador y el proceso de control.

Los sistemas SCADA mejoran la eficacia del proceso de monitoreo y control proporcionando información para toma de decisiones operacionales oportunas. Estos sistemas son aplicables en los siguientes sistemas.

- Estaciones de generación Hidroeléctrica que operan de acuerdo a la demanda de clientes generalmente ubicadas en localidades remotas.
- Producción de Gas o Petróleo, donde los sistemas de adquisición, equipos de medición y equipos de bombeo distribuidos a lo largo de extensas áreas. Estos sistemas requieren básicamente control de la operación de motores, regulación de válvulas y recopilación de información de medida.
- Estaciones de medición, regulación, equipos de bombeo, entre otras, ubicadas a lo largo de las redes de tuberías en los sistemas de distribución de Agua o Gas supervisadas y controladas desde un punto central de control.
- Sistemas de Transmisión de electricidad que cubren áreas muy extensas a lo largo de un territorio y que son controlados mediante la apertura y cierre de interruptores, y deben responder inmediatamente a cambios de carga en las líneas de transmisión.

### 1.3 Estándares Aplicables.

- **IEEE Recommended practice for Master/Remote Supervisory Control and Acquisition (SCADA) communications.** Se inicio en 1980s como un intento de estandarizar las comunicaciones Master/Remotas.
- **IEEE Standard Definition, Specification, and Analisis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.** Este Estándar se aplica a sistemas para monitoreo, conmutación, y control de equipos eléctricos en subestaciones atendidas y no atendidas, estaciones de generación, y utilización y conversión de potencia. Este estándar no aplica para equipos de protección automática en sistemas de potencia.

El ANEXO A incluye la definición de terminología utilizada en la norma.

Los protocolos propietarios de comunicación para sistemas SCADA son desarrollados por fabricantes conociendo la aplicación específica de una industria particular. Estos protocolos presentan múltiples desventajas para los usuarios por que están sujetos al

escalamiento o expansión usando el mismo sistema o están obligados a reemplazar partes sustanciales del sistema para cambiar protocolos de otro fabricante.

El aporte de los estándares en protocolos abiertos proporciona interoperatividad entre equipos de diferentes fabricantes. Esto significa que el usuario puede comprar los programas de telecontrol de un fabricante, y podrá utilizar dispositivos de otros fabricantes. Los estándares abiertos proporcionan beneficios inmediatos y futuros.

#### **a) Beneficios Inmediatos**

- Empleo un número mínimo de protocolos en campo.
- Costos reducidos en software
- No se requiere el uso convertidores de protocolos
- Cronograma corto de entrega
- Pocas pruebas, mantenimiento y entrenamiento
- Pueden entregarse pruebas de conformidad

#### **b) Beneficios Futuros**

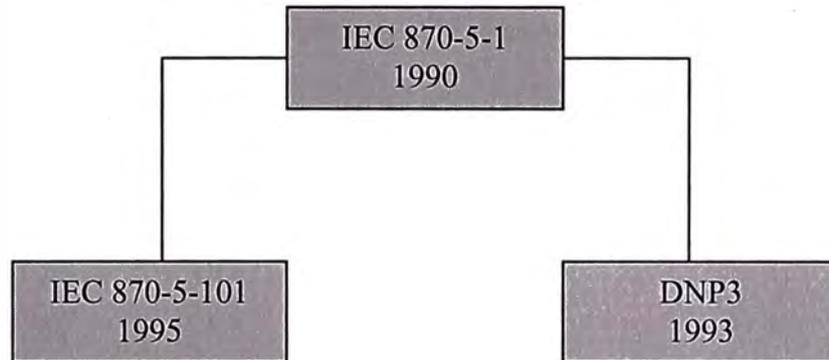
- Facilidades de expansión del sistema
- Extensa duración del producto
- Mejores productos de valor añadido de fabricantes
- Fácil Migración a nuevas tendencias tecnológicas

### **1.3.1 Desarrollo de Estándares DNP3.0 y IEC 60870**

El modelo EPA (Enhanced Performance Architecture) basado en tres capas de ISO propuesta por la IEC, fue adoptado como base para la transmisión de datos de telemetría en el estándar IEC 870 para equipos y sistemas de telecontrol. Las partes principales del estándar fueron desarrollados y publicados entre 1990 y 1993, de los cuales una de ellas fue el IEC 870-5 protocolos de transmisión Sección I, titulado: Formatos de Tramas de Transmisión. Este documento incluye la especificación de cuatro formatos de trama o estructura de mensajes (FT1.1, FT1.2, F2 y F3) que podrían ser adoptados para aplicaciones de telecontrol.

El estándar DNP3.0 fue desarrollado por Harris Controls utilizo el formato de trama F3 y el IEC870 específico en el estándar IEC870-5-101 Basic Control task el formato de trama FT1.2. Desde entonces, estos dos protocolos han sido desarrollados paralelamente por diferentes fabricantes de sistemas y dispositivos de telecontrol, teniendo como un punto de

partida la documentación IEC870-5. Actualmente, los protocolos DNP3.0 y IEC870-5-101 proporcionan interoperatividad entre sistemas para aplicaciones de telecontrol y compiten en el mercado mundial. El DNP3.0 tiene fuerte aceptación en Norte América, Suda América, Australia y Asia. Mientras el IEC870-5-101 tiene aceptación en la región Europea.



**Fig. 1.1 Desarrollo de Estándares**

### **1.3.2 Introducción del Estándar IEC 60870-5**

El IEC 60870-5 constituye un conjunto de estándares producidos por la Internacional Electromecánica comisión IEC, para proporcionar un estándar abierto para la transmisión de información de control y telemetría SCADA.

El Estándar proporciona una detallada descripción funcional para equipos de telecontrol y sistemas para controlar procesos geográficamente dispersos. El estándar tiene objetos de datos que son especialmente desarrollados para tales aplicaciones en la industria eléctrica, sin embargo, no esta limitada por que también incluye objetos de datos aplicables en aplicaciones SCADA para otras industrias.

El conjunto de estándares IEC 60870-5 fue inicialmente completada en 1995 con la publicación del perfil IEC 60870-5-101, el cual cubre la transmisión sobre circuitos de comunicación seriales de banda relativamente angosta. Con el avance de la tecnología de comunicaciones sobre redes de datos, el IED 60870-5 ahora también proporciona para comunicaciones usando protocolo TCP/IP. Esta misma secuencia de desarrollo también ha ocurrido con el protocolo DNP3.

### **1.3.3 Estructura General del Estándar IEC 60870-5**

Las **TABLAS N° 1.1, 1.2 y 1.3** presentan la estructura general del estándar IEC 60870 con las publicaciones y partes confortantes.

Las secciones IEC 60870-5-1 al IEC 60870-5-5 son los documentos de especificación Part 5-Parte de Protocolos de transmisión del estándar. Los protocolos IEC 60870-5-101 al IEC 60870-5-104 proporcionan las definiciones de los objetos de datos del nivel de aplicación y funciones para completamente definir la funcionalidad del protocolo. Estos también son denominados como perfiles.

El IEC 60870-5-101 define todas las funciones del nivel de aplicación y objetos de datos para aplicaciones de telecontrol que cubren áreas geográficas amplias, usando comunicaciones seriales de banda angosta. En general cubre las comunicaciones con dispositivos de telecontrol, incluyendo tipos de datos y servicios en sistemas de subestaciones eléctricas.

Los estándares IEC 60870-5-102 y IEC 60870-5-103 proporcionan tipos de datos y funciones para sistemas de protección eléctrica. Esto incluye protección de distancia, protección diferencial de línea y protección diferencial de transformador.

El IEC 60870-5-104 tiene una significación especial, por que define la operación del protocolo de transmisión sobre redes usando perfiles de transporte estándar especificando los protocolos TCP/IP. Este estándar realmente no es independiente del IEC 60870-5-101, porque reemplaza la sección de transporte de mensaje con una versión de red, dejando las funciones del nivel de aplicación inalterable.

**TABLA N° 1.1 Partes Principales Estándar IEC 60870**

Referencia	Descripción	Año
IEC 60870-1	Consideraciones Generales	1988
IEC 60870-2	Condiciones de Operatividad	1995
IEC 60870-4	Características eléctricas de Interfaces	1989
IEC 60870-5	Protocolos de Transmisión	1990
IEC 60870-6	Compatibilidad de protocolos de Telecontrol con las recomendaciones ISO y ITU-T	1995

**TABLA N° 1.2 Secciones del IEC 60870-5**

Referencia	Descripción	Año
IEC 60870-5-1	Formatos de Tramas de Transmisión	1990
IEC 60870-5-2	Procedimientos de transmisión	1992
IEC 60870-5-4	Estructura General del datos de aplicación	1993
IEC 60870-5-5	Funciones básicas del nivel de aplicación	1995

**TABLA N° 1.3 Estándares IEC 60870-5**

Referencia	Descripción	Año
IEC 60870-5-1	Estándar para tareas de telecontrol básicas	1995
IEC 60870-5-2	Estándar para transmisión de integridad total	1996
IEC 60870-5-4	Estándar para comunicaciones de Protección	1997
IEC 60870-5-5	Acceso a redes usando perfiles de transporte estándar	2000

## **CAPITULO II**

### **ANÁLISIS Y EVALUACIÓN DE LA ARQUITECTURA DE SISTEMAS SCADA**

#### **2.1 Descripción de Arquitectura Scada**

La arquitectura de los sistemas industriales de mediciones y control consisten básicamente de una computadora principal algunas veces llamada Estación Principal, Master Terminal Unit (MTU); una o varias estaciones remotas en donde las unidades de control obtienen datos de campo típicamente denominadas Remote Terminal Units, (RTU); y una colección de software estándar para monitorear y controlar remotamente dispositivos de campo. Estos Sistemas están presentes en las Industrias manufactureras, plantas de tratamiento, entre otras, y son comúnmente denominados Sistemas de Control Distribuidos (DCS) y están conformadas por unidades de recolección de datos de campo y control localizados dentro de un área confinada. Las comunicaciones pueden ser vía una red de área local (LAN) basados en medios ópticos o cobre, confiable y de alta velocidad por lo que típicamente están conformadas por lazos cerrados de control.

Los sistemas SCADA generalmente cubren áreas geográficas más extensas, y dependen de una variedad de sistemas de comunicación menos confiables que una red LAN, por lo que, el control a lazo cerrado es menos deseable. Estos sistemas exhiben predominantemente características de control a lazo abierto y utilizan comunicaciones interurbanas, aunque algunos elementos de control a lazo cerrado y/o de comunicaciones de corta distancia pueden también estar presentes en la arquitectura.

Las estaciones remotas típicamente están conformadas por dispositivos de campo (válvulas, bombas, medidores) conectados a una RTU o PLC (controlador Lógico Programable) que recopilan y ejecutan lógica de control. Al mismo tiempo, cada PLC o RTU puede enviar órdenes a los dispositivos de campo (abrir/cerrar una válvula, arrancar/parar una bomba, enviar consignas). Para la adquisición los datos y el envío órdenes a campo desde un sistema SCADA es necesario contar con una infraestructura de

comunicaciones que permita establecer enlaces de comunicación entre el SCADA y las RTUs o PLCs asociados a los dispositivos de campo en la Estación Remota.

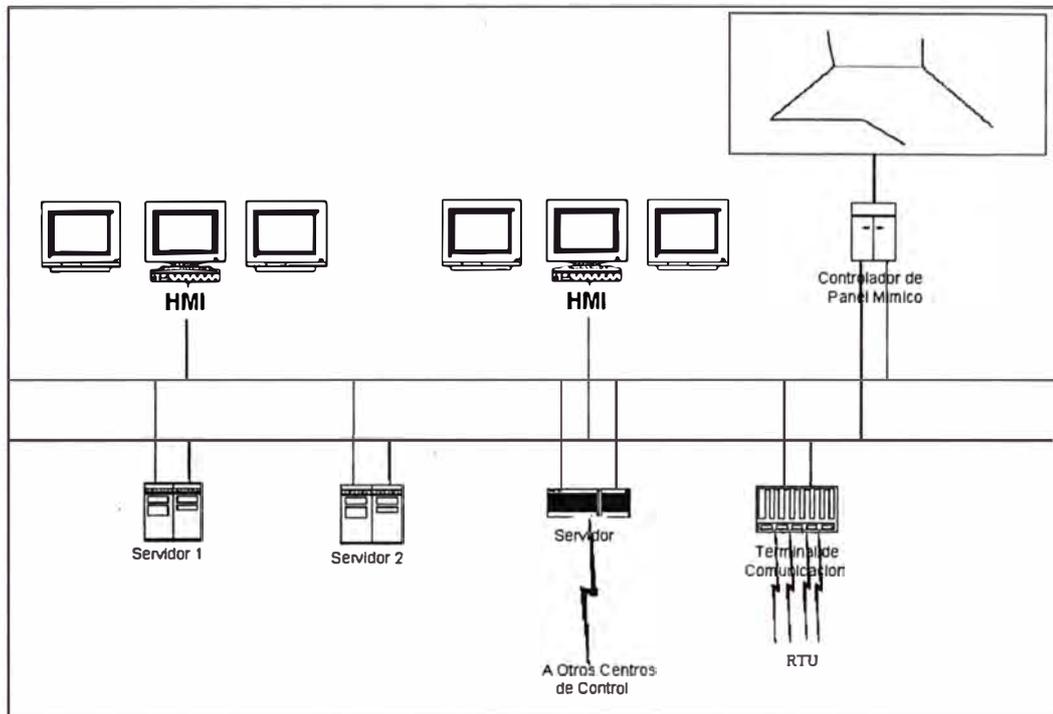
## **2.2 Elementos de Sistemas Scada**

Las modernas Estaciones principales SCADA tienen arquitectura distribuida en hardware y software. El procesamiento es distribuido en varias estaciones y ordenadores que se comunican entre sí a través de una red LAN redundante en el Centro de Control, y pueden utilizar características de arquitectura abierta para la interoperatividad con sistemas de otros fabricantes.

Para alcanzar un nivel aceptable de tolerancia de fallas con estos sistemas, es común tener ordenadores SCADA redundantes operando en paralelo en el centro de control. Esta arquitectura proporciona la transferencia automática de la responsabilidad de cualquier ordenador que pueda llegar a ser inasequible por cualquier razón, sin interrupción significativa de las operaciones.

Para asegurar la interoperatividad, los sistemas deberían cumplir con estándares internacionales, tales como POXIS o IEC60870-6 o estándares de-facto para la industria y productos relacionados para aplicaciones computacionales, IEC-60870 (TASE.2) para comunicaciones entre centros de control, y DNP3.0 / IEC60870-5-101 para comunicaciones con unidades terminales Remotas RTU. Sin embargo, a pesar de que los fabricantes ofrecen sistemas abiertos también desarrollan sus propias APIs (Aplicación Programming Interface). Las APIs habilitan módulos de software para comunicarse entre sí mediante el uso de objetos y mecanismos de intercambio de información.

### 2.2.1 Funciones y Arquitectura de la Estación Master MTU



**Fig. 2.1 Arquitectura de Configuración de Estación Master**

**a) Adquisición de datos.** Recolección y almacenamiento de datos de los RTU's o PLCs. Los datos (analógicas, estados y contadores) son agrupados dentro de tablas o en grupos funcionales y permiten que se pueda distribuir el control entre distintos operadores, y cada operador con sus áreas de control asignadas.

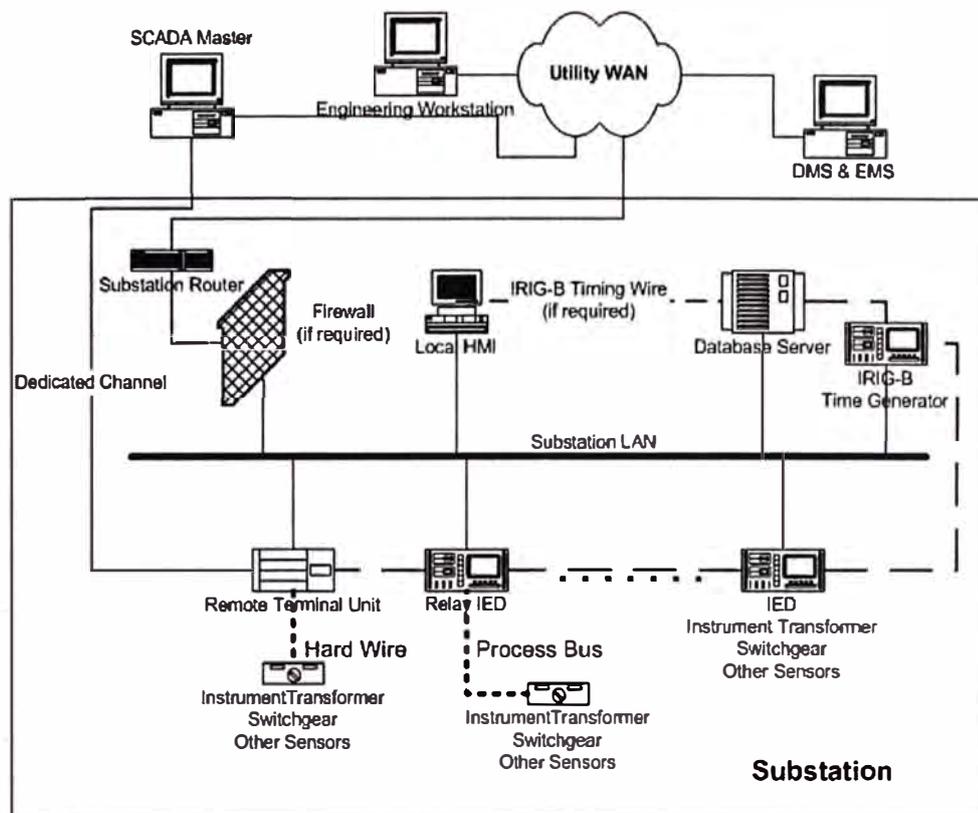
**b) Sistema Redundante.** Disposición de servidores redundantes en tiempo real y servidor de históricos HIS, de forma que si alguno de los servidores falla, el servidor redundante toma el control y la operación podrá seguir realizándose con normalidad. Los servicios conmutan automáticamente en caso de pérdida de conexión con un servidor.

Por ejemplo, los sistemas SCADA pueden constar de dos centros de control: el Primario (MCC) y el de Contingencias o Secundario (CCC). En condiciones normales el Primario tiene la responsabilidad de la adquisición de datos y telecontrol. El Centro de Contingencias puede tomar el control si existieran problemas en el Centro Primario que impidieran la operación del sistema. Además, puede existir un tercer centro, el Centro de Soporte o Ayuda para simulaciones y entrenamientos.

- c) **Trending.** Guardar los datos recopilados en una base de datos, y ponerlos a disposición de los operadores en forma de gráficos.
- d) **Procesamiento de Alarmas.** Recopilar datos de las RTU's para analizar si han ocurrido condiciones anormales, y alertar a personal de operaciones.
- e) **Control.** Control a Lazo Cerrado iniciados por operador.
- f) **Reportes.** Los sistemas SCADA tienen un módulo software dedicado a la producción de reportes.
- g) **Interfaces con otros Sistemas.** Transferencia de datos hacia y desde otros sistemas corporativos.
- h) **Seguridad.** Control de acceso a los distintos componentes del sistema.
- i) **Administración de la red.** Monitoreo de la red de comunicaciones.
- j) **Administración de la Base de datos.** Adición de nuevas estaciones, variables, gráficos, puntos de cambio de alarmas, y en general, reconfigurar el sistema.
- l) **Aplicaciones especiales.** Software de aplicación especial, asociado al monitoreo y al control de la planta.
- m) **Sistemas expertos, sistemas de modelado.** Los más avanzados pueden incluir sistemas expertos incorporados, o capacidad de modelado de datos.

### **2.2.2 Funciones y Arquitectura de la Estación Remota (Subestación)**

Unidades Terminales Remotas (RTUs o PLCs) encargados de la recolección de datos de campo y transmitir datos a la Estación Master MTU vía un sistema de comunicaciones. Estas Unidades proporcionan interfaces para los sensores de campo y Dispositivos Electrónicos Inteligentes (IEDs) situados en la Estación Remota.



**Fig 2.2 Arquitectura de Sistema de Automatización de Subestación**

La figura 2.2 muestra dos métodos de adquisición de datos y control, uno a través de IEDs conectados al sistema de potencia de subestación, la otra es a través de conexiones directas a la RTU de la Subestación.

Ejemplo: Las funciones ejecutadas por el sistema de automatización de una subestación eléctrica incluye protección, control y adquisición de datos, mantenimiento de base de datos, interfaz hombre maquina (HMI), acceso a base de datos y controles

### 2.2.2.1 Unidades Terminales Remotas RTU

La RTU es una unidad de adquisición de datos basado en microprocesadores y que tienen facilidad para la configuración y control de programas dinámicamente configurables desde la Estación Central. La función principal de estas unidades es controlar y recopilar datos desde equipos de procesamiento de la estación remota y transmitir hacia la Estación Master MTU. Para la función de adquisición de datos, las RTUs exploran las entradas de información de campo conectadas a sus interfaces (pueden también ser usados PLC's).

El hardware típico de una RTU: 01 procesador central CPU y memoria asociada, entradas analógicas, salidas analógicas, entradas para contadores, salidas digitales, interfaces de comunicación, fuente de alimentación. El CPU es un microprocesador basado en 16 o 32 bits y capacidad de memoria total de 256kBytes expandible a 4Mbytes divididos en tres tipos denominados EPROM, RAM, y Flash /EEPROM

Incluyen típicamente puertos de comunicación (RS232/RS485/RS422), interface de diagnostico, comunicación Ethernet para una estación central, un reloj en tiempo real para exactitud del estampado de tiempo de los eventos, y un temporizador Watchdog que verifica que el programa de la RTU este ejecutándose regularmente.

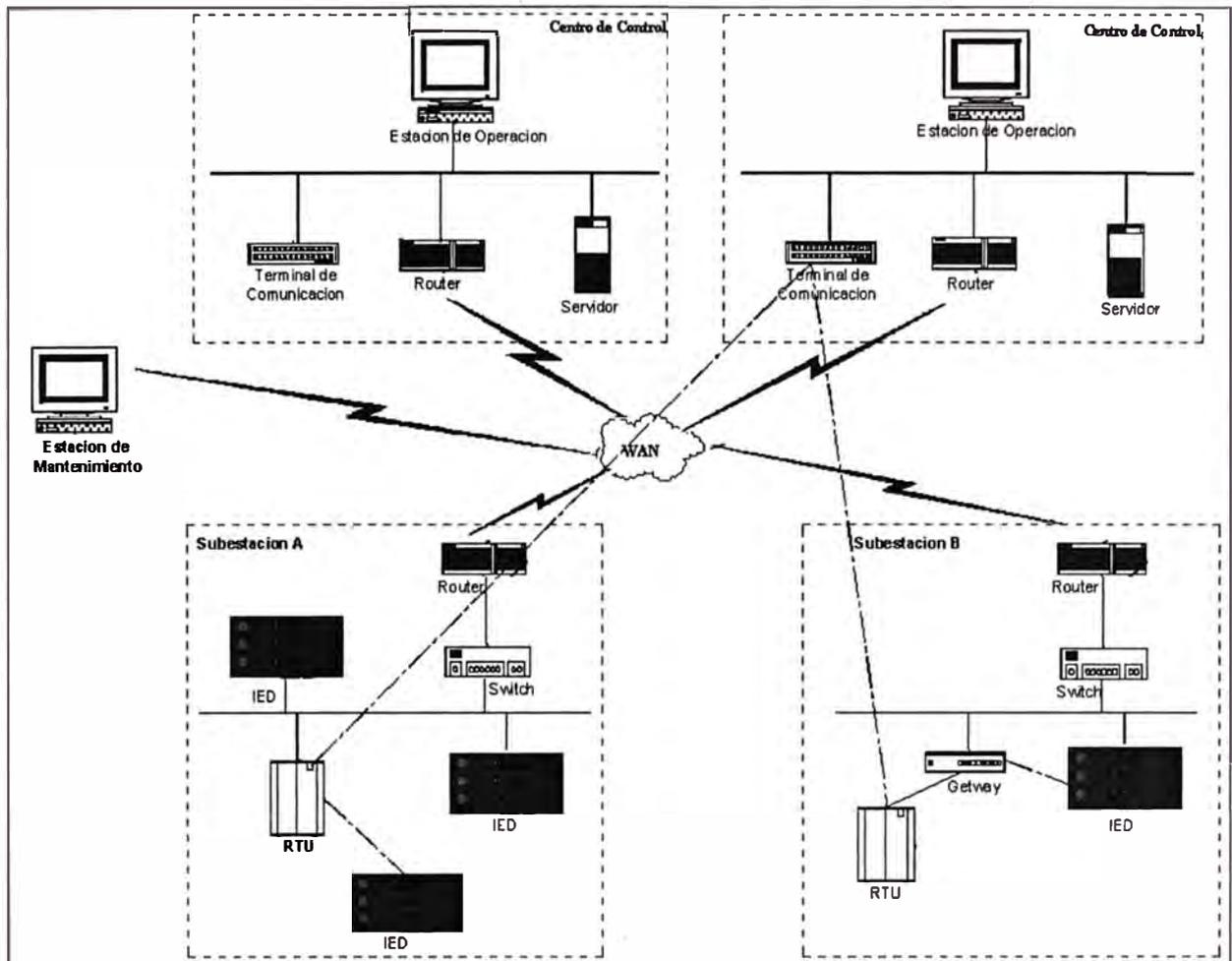
Los datos pueden ser de tres tipos principales:

- a) Datos analógicos (por ejemplo números reales) que quizás sean presentados en gráficos.
- b) Datos digitales (on/off) que pueden tener alarmas asociadas a un estado o al otro.
- c) Datos de pulsos (por ejemplo conteo de revoluciones de un medidor) que serán normalmente contabilizados o acumulados.

Las RTUs modernas son flexibles en el manejo de distintos medios de comunicación:

- RS232/RS422/RS485
- Ethernet
- Líneas telefónicas Dial Up / dedicadas
- Microondas/Mux
- Satélite
- Protocolo X.25
- Radio VHF/UHF

La fig.2.3 muestra un esquema típico de un sistema SCADA incluyendo los subsistemas que lo conforman.



**Fig. 2.3 Arquitectura Sistema SCADA**

### **2.3 Especificaciones y Recomendaciones Básicas para la Implementación de Sistemas Scada**

La definición de las especificaciones para el un sistema SCADA debe estar basado sobre la infraestructura existente o planificada. La definición de requerimientos están basado en satisfacer las necesidades actuales y futuras de los usuarios con desarrollos necesarios para actualizaciones cuando sean necesarios.

Después de la definición de requerimientos funcionales, las decisiones deben estar enfocadas en los protocolos de comunicación (externos e internos), IEDs, seguridad, disponibilidad y arquitectura. La selección de componentes y arquitecturas esta generalmente conformado por el equipamiento pre-existentes, selección de IEDs, selección de equipos, estándares, así como un análisis de costos beneficio.

Ejemplo: Para la automatización de subestaciones eléctricas se deben proporcionar especificar lo siguientes requisitos:

- Mediciones
- Monitoreo de Estados
- Control
- Protección
- Servicios Auxiliares
- Sincronización de tiempo
- Funciones de lógica programable

Después de la definición de requerimientos funcionales, se deberá evaluar el sistema para definir los requerimientos de rendimiento.

Las Tablas del **ANEXO C** pueden ser utilizadas para la evaluación básica de los aspectos de rendimiento del sistema para una red de transmisión de energía (los requerimientos para sistemas de servicios de distribución y generación son ligeramente diferentes). Las tablas incluyen las funciones previamente listadas, las cuales, no todas las funciones requieren el mismo conjunto de datos. El diseñador puede encontrar importante para definir puntos de medida, estados y control que tienen diferentes requerimientos de rendimiento.

Las tablas del **ANEXO C** incluyen los siguientes requerimientos de rendimiento:

- Periodicidad de actualización
- Exactitud
- Disponibilidad
- Latencia
- Resolución
- Desviación de tiempo (Time Skew)

### **2.3.1 Requerimientos de Seguridad**

La política corporativa debería establecer una seguridad electrónica perimetral alrededor del sistema. Esta política debería basarse en alguna combinación de procedimientos y tecnología.

La aplicación de requerimientos de seguridad debe considerar lo siguiente:

- Estándares y regulación industrial
- Seguridad corporativa y políticas de personal.

Con estos requerimientos las especificaciones de seguridad necesitaran equilibrarse con operaciones y deben proporcionar otros mecanismos tales como:

- Herramientas de mantenimiento y diagnostico
- Archivos y software de configuración
- Documentos y manuales técnicos
- Contraseñas y procedimientos del control de acceso
- Mantenimiento y políticas de acceso a IEDs

La seguridad física incluye acceso físico a la red del sistema de automatización y equipamiento. La seguridad electrónica puede incluir técnicas de encriptación, detección de intrusos en la red, autenticación, Firewalls y detección de acceso a IEDs.

### **2.3.2 Selección de Protocolos**

Es importante reconocer que algún específico IED puede entender solo un protocolo. Si un protocolo estándar esta siendo usado en una subestación se debe seleccionar un IED con el mismo protocolo para conexión a la red o canal de comunicaciones. Si un protocolo propietario esta instalado en la subestación y nuevos IEDs está adicionándose, entonces las opciones son.

- Actualización de RTUs, IEDs y Master existentes con protocolos estándares
- Uso de protocolos diferentes pero con convertidores de protocolos de modo que los datos puedan ser transferidos a través de un canal común

## **CAPITULO III**

### **ANÁLISIS DE SISTEMAS DE COMUNICACIONES PARA APLICACIONES SCADA**

#### **3.1 Descripción de la Filosofía de Comunicación**

La RTU recopila datos y procesa datos de los dispositivos conectados, y responde a la petición de la MTU. Las comunicaciones son controladas por la MTU, este registra los datos con la hora de recepción distinta a la hora que fueron generados.

La MTU solicita algunos datos de la RTU en cada encuesta principal, y extrae todos los datos en una segunda encuesta realizada a una frecuencia menor. La RTU explora sus entradas de información en forma continua, y los agrupa para el envío a la MTU.

La MTU realiza una encuesta continua a la RTU si tiene información para reportar; si nada hubiera cambiado desde la última encuesta, la RTU responderá sin novedad, y la MTU pasara a encuestar a la siguiente RTU. Para asegurarse de que un cierto acontecimiento en la RTU no fue reportado, ocasionalmente la MTU realiza una encuesta completa.

El informe por excepción reduce drásticamente el tráfico de comunicaciones, siempre y en cuando los datos estén cambiando relativamente lenta. Sin embargo, cuando se miden parámetros altamente volátiles puede aumentar drásticamente el tráfico. En este caso una solución es poner estos parámetros volátiles en una encuesta rutinaria, sacrificando una cierta exactitud en la hora de registro.

El acercamiento mas sofisticado es configurar la RTU en modo reporte por excepción sin la encuesta de la MTU. Esto significa que el sistema de comunicaciones no será utilizado para las repetidas encuestas. Sin embargo bajo este modo de reporte, la MTU también realiza una encuesta general, de otro modo una RTU podría salir de servicio y el sistema nunca se daría por enterado.

Para utilizar esta técnica, el protocolo de comunicación debe tener la capacidad de proporcionar las direcciones de destino del mensaje, y de la fuente.

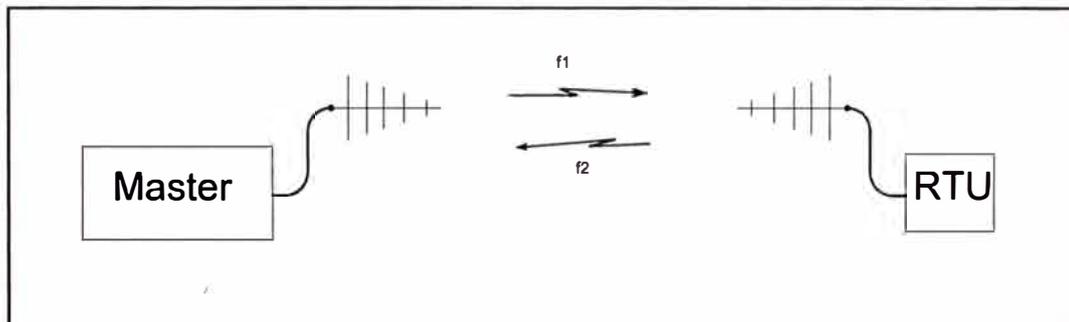
Esta técnica también implica que dos RTUs pueden transmitir simultáneamente, interfiriendo uno con otro, luego ambos tienen el mismo tiempo de reenvío otra vez interferirán. En este caso lo típico es repetir el envío después de un tiempo aleatoriamente seleccionado.

### 3.2 Arquitectura de Comunicaciones

Los sistemas SCADA se basan principalmente en tres arquitecturas de comunicación, las cuales pueden ser combinadas en un mismo sistema.

#### 3.2.1 Arquitectura Punto-Punto

Esta es la configuración más simple donde se intercambia información entre dos estaciones, una configurada como master y la otra como esclava. Es posible la comunicación para ambas estaciones en el modo Full Duplex (transmisión y recepción en dos separadas frecuencias) o Half Duplex con solo una frecuencia. La Fig. 3.1 muestra un esquema básico de la arquitectura punto-punto.

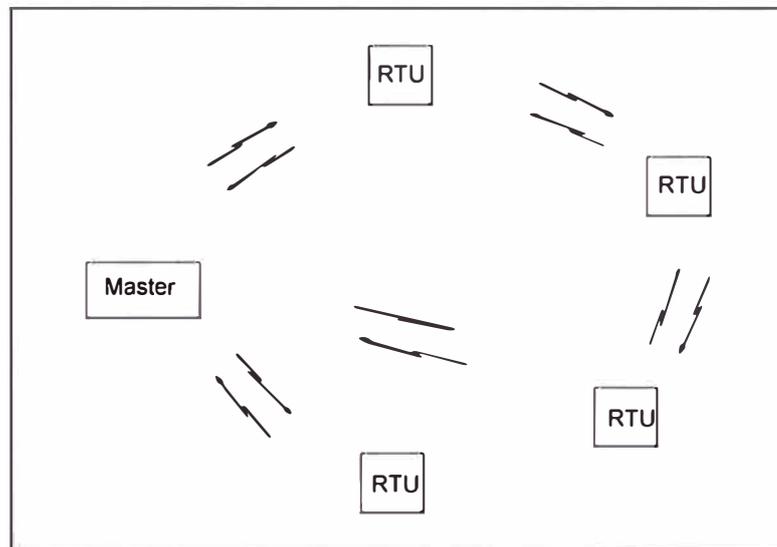


**Fig.3.1 Arquitectura Punto-Punto**

### 3.2.2 Arquitectura Punto-Multipunto

En esta configuración existe una estación master y varias esclavas. Normalmente la información es transferida entre la estación master y cada una de las estaciones esclavas. Si dos estaciones esclavas necesitan transferir datos entre ellos lo deberían realizarlo a través de la estación master que actuara como moderador. Tal como se muestra en el esquema de la Fig. 3.2.

Alternativamente, es posible para todas las estaciones actuar en una relación peer to peer, requiriendo para ello protocolos mas sofisticados para manejar las colisiones de datos cuando dos o mas estaciones transmiten datos al mismo tiempo.

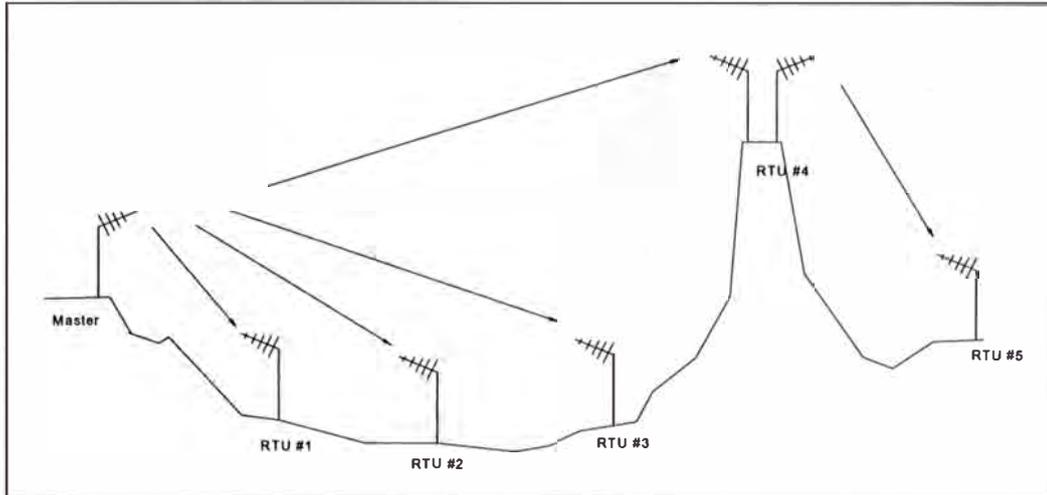


**Fig. 3.2** Arquitectura Punto - Multipunto

### 3.2.3 Arquitectura Estación Relay (Repetidora)

Esta arquitectura presenta dos posibilidades, las estaciones denominadas concentradoras y retransmisoras (store and forward) o las estaciones repetidoras.

- La estación llamada Relay concentradora y repetidora actúan como retransmisor de mensajes a otra estación que esta fuera del rango de la estación master. En estas estaciones no hay transmisión simultánea de mensajes, porque primero recibe y concentra la información, y luego retransmite hacia la estación master. La Fig.3.3 muestra la Arquitectura Relay.
- Las estaciones repetidoras son preferidas generalmente para incrementar el rango del sistema de radio



**Fig. 3.3 Arquitectura Relay (Repetidora)**

### 3.3 FILOSOFIAS DE COMUNICACIONES

#### 3.3.1 Polled (Master – Esclavos)

Esto puede ser usado en una configuración Punto-Punto o Punto-Multipunto y probablemente sea la filosofía de comunicación más simple, donde la estación master tiene el control total de las comunicaciones y ejecuta encuestas regulares a cada una de las estaciones esclavas. Las estaciones esclavas no tienen la iniciativa de iniciar transacciones, y esencialmente responden a la consulta de la estación master. Si los esclavos no responden en un tiempo definido, la master reintenta un número de veces y luego lo etiqueta al esclavo indicando que se encuentra fuera de servicio antes de intentar al siguiente nodo en la secuencia de encuesta.

Las ventajas de esta filosofía son:

- El software es simple y confiable por la simplicidad de la filosofía.
- La falla del enlace entre la estación master y un nodo esclavo es rápidamente detectado.
- No ocurren colisiones en la red

Las Desventajas de esta filosofía son.

- Los requerimientos de variación en la transferencia de datos de cada esclavo no puede ser manejada.
- Requerimientos tipo interrupción de un esclavo solicitando urgente acción no puede ser ejecutadas

- En sistemas altamente recargadas de información y con mínimos cambios en los esclavos son muy ineficientes e innecesariamente lentos.
- La necesidad de comunicación entre esclavos es necesariamente a través de la master implicando complejidad adicional en el diseño de la estación master.

### **3.3.2 Contención (Peer to Peer)**

Es un método basado en la detección de portadora con múltiple detección de acceso/ donde no hay control de la estación master y las estaciones esclavas tienen la libertad de acceder al medio.

#### **a) Comunicación RTU-RTU**

En un escenario donde una RTU quiere comunicarse con otra RTU. Una técnica usada es la respuesta a una encuesta (poll) por la estación maestra con un mensaje con la dirección destino correspondiente a la RTU destino.

La estación master examina el campo de dirección destino del mensaje recibido desde la RTU, y si no observa su propia dirección, retransmitirá hacia la RTU apropiada.

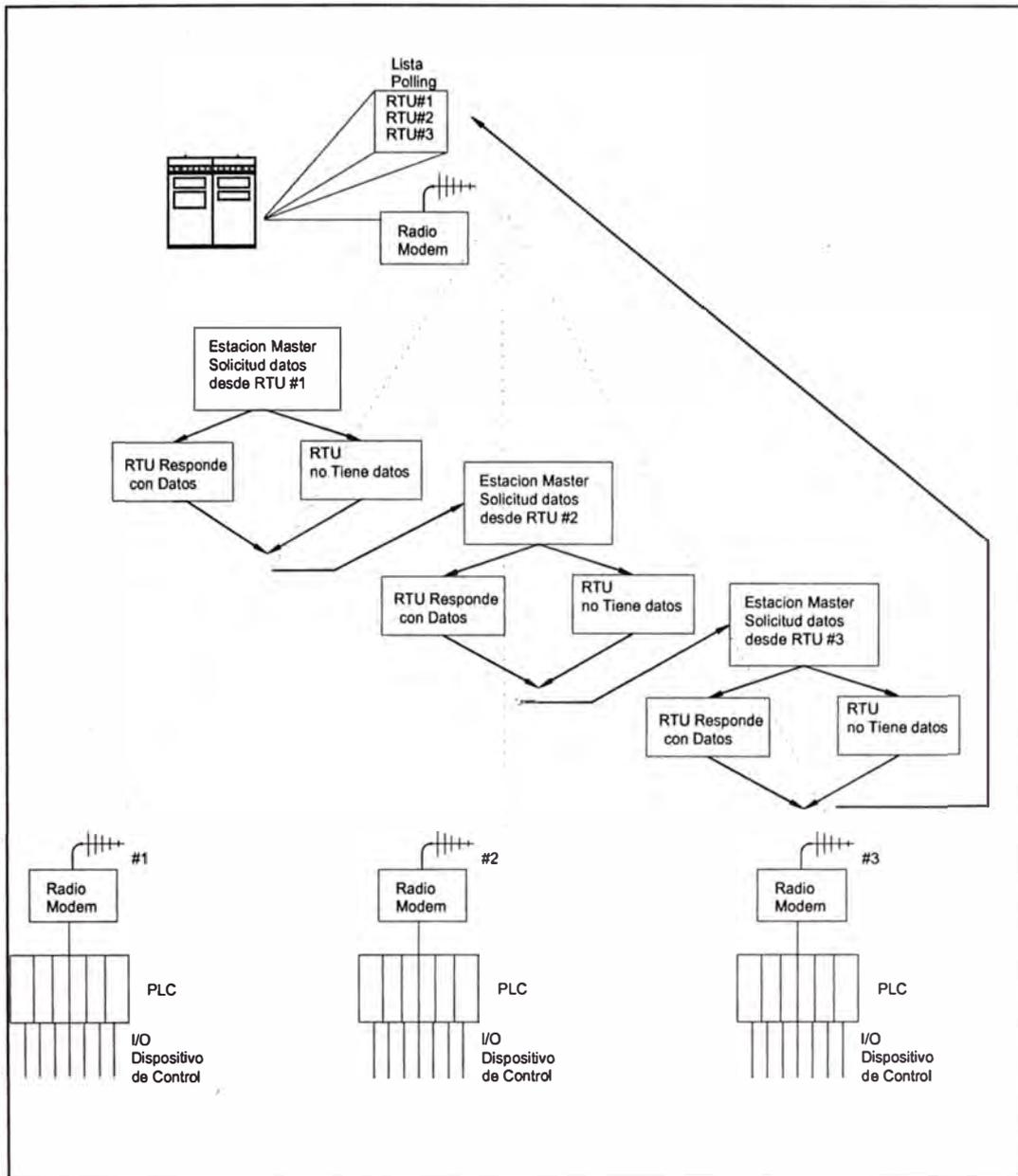
Este enfoque puede ser utilizado en una red master esclavos, o un grupo de estaciones todas con el mismo estatus.

#### **b) Reporte por excepción**

Una técnica para mejorar la innecesaria transferencia de datos es usar alguna forma de reporte por excepción

Las estaciones remotas monitorean sus propias entradas para un cambio de estado o dato. Solo si ocurre un cambio de estado, la estación remota escribirá un bloque de datos a la estación master.

La Fig. 3.4 representa la filosofía de comunicación del modo de reporte por excepción.



**Fig. 3.4 Comunicación en Modo Reporte Espontáneo**

### 3.4 Alcances Generales de los Protocolos mas Utilizados.

Los sistemas de comunicaciones para los sistemas SCADA se han desarrollado para tener alta confiabilidad y para manejar canales de comunicaciones de muy poca fiabilidad. Esto es importante donde esta implicado el control, ya que podría ser desastroso si las fallas de comunicaciones causaran que el sistema SCADA haga funcionar inadvertidamente el proceso.

La operación normal para un sistema SCADA es esperar siempre que cada transmisión sea reconocida. El método de encuesta que emplea tiene seguridad incorporada, en la que cada

estación remota esta controlada y debe periódicamente responder. Si no responde un número predeterminado de recomprobaciones será etiquetada como fuera de servicio.

La exactitud de la transmisión de un SCADA se ha observado tradicionalmente como tan importante que la aplicación SCADA toma directamente la responsabilidad sobre ella. Esto se produce en contraste con protocolos de comunicación más generales donde la responsabilidad de transmitir datos confiablemente se dejan a los mismos protocolos. Se han desarrollado técnicas para transmisión de datos confiablemente sobre medios de baja fiabilidad, y es así que muchas compañías alcanzaron una ventaja competitiva respecto de sus competidoras simplemente debido al merito técnico de sus protocolos.

### 3.4.1 Protocolo Modbus

El protocolo modbus se ha convertido en un standard 'de facto' muy empleado en sistemas de captación de datos en entornos de comunicaciones master-slave. y que en general emplea transacciones pregunta-respuesta (aunque existen transacciones broadcast, pregunta sin respuesta)

Las principales características incluye:

- Formato de trama, secuencia de trama, manejo de errores de comunicación, y ejecución de funciones.
- La información de los mensajes contiene la dirección del receptor, datos necesarios para ejecutar la acción y medios de verificación de errores.
- La unidad esclava recibe el mensaje, y si no existen errores, ejecutara la operación y enviara una respuesta a la maestra.
- La información en el mensaje de respuesta es la dirección del esclavo, la acción ejecutada, el resultado de la acción y un medio de verificación de errores.
- Los datos pueden ser intercambiados en dos modos de transmisión:
  - ASCII-Usado para pruebas
  - RTU-Compacto y rápido, usado para operación normal

La Fig. 3.5 Muestra el formato de Trama del protocolo Modbus

Dirección	Función	Datos	Check Errores
1 Byte	1 Byte	Variable	2 Bytes

Fig 3.5 Formato de Trama Modbus

Ejemplo: Los códigos de función de Modbus desarrollado por Modicon:

- 01 (H01), Lectura de n salidas digitales
- 02 (H02), Lectura de n entradas digitales
- 03 (H03), Lectura de n registros de salidas
- 04 (H04), Lectura de n registros de entradas
- 05 (H05), Escritura de 1 salida digital
- 06 (H06), Escritura de 1 registro de salida
- 07 (H07), Lectura de estados de excepción
- 11 (H0B), Lectura contador de eventos de comunicaciones
- 12 (H0C), Lectura diario de eventos de comunicaciones
- 15 (H0F), Escritura de n salidas digitales
- 16 (H10), Escritura de n registros de salida
- 17 (H11), Reporta ID esclavo

### 3.4.2 Protocolos DNP3 y IEC 60870-5

La estructura del modelo EPA es apropiada para sistemas que operan sobre una red simple. Una capa de nivel superior identificado como capa de usuario es normalmente es incluida en el modelo básico EPA para representar las diversas funciones o procesos que deben ser definidos para proporcionar operaciones en sistemas de telecontrol. Para el caso de la versión IEC 60870-5-104 o perfil T104, es completamente diferente que la versión IEC 60870-5-101 por que incluye capas adicionales por debajo de la capa de aplicación para proporcionar transporte de mensajes sobre redes utilizando protocolo estándares. Estos son las capas de red y transporte equivalente al uso de los protocolos TCP/IP. La Fig. 3.6 presenta la arquitectura las arquitecturas para T104 y T101

Capa	Usuario	=	Usuario
7	Aplicación	=	Aplicación
6			Presentación
5			Sesión
4			Transporte
3			Red
2	Enlace	=	Enlace
1	Física	=	Física

IEC 60870-5-101 IEC 60870-5-104

**Fig 3.6 Arquitectura T101 y T104**

La TABLA N° 3.1 presenta las diferentes secciones del estándar IEC 60870-5 correspondientes con el modelo de capas. Asimismo, en la TABLA N° 3.2 se presenta como las capas de niveles inferiores del IEC 60870-5-101 han sido completamente reemplazados por los perfiles de transporte y red del protocolo TCP/IP.

**TABLA N° 3.1**

Capa	Fuente	Selección
Procesos de Usuario	IEC 60870-5-5	Funciones de aplicación
Aplicación	IEC 60870-5-4	Elementos de información de aplicación
	IEC 60870-5-3	ASDUs
Enlace	IEC 60870-5-2	Funciones básicas del nivel de aplicación
	IEC 60870-5-1	Formato de tramas
Física	ITU-T	Especificación de Interface

TABLA N° 3.2

Capa	Fuente	Selección
Procesos de Usuario	IEC 60870-5-101	Funciones de aplicación
Aplicación	IEC 60870-5-101	ASDUs y Elementos de información de aplicación
Transporte	Protocolos de Red y Transporte TCP/IP	
Red		
Enlace		
Física		

### 3.4.3 FieldBus

Diseñado para plantas industriales, permite conectar diversos dispositivos (sensores, actuadores y autómatas programables) en extensas distancias locales utilizando medio de comunicación compartido (buses de campo). Los buses pueden ser propietarios y abiertos, este ultimo permite la conexión de dispositivos de distintos fabricantes, siendo uno de los buses de mayor aceptación el estándar Profibus definido por la German DIN19245 part 1 y 2 basado en un mecanismo híbrido de control de acceso al bus de campo utilizando un procedimiento de paso de testigo para la comunicación entre nodos activos (maestros), y un procedimiento de comunicación maestro-esclavo entre los nodos activos y pasivos (esclavos).

#### 3.4.3.1 Protocolo Profibus

El estándar EIA-485 para las versiones FSM y DP del Profibus especifica la velocidad de transmisión que depende de la longitud del segmento (TABLA N° 3.3).

El IEC 1158-2 es usado en Profibus PA y puede alcanzar velocidades de hasta 31.25kbps a través de fibra óptica.

TABLA N° 3.3

Velocidad de Transmisión (kbps)	Máxima longitud del segmento (m)
1200-3000	100
1500	200
500	400
187.5	1000
9.6 – 93.75	1200

### Propiedades básicas del estándar RS 485

Topología:	Bus lineal, con terminaciones en ambos extremos
Medio:	Cable apantallado par trenzado
Cable:	18 AWG (0.8mm)
Atenuación:	3 dB/km a 39 kHz
Numero de estaciones:	32 estaciones sin repetidores extensible hasta 127

EL IEC 1158-2 es un estándar actual usado en áreas especiales de una planta, y requiere de dispositivos intrínsecamente seguros. Este estándar especifica la modulación en código bipolar Manchester NRZ +/-10 mA sobre un voltaje de 9 a 32 Vdc. Este 10 mA genera una señal de +/- 1 voltio que es leído por cada dispositivo en la red.

Las versiones de Profibus FSM, DP y PA pueden ser conectados juntos en un mismo sistema. Esto permite desarrollar dispositivos de bajo costo (FSM) en muchas plantas, dispositivos (DP) en partes de la planta que necesitan alta velocidad y dispositivos PA en áreas de planta donde se requiere comunicaciones seguras y fiables.

Capa de Enlace es definida por Profibus como la capa de enlace de datos Fieldbus (FDL). La parte de control de acceso al medio del FDL define cuando una estación puede transmitir datos, y la MAC asegura que solo una estación transmita datos en un tiempo determinado. La comunicación Profibus utiliza dos métodos de operación denominadas paso de testigo y operación master/esclavo. El paso de testigo asegura la asignación de derechos de acceso al bus con un intervalo de tiempo definido. El Testigo circula entre todas las master con un máximo tiempo de rotación del testigo (configurable) y es especialmente utilizado entre master complejos que requieren iguales derechos en el bus.

El método Master/esclavo permite a la estación master que actualmente tiene el testigo comunicarse con los dispositivos esclavos asociados para leer datos o escribir datos a los dispositivos esclavos.

#### **3.4.3.2 Modelo de Comunicación Profibus**

Los procesos de aplicación en dispositivos de campo son legibles para propósitos de comunicación a través de los llamados dispositivos de campo virtuales (VFD). Estos contienen objetos que pueden ser manipulados por los servicios de la capa de aplicación. Los objetos del un dispositivo real accesibles por comunicación son llamados objetos de comunicación. Los objetos de comunicación de una estación Profibus están dentro de su

librería de objetos (OD), y pueden ser clasificados como objetos de comunicación dinámica o estática.

Los objetos de comunicación estática están definidos en el diccionario de objetos estáticos, estos pueden ser definidos por el fabricante del dispositivos, o definido durante la configuración del bus del sistema.

Profibus reconoce los siguientes objetos de comunicación estática.

- Variable simple
- Arreglos de variables simples del mismo tipo
- Record de variables simples, no necesariamente del mismo tipo
- Dominio rango de datos
- Eventos

Los objetos de comunicación dinámica están dentro de parte dinámica del OD. Estos pueden ser predefinidos o definidos, borrados o cambiados por los servicios de aplicación en la fase operacional.

Profibus soporta los siguientes objetos de comunicación dinámica

- Invocación a programas
- Lista de variables

### **3.5 Introducción a la Arquitectura UCA (Utility Communication Architecture)**

La industria eléctrica a través del instituto de investigación EPRI inicio el desarrollo de la arquitectura de comunicaciones en 1988. El resultado es un conjunto de estándares desarrollados para resolver el problema de interoperatividad entre diferentes fabricantes de dispositivos de monitoreo y control.

UCA no es un protocolo, es un sistema complejo diseñado especialmente para integrar las todas áreas funcionales de las empresas relacionadas con la generación, distribución de servicios (electricidad, agua y gas) utilizando dispositivos que cumplan la especificación UCA (Reconectadores, Transformadores, bombas, válvulas, medidores, etc.), y tener estos dispositivos automáticamente integrados en sistemas SCADA y sistemas de tecnología de la información (IT)

UCA incorpora varios protocolos de comunicaciones para responder a los requerimientos de distintos entornos. La Selección y organización de protocolos se ha diseñado para proporcionar flexibilidad en la elección apropiada aun cumpliendo los criterios de precio y rendimiento.

Los conceptos de “Plug and Play”, fácil configuración e integración, y modelos de datos predefinidos mediante UCA reducirán los costos en varias industrias de servicios y que asegura el éxito de UCA.

La primera versión de UCA identifico requisitos mínimos que deberían satisfacer para comunicar los diferentes equipos involucrados. Para ello, se constituyeron equipos con expertos de cada una de las seis áreas funcionales identificadas (gestión, plantas de generación, centros de control, transmisión, automatización de la distribución e interfaz al cliente) con el objeto de identificar los requisitos de comunicación del sector. Al mismo tiempo, se identificaron los protocolos disponibles y a los que podrían ser integrados en la arquitectura. Uno de los protocolos de mayor interés fue MSS (utilizado fundamentalmente en la industria manufacturera) y fue propuesto para aplicarse en sistemas de adquisición de datos y control en tiempo real.

La primera versión de UCA proporcionaba un gran nivel de funcionalidad. Sin embargo, su adopción en la industria fue limitada. Esto debido, a la falta de especificaciones suficientemente detalladas acerca de cómo deberían ser implementada.

La necesidad de mejorar las comunicaciones fue preponderante, y condujo a UCA 2.0 orientarse al área de las comunicaciones entre centros de control, dado que se utilizaban varios estándares se acordó crear un único estándar que sustituyese a los anteriores. Este

nuevo estándar recibió el nombre de ICCP (Inter Control Center Communication Protocol) que luego paso a denominarse TASE.2 (Telecontrol Application Service Element 2). Su principal misión consistía en mejorar el intercambio de datos entre los centros de control, plantas de generación y sistemas SCADA. Sin embargo, este nuevo estándar no pretendía acceder a los dispositivos de campo, por lo que no presentaba modelos para estos dispositivos. Posteriormente, se observó la necesidad de acceder de forma directa a los dispositivos de campo para tareas requeridas de forma remota relacionadas con operaciones de configuración, pruebas y monitorización de variables de proceso.

La respuesta de UCA llegó con GOMSFE (Generic Object Model for Subestación and Feeder equipment) lo cual proporcionaba una serie de modelos de objetos para modelar dispositivos. Esto condujo a la difusión de un estándar para mapear los modelos de los dispositivos a partir de los modelos GOMSFE sobre MMS (capa de aplicación). Este estándar recibió el nombre de CASM (Common Application Service Models) y se encarga de implementar servicios definidos para los dispositivos sobre el protocolo MMS. Así, al utilizar CASM en todos los modelos de dispositivos se simplifica el proceso de integración. La Fig. 3.1 muestra los estándares de UCA.

<b>Base de datos en Tiempo Real</b>	<b>Dispositivos en Tiempo Real</b>
<b>Modelo de Objetos TASE 2.0</b>	<b>Modelo de Dispositivos UCA (GOMSFE)</b>
<b>MMS</b>	
<b>Perfiles UCA</b>	

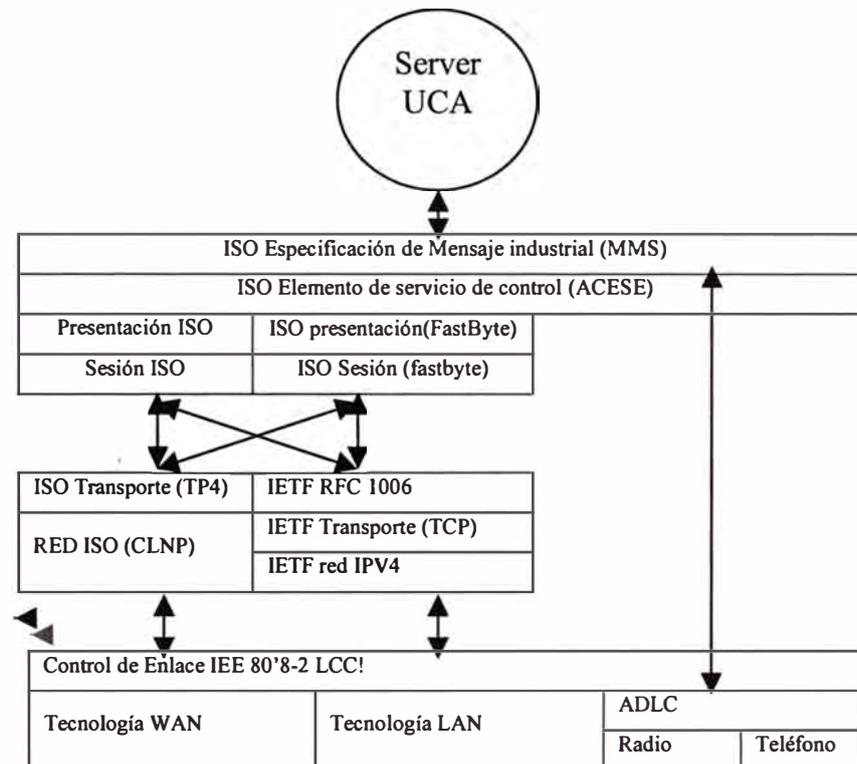
**Fig. 3.1 Estándares UCA**

### 3.5.1 Tecnología UCA

La estructura de UCA esta basada en tres bloques tal como se muestra en la Fig. 3.2. Estos son:

- Una Infraestructura de comunicación uniforme
- Un modelo de datos uniforme
- Una interface de comunicación uniforme

UCA versión 2 esta constituido por los perfiles L, T y A. El perfil L corresponde a las capas fisica y enlace del modelo OSI. El perfil T corresponde a las capas de transporte y red del modelo OSI. Finalmente el Perfil A corresponde a las capas de sesión, presentación y aplicación.



**Fig. 3.2 Perfil de UCA versión 2**

UCA proporciona dos opciones en el nivel T. Los estándares de transporte y red ISO o los estándares de red y transporte IETF (Internet). En el nivel de aplicación (Perfil A), UCA utiliza las capas de sesión y presentación. Utiliza el elemento del servicio de control asociado (ACSE) para establecer una conexión entre aplicaciones. Finalmente, UCA utiliza el estándar MMS, que proporciona la estructura del mensaje, sintaxis y procedimientos de dialogo para monitorear y controlar las comunicaciones.

El comité de estándares DNP3 ha expresado interés de incluir al protocolo DNP3 capacidades adicionales con el objeto de ser utilizado como alternativa del estándar MMS. Esto lo tendremos disponible en un futuro cercano. La filosofía de UCA es utilizar otros protocolos que tengan la suficiente funcionalidad para soportar sus requerimientos.

### **3.5.2 Interface de Aplicación**

Modelo de servicios de aplicación común (CASM). Consiste de un conjunto de definiciones que permite a las aplicaciones y dispositivos ser realmente compatibles. CASM define un conjunto de estándares de funciones, entre ellas incluye las siguientes:

- Capacidad de integrar dispositivos y computadores en una red extensa y heterogénea
- Ser independientes de los protocolos de bajo nivel que puedan utilizarse de manera subyacente.
- Dirigido a un número indeterminado de dispositivos. El número de dispositivos encontrado en las subredes puede variar de uno a varios miles.
- Servicios básicos de aplicación proporciona funciones para monitorear y controlar dispositivos. Estos servicios permitir realizar las siguientes funciones:
  - Lectura y escritura de datos, control de equipos, y detección de alarmas y eventos.
  - Servicios de transmisión multicast
  - Servicios de sincronización de tiempo.
  - Servicios de seguridad.
  - Servicios para transmisión de objetos de datos binarios (Carga y descarga de archivos de configuración de dispositivos).
- Ofrecer un formato de datos de aplicación orientado a objetos.

### **3.5.3 Modelo de Datos**

Los modelos que CASM ofrece se basan en técnicas de modelamiento de objetos actuales. Los dispositivos de campo incorporan estos servicios especificando que objetos se heredan de CASM. Es decir, si el modelo de un dispositivo contiene un objeto de control que requiere un comportamiento determinado, el objeto deberá heredar los atributos y métodos asociados con el objeto propuesto por CASM que proporciona el comportamiento deseado. Los modelos de dispositivos basados en CASM representan el comportamiento de dispositivos reales definiendo clases estándar y objetos construidos a través de herencia y agregación de las definiciones de las clases básicas .

Los usuarios de dispositivos basados en CASM pueden acceder al dispositivo a través del servicio de red bien definidos que operan en los objetos. Los Objetos que son accesibles desde los clientes están contenidos en un objeto de la clase Server. A través de este objeto Server, heredan la estructura que permite las comunicaciones.

UCA También define componentes para implementar funciones de concentrador de datos. Estos componentes están conformados por el cliente de adquisición y control de datos UCA, el contenedor de datos UCA y servidor de adquisición y control de.

## **CAPITULO IV**

### **DISTRIBUCIÓN NETWORK PROTOCOL DNP3.0**

#### **4.1 Introducción**

El protocolo DNP3.0 es un estándar utilizado en sistemas de telecontrol SCADA. Define comunicaciones entre estaciones master, unidades de telemetría RTUs y otros dispositivos electrónicos inteligentes IEDs (Dispositivos Electrónicos Inteligentes).

El DNP3 esta diseñado especialmente para aplicaciones SCADA, define un conjunto de reglas para la comunicación Master - Esclavo en el proceso de adquisición de información y envío de comandos de control.

El DNP3 es diferente a los protocolos de propósito general, como el FTP que es parte del TCP/IP, y que puede enviar extensos archivos, pero de una forma que no aplica para sistemas de control SCADA.

En las Estaciones Remotas las RTUs recopilan datos para transmitir a la Estación Master, Estos datos pueden ser:

- a) Datos de entradas binarias para monitorear estados de dispositivos. Por ejemplo, el estado de un Interruptor Abierto o Cerrado, presión en tuberías para mostrar alarmas de estado normal o excesivo.
- b) Entradas de datos analógicos. Por ejemplo, Corrientes, potencias, nivel de agua de reservorios, temperatura, etc.
- c) Contadores de datos para reportar datos de energía.
- d) Archivos de configuración.

La estación master envía comandos de control, Por ejemplo: Cerrar o abrir un interruptor, abrir o cerrar una válvula.

Valores de salidas analógicas para fijar una presión regulada, fijar un nivel de voltaje deseado.

## 4.2 Características del Protocolo DNP3

- El dnp3 es un protocolo estándar adoptado por diversos fabricantes de equipos y sistemas para proporcionar interoperatividad entre fabricantes.
- Solicitar y responder con múltiples tipos de datos en un solo mensaje.
- Segmentar mensajes en múltiples tramas para asegurar excelente detección y recuperación de errores.
- Incluir en sus respuestas solo datos cambiados
- Asignar clases a los ítems de los datos y solicitar periódicamente basado en clases
- Responder sin solicitud previa
- Utilizar sincronización de tiempo y con un formato estándar
- Permitir múltiples operaciones punto a punto y al Master
- Permitir objetos definibles por el usuario incluyendo transferencia de archivos.
- El DNP3 es reconocido por tener un estricto cumplimiento de las especificaciones de los objetos, y detallada en la certificación para las puestas en servicio del DNP3. Esto se basa en el documento “DNP Subsets” definiciones para que los dispositivos de los fabricantes puedan ser certificados.

## 4.3 BENEFICIOS DEL DNP3

El DNP3 que proporciona los siguientes beneficios a los usuarios:

- Estándar abierto adoptado por un gran número y creciente número de fabricantes de equipos y sistemas.
- Soportado por un activo Grupo de usuarios DNP3.
- Arquitectura conforme al modelo IEC EPA (Enhanced Performance Architecture).
- Optimizado para comunicaciones SCADA eficientes y confiables.
- Soportado por comprensibles estándares de prueba de implementación.
- Tiene definido Subsets para aplicaciones particulares.
- Libertad de seleccionar de múltiples vendedores para futuras modificaciones o expansiones del sistema.

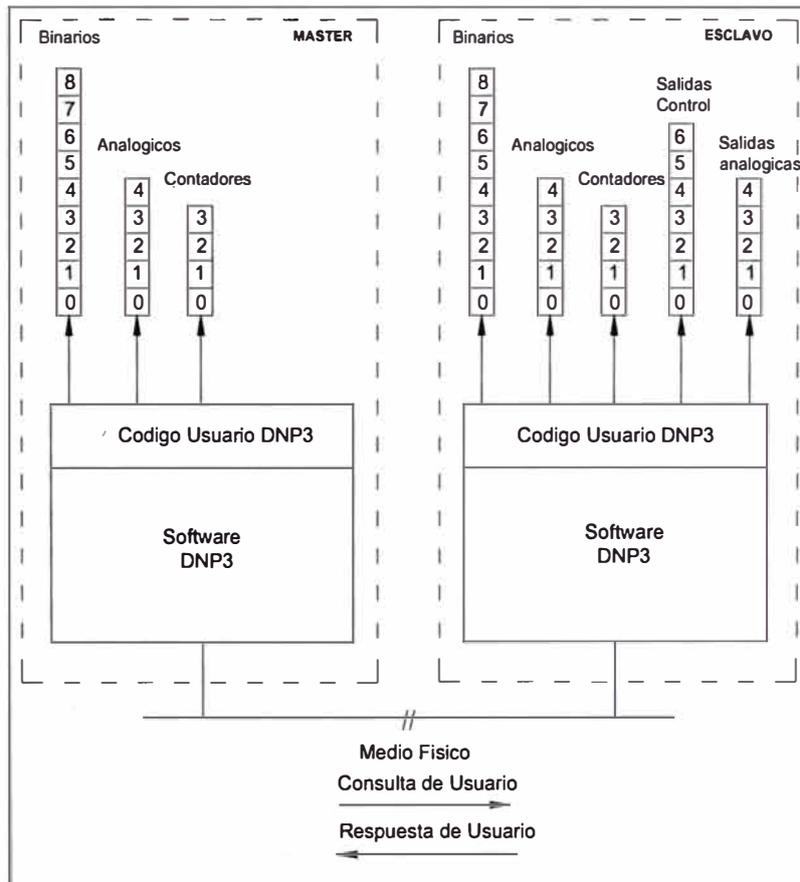
## 4.4 Filosofía de Comunicación

Los términos Servidor (Esclavo) y Cliente (Maestro) son aplicados para sistemas SCADA que utilizan protocolo DNP3. El servidor es un dispositivo o procesos de software que

contiene información disponible para algún dispositivo cliente. En Sistemas SCADA las RTUs son servidores y una Estación Master es cliente.

La Figura 4.1 muestra la relación Cliente-Servidor y proporciona una visión básica de los procesos involucrados, por el cual los distintos tipos de datos tales como entradas binarias, entradas analógicas, contadores, salidas de control y salidas analógicas son conceptualmente organizados como arreglos. Los elementos de los arreglos son enumerados iniciando desde 0 hasta N-1, donde N es el número de elementos. Estos números son denominados índices de puntos en la terminología DNP3.

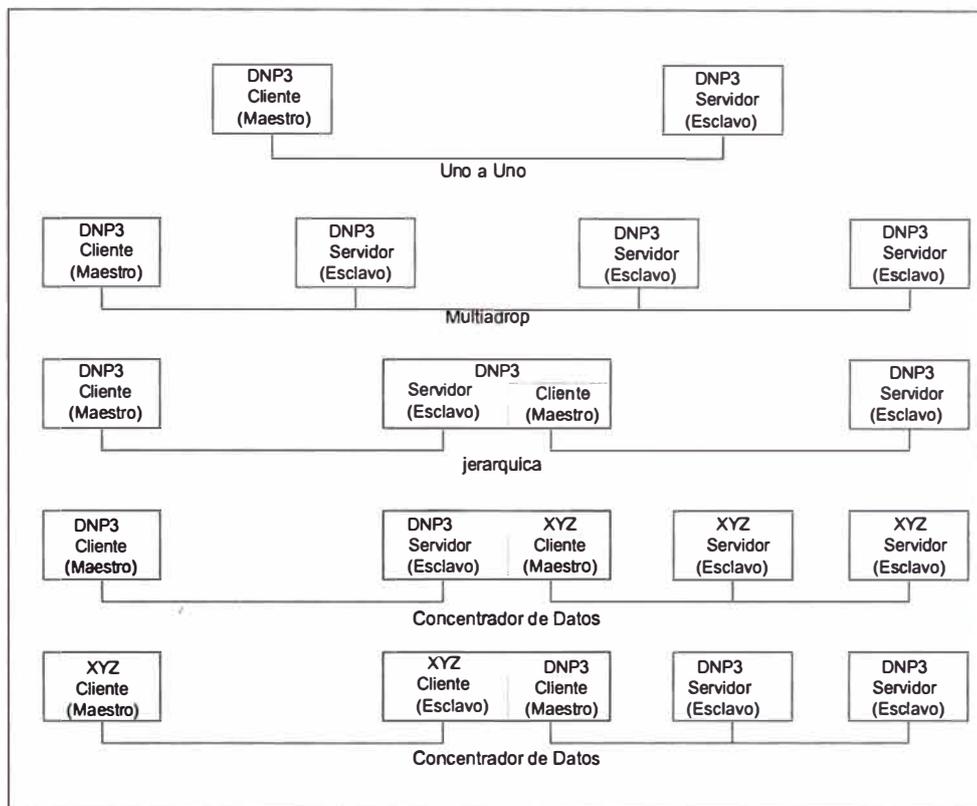
El Servidor y Cliente tienen una similar base de datos para los tipos de datos (binarios, analógicos, contadores). El objetivo de cliente es mantener su base de datos actualizada mediante consultas enviadas al servidor y la respuesta de este con el contenido de su base de datos.



**Fig. 4.1 Relación Cliente Servidor**

Arquitecturas manejadas por el protocolo DNP3.0:

- Master-Esclavo, en esta arquitectura la conexión típica es una línea dedicada.
- Multi-drop, esta arquitectura una Estación maestra comunica varias estaciones esclavas.
- Jerárquica con concentradores de datos intermedios, en esta arquitectura un dispositivo puede recopilar datos de múltiples servidores y almacenar estos datos en su base de datos y ser recuperada por una estación esclava cliente. Este diseño es frecuentemente utilizada en Subestaciones.



**Fig. 4.2 Arquitectura Utilizadas**

DNP3 soporta múltiples esclavos (peer - peer) y múltiples comunicaciones master, modos de operación de encuesta (poll), y modo reporte espontáneo. Este último modo, las encuestas por cambios no son necesarios, por que la master estación master puede confiar que la estación remota enviara una respuesta no solicitada cuando ha sucedido un cambio que necesita ser reportado. En ausencia de cambios, el sistema permanece en un estado quieto, sin ninguna encuesta de la estación master o respuestas de las estaciones remotas.

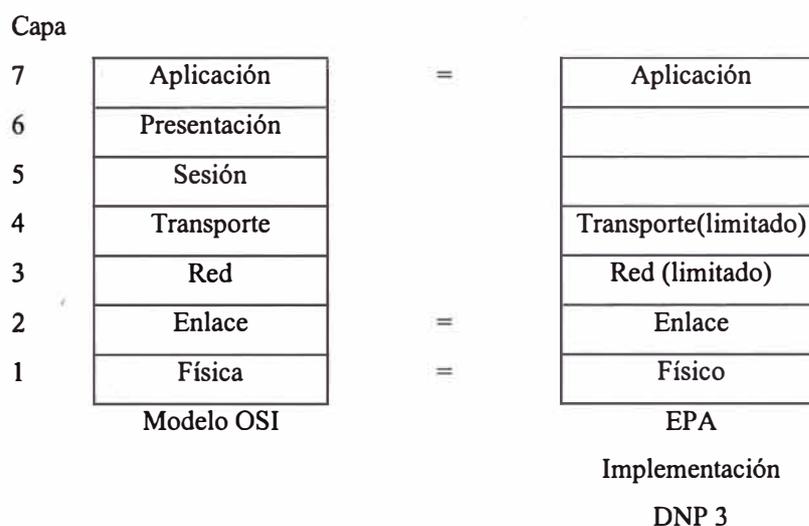
Este modo de operación de la estación master aprovecha mejor la capacidad del sistema de comunicaciones.

La capacidad para soportar la operación peer - peer y modo espontáneo requiere que estaciones que no están diseñados como estación master y que puedan iniciar la transacción de datos. Esto algunas veces esta relacionado con comunicaciones balanceadas, el cual significa que cualquier estación pueda actuar primaria o secundaria al mismo tiempo.

#### 4.5 Análisis de la Arquitectura del DNP3

EL DNP3.0 agrega una cuarta al modelo EPA (Enhanced Performance Architecture) basada en 3 capas del modelo de referencia OSI, denominada la capa de pseudo - transporte encargada de la segmentación de mensajes.

La figura 4.3 muestra la relación entre las 3 capas del modelo EPA, y el modelo de referencia OSI.



**Fig. 4.3 Relación OSI-EPA**

La Fig. 4.4 Muestra la arquitectura del DNP3 basados en niveles

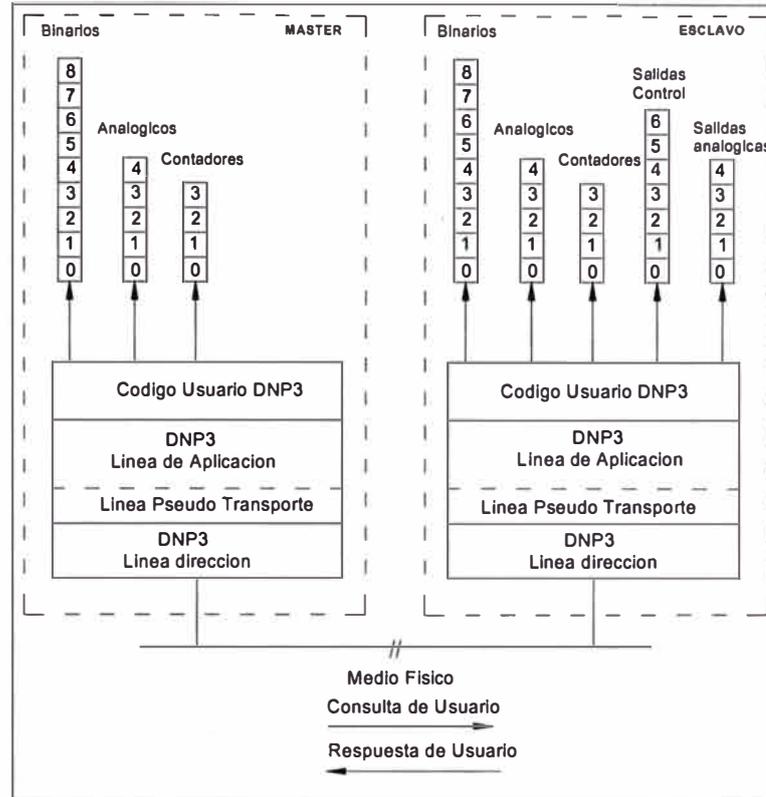
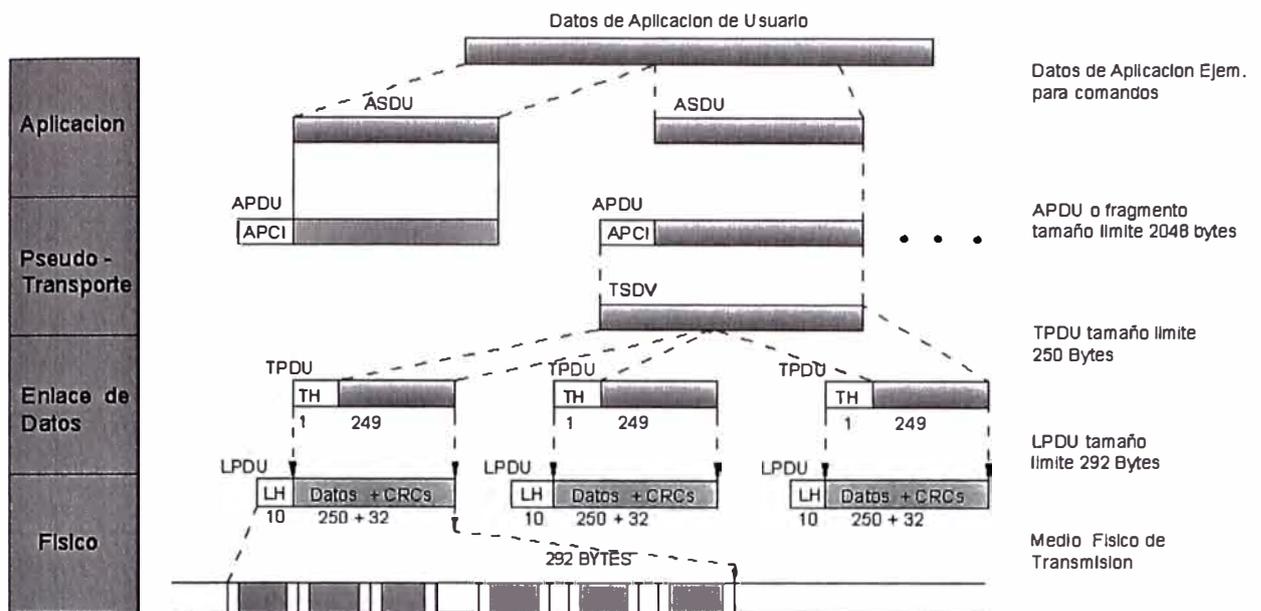


Fig. 4.4 Capas del DNP3

Cada capa del modelo recoge la información transferida desde las capas superiores, y adicionan información relacionada con los servicios ejecutados por dicha capa. Durante la construcción del mensaje, el mensaje aumentara de tamaño en cada capa de nivel inferior conforme desciende a las capas inferiores. Mientras que en el proceso de reconstrucción de datos se obtendrá unidades pequeñas de datos.

La Fig. 4.5 muestra la estructura del mensaje DNP3



**Fig 4.5 Secuencia de construcción del mensaje DNP3**

#### 4.5.1 Capa física

Define las características de la interfaz física sobre el cual se comunica el protocolo. Realiza funciones para el control del medio para establecer y mantener el enlace físico, y control de flujo de datos.

DNP3 especifica normalmente el estándar ITU-T V.24, EIA RS232 o RS485 usando medios tales como Fibra óptica, radio o Satélite, y Ethernet. .

#### 4.5.2 Capa de enlace.

Maneja la conexión lógica entre el remitente y el receptor haciendo la transmisión confiable de la información a través del medio físico. Esta capa está específicamente relacionada con la transferencia de datos, para lo cual proporciona funciones de control de flujo y detección de errores.

La capa de enlace el DNP3 utiliza el formato de trama FT3 (LPDU) especificado por el estándar IEC 60870-5-1. El formato especifica una cabecera de 10 octetos, seguido opcionalmente por 16 bloques de datos. El mensaje total es limitado a 292 octetos, el cual proporciona una capacidad máxima de 250 octetos de datos

La Fig. 4.6 representa el formato de trama FT3

Start	Lengt	Control	Address	Sourse	CRC	User	CRC	.	.	.	User	CRC
			Address	Address		Data					Data	
2	1	1	2	2	2	16	2				1-16	2
Longitud de cabecera 10 Bytes						0-282 bytes 250 bytes de datos						

Fig. 4.6

La cabecera de la Trama DNP3 empieza con dos octetos de sincronización que ayudan a los receptores de las tramas determinar donde inicia la trama. El campo longitud especifica el número de octetos de la trama, no incluye los octetos del código CRC. El octeto de control de enlace es usado entre las capas de enlace del transmisor y receptor para coordinar sus actividades.

El campo de dirección de destino que dispositivo DNP3 debe procesar el mensaje, y el campo dirección fuente identifica que dispositivo DNP3 envió el mensaje. Cada dispositivo remoto debe tener una única dirección, en total 65520 son disponibles. Tres direcciones están reservadas por DNP3 para denotar un mensaje que deben ser procesados por todos los dispositivos DNP3, y 13 direcciones son reservados para especiales necesidades en el futuro.

La información útil (payload) en la trama de enlace contiene un par de octetos CRC para cada 16 octetos de datos, esto proporciona un alto grado de seguridad en la detección de errores que pueden ocurrir durante en la transmisión de datos. El máximo numero de octetos de la información útil es 250, sin incluir los octetos CRC.(La longitud de la trama de enlace es de 292 octetos incluyendo los octetos CRC y cabecera)

Una de las características de la capa de enlace del DNP3 es la habilidad del transmisor de trama solicitar al receptor un acuse de recibo de la trama. Esto proporciona un grado extra de seguridad de la confiabilidad de las comunicaciones, dado que si la confirmación no es recibida, la capa de enlace puede reintentar la transmisión. Sin embargo, la desventaja el tiempo extra requerido para la confirmación de mensajes y tiempos de espera para tiempos de expiración (tiemouts) cuando existe configuración de reintentos.

#### a) Octeto de Control

Proporciona el control del flujo de datos sobre el enlace fisico, e indica la dirección. La interpretación del octeto de control es dependiente si la comunicación es un mensaje primario o secundario.

DIR: Dirección (1=A hacia B, 0=B hacia A)

PRM: Mensaje primario (1=mensaje desde Primario, 0=mensajes desde Secundario)

FCB: Bit contador de trama

FCV: Bit contador de trama valida

RES: Reservado

DFC: Bit de control de flujo de datos. 1 colocado por la estación secundaria si los datos de usuario causan desbordamiento de buffer.

FC: Código de Función.

La Fig. 4.7 muestra los bits del octeto de control, y las Tablas 4.1 y 4.2 muestran los códigos de función (Primario-Secundario) y (Secundario-Primario).

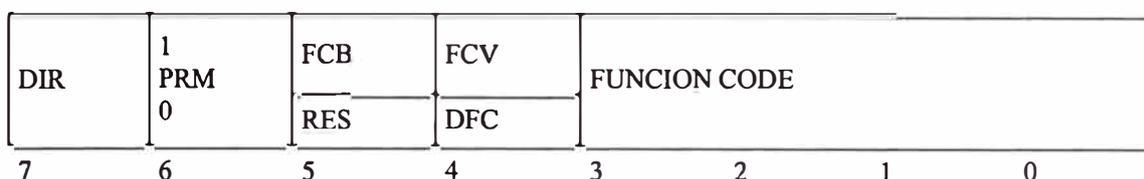


Fig 4.7 Octeto de Control

TABLA N° 4.1 Función Code (Primario a Secundario)	
Code	Descripción
0	Reset Link
1	Reset Process User
2	Test Link
3	User Data-Confirm Expected
4	User Data – No confirm
9	Request Link Status

TABLA N° 4.2 Función Code (Secundario a Primario)	
Code	Descripción
0	Confirm-ACK
1	Confirm-NAK
11	Respond-Link Status
14	Link not Funtioning
15	Link not Used

**Bit Dirección (DIR).** Indica la dirección de mensajes entre las estaciones primarias y secundarias.

**Bit Primaria (PMR).** El PMR = 1 si la trama es inicializada por la estación primaria o respuesta de la estación secundaria.

**Bits contadores de Tramas (FCB y FCV):** Estos bits son usados por los mensajes primarios. FCB es usado para detectar pérdidas o duplicación de tramas a una estación secundaria. Si FCV =1, el FCB es para cada transacción exitosa SEND – CONFIRM entre las mismas estaciones primaria y secundaria.

- Reiniciando el enlace de datos o una transacción fallada, la estación secundaria no aceptara tramas SEND-CONFIRM con FCV=1 hasta que una transacción reset este

completada. Esto significa que solo aceptara un reset de enlace o un comando de reset de proceso de usuario.

- Después de que la estación secundaria recibe la trama para reiniciar el enlace (RESET link) responderá con una confirmación y el enlace quedara operativo hasta que un error de transmisión de trama ocurra nuevamente.
- La estación secundaria quedara a la espera de la trama siguiente que con FCB=1 y FCB=1.
- El siguiente mensaje primario SEND-CONFIRM tendrá FCB=1 y FCB=1. La estación secundaria aceptara como FCB valido.
- Cada mensaje primario SEND – CONFIRM tendrá el FCB=0 o 1 Bit de control de flujo de datos (DFC). La estación secundaria colocara DFC=1 si los datos de usuario causaran desbordamiento de buffer, o por alguna otra razón no procesa los datos. La recepción de trama con DFC=1 en la estación primaria detendrá el envío de datos, pero solicitara estado del enlace para determinar cuando enviar datos nuevamente (DFC=0)

### Códigos de Función de la capa de enlace

La TABLA N° 4.3 muestra en detalle el significado para diferentes valores de los códigos función. El significado es diferente dependiendo si el mensaje es una transmisión primario o secundario.

**TABLA N° 4.3 Códigos de Función desde la estación primaria**

Función Code	Tipo de Trama	Función de Servicio	FCV bit
0	Send – Confirm expected	Reset de enlace remoto	0
1	Send –Confirm expected	Reset de User Process	0
2	Send –Confirm expected	Test funtion for link	1
3	Send –Confirm expected	User data	1
4	Send –No reply expected	Unconfirmend user data	0
9	Request – Respond expected	Request Link Status	0

Los códigos 5-8, 10-15 no son usados

**TABLA N° 4.4 Códigos de función de estación Secundaria**

Función Code	Tipo de Trama	Función de Servicio
0	Confirm	ACK- positive acknowledgment
1	Confirm	NACK – Message not accepted, link busy
11	Respond	Status of link (DFC =0 o 1)
14		Link service not functioning
15		Link service not used o implemented

Los códigos 2-10, 12-13 no son usados

### b) Código de Error CRC

EL código de redundancia cíclica es usado para detectar errores en las tramas transmitidas. el DNP3 define un código de redundancia cíclica de 16 bits para la cabecera de datos de 64 bits, y para cada 128 bits de bloques de datos de usuario transmitidos. Para ello utiliza el siguiente polinomio generatriz:

$$P=X^{16} + X^{13}+ X^{12}+ X^{10}+X^8+ X^5+ X^2+ +1$$

Este forma un número de 17 bits (13D65 Hex)

### 4.5.3 Capa de Transporte

Esta capa esta incluido en el protocolo DNP3.0 para permitir la transmisión de grandes bloques de datos. Para lo cual divide los datos de la capa de aplicación en múltiples tramas de transmisión. Para cada trama, inserta un octeto que indica si la trama es el primero del mensaje o ultima trama del mensaje o ambos para mensajes simples. También indica un numero de secuencia de trama que permite que a la capa de transporte recipiente detectar tramas perdidas. Los servios de esta capa no están relacionados exactamente con ruteo o control de flujo de paquetes de datos sobre redes.

La capa de transporte en DNP3 divide la Unidad de Datos del Servicio de Transporte (TSDUs), en una o más unidades de datos de protocolo de transporte (TPDUs) y enviar a la capa de enlace para ser transmitidas, y en la recepción reconstruye los mensajes. Es decir, el TPDU convierte los datos de usuario en datos de capa de enlace (LSDUs) y viceversa. El DNP3 requiere un solo octeto en el mensaje para realizar la función de transporte, el cual esta incluido en la capa de enlace. Por consiguiente, como la capa de enlace puede manejar hasta 250 octetos de datos uno de estos es utilizado para la función de transporte.

En DNP3 la función de la capa de transporte es limitada comparada con las definiciones de la capa de transporte definida en el modelo OSI, por ello, muchos de usuarios lo denominan con el prefijo “pseudo” por su simplicidad.

La capa de aplicación divide los mensajes en fragmentos. El tamaño de los fragmentos es determinado por tamaño de buffer del dispositivo receptor de datos y que normalmente son de 2048 y 4096. Un mensaje que es más grande que uno de los fragmentos requiere múltiples fragmentos. Esta función de fragmentación de los mensajes es responsabilidad de la capa de aplicación.

#### a) Cabecera de Transporte

La Figura 4.8 ilustra el octeto de cabecera de transporte; contiene bits de inicio y final de secuencia de tramas (TPDUS), y un contador de secuencia de 6 bits.



**Fig.4.8 Octeto Cabecera de Transporte**

FIN: Final de Trama

FIR: Primera Trama

TABLA N° 4.5

FIR	FIN	
0	1	Primero de las múltiples tramas
0	0	No Primero, no Último
1	0	Trama Final
1	1	Un mensaje de trama

### b) Sumario de las funciones de la capa de transporte

- EL TSU fragmenta mensajes de 2048 octetos y los divide en múltiples TPDUs
- Incluye un 1 Octeto de cabecera
- TPDU transporta 249 Octetos de datos de usuario
- EL TPDU puede encajar en una trama FT3 (LSDU)
- La cabecera contiene Bits FIR y FIN y número de secuencia 6 bits
- Translada los TPDUs hacia y desde la capa de transporte
- Reconstruye TPDUs en TSDU.

### 4.5.4 Capa de aplicación

Esta capa es el nivel más alto del protocolo, y proporciona servicios a los programas de aplicación de usuario. La Estación Master genera mensajes para solicitar información a las estaciones secundarias, y las Estaciones Secundarias generan respuestas del nivel de aplicación. Los mensajes son construidos y se pasan a la capa de transporte donde se dividen en segmentos y luego se entrega a la capa de enlace para ser transmitido. Si los datos a transmitir es muy grande para un solo mensaje de la capa de aplicación, se construye múltiples mensajes, y se transmiten secuencialmente. Cada mensaje es independiente de la capa de aplicación y existe una indicación de asociación con el siguiente en todos los mensajes excepto en el último.

En la sección anterior se observa como el primer octeto de la información de control del protocolo de aplicación (APCI) es usado en el manejo de la secuencia de los mensajes del nivel de aplicación entre la Estación Master y las Estaciones Secundarias. En esta sección se realiza un análisis de los mensajes de aplicación y la información que transportan básicamente consistente en comandos y datos que son generados en respuesta a los comandos. Es decir la funcionalidad del nivel superior proporcionado por los sistemas SCADA.

La capa de aplicación proporciona estandarización de funciones y formato de datos con los que interactúa la capa de usuario. Los mensajes de aplicación contienen números de función y objetos de datos. Los números de función definen exactamente el significado y propósito del mensaje, por ejemplo cuando un servidor DNP transmite un mensaje conteniendo respuesta de datos, el mensaje identifica el número de objeto y la variación de cada valor en el mensaje. Los objetos y números de variación son asignados para contadores, entradas binarias, salidas analógicas y de control. En DNP3 los tipos de datos y formatos están identificados por objetos y números de variación, a través de los cuales se asegura la interoperatividad entre dispositivos. La capa de usuario del Cliente formula su solicitud por datos al servidor especificando a la capa de aplicación la función a ejecutar, y especifica los objetos requeridos. La solicitud puede especificar cuantos objetos desea o especificar algunos objetos a partir del número de índice X hasta un número de índice Y.

La capa de aplicación envía la solicitud a la capa de enlace a través de la capa de transporte que a su vez este envía el mensaje al servidor.

La respuesta opera de manera similar, en el que la capa de usuario del servidor recoge los datos deseados y los presenta a la capa de aplicación en formatos de datos mediante objetos y variación. La data es transmitida a través del canal de comunicaciones y entregadas a la capa de aplicación del cliente. Aquí los objetos son presentados a la capa de usuario.

La transmisión de mensajes no solicitados es un modo de operación, donde el servidor transmite una respuesta no solicitada, sin tener que recibir una solicitud específica por datos del cliente. No todos los servidores tienen esta capacidad, pero aquellos que lo hacen tienen que ser configurados para operar en este modo. Este modo de operación es usado cuando existen muchos dispositivos esclavos y el servidor requiere notificación inmediata después de la ocurrencia de un cambio

Para configurar un sistema con reporte espontáneo requiere básicamente. Primero que las transmisiones suceden espontáneamente, y ocurren muchas disputas por el control de acceso al medio, y por lo tanto el acceso al medio debe ser mejor. La otra es que el servidor debe tener forma de conocer si puede transmitir sin que algún mensaje este en progreso. DNP3 especifica algoritmos a los desarrolladores de sistemas.

El grupo DNP3 reconoce que la especificación del DNP3 no es necesariamente para cada dispositivo. Algunos dispositivos son limitados en memoria y velocidad y otras pueden tener características más sofisticadas. Considerando esto, DNP3 organiza la complejidad

en niveles. El nivel 1 proporciona funciones básicas y las otras son opcionales. Nivel 2 proporciona mas funciones, variaciones y objetos, y el Nivel 3 es mas sofisticado.

### a) Códigos de Función de Aplicación

El código de función es el segundo octeto del APCI. El siguiente es el octeto de control de aplicación, en ambos se requiere cabeceras desde estaciones master y cabeceras de respuesta desde las estaciones secundarias. La tabla N° 4.6 muestra los códigos de función indica la tarea a ser ejecutada.

**TABLA N° 4.6 Códigos de función de estación Secundaria**

Función Code	Tipo de Trama	Función
0	Función	Confirmación
1		Lectura
2		Escritura
3-6	Función de control	
7-12	Confirmación de control de aplicación	
13-22	Configuración de función	
23	Sincronización de tiempo	
24-128	Reservado	

**TABLA N° 4.7 Códigos de función de respuesta**

Función Code	Tipo de Trama	Función
0	Función de respuesta	Confirmación
129		Lectura
130		Mensaje no solicitado

Muchas de las funciones necesitan identificar datos específicos en los cuales van operan. Estos lo realizan con las referencias de los objetos que están incluidas en los datos ASDU que sigue a la cabecera APCI.

La Tabla N° 4.8 presenta las funciones de transferencia que son aquellas relacionadas con transferencia de datos definidos que recopilan datos desde las estaciones secundarias, o información de control y escritura.

**TABLA N° 4.8 Función de Transferencia**

<b>Función Code</b>	<b>Tipo de Trama</b>	<b>Acción</b>	<b>Respuesta</b>
0	Confirmación	Confirmación de fragmento de mensaje. Usado por ambos consultas y respuesta	Confirmación
1	Lectura		Lectura
2	Escritura	Almacena datos específicos	Mensaje no solicitado

La Tabla N° 4.9 muestra las funciones de control usados para operar o cambiar puntos de control en una estación secundaria. Estos pueden ser salidas por rele, puntos digitales, valores de setpoints analógicos, que pueden ser operados directamente, sin o con reconocimiento, o con la secuencia Select Befote Operate.

La Secuencia Select Befote Operate SBO es una característica es conocida en la industria eléctrica por el nivel de seguridad adicional para asegurar contra error de operación surgido de un mensaje corrompido o una equivocación en la selección del dispositivo de un grupo de dispositivos idénticos en una pantalla HMI

La secuencia Select Befote Operate requiere lo siguiente.

- Selección del Punto
- La estación Secundaria responde con la identidad del punto seleccionado y el estado de los puntos seleccionado
- La estación Secundaria inicia un temporizador Select-Operate
- El HMI muestra los puntos seleccionados de manera que muestren que han sido seleccionados
- La función de operación es enviada para los puntos seleccionados
- La estación secundaria rechazara el mensaje de operación si el punto no coincide con el seleccionado previamente.

La estación secundaria finalizara la selección del punto si el temporizador Select -Operate expira antes de la recepción de la función Operate

**TABLA N° 4.9 Funciones de Control**

Código	Tipo de Trama	Acción	Respuesta
3	Select	Select, pero no produce ninguna acción de control o cambio de setpoint. La función Operate debe seguidamente recibir para activar las salidas.	Respuesta con el estado del punto de control seleccionado
4	Operate	Producir las acciones de salida en los puntos previamente seleccionados por la función select	Responde con el estado de los puntos de control
5	Direct Operate	Selecciona y opera las salidas especificadas o puntos de control.	Responde con el estado de los puntos de control
6	Direct Operate, no ack		No responde al mensaje enviado

La Tabla N° 4.10 muestra las funciones de congelamiento típicamente usados para lo siguiente:

- Almacenar datos de estado en un tiempo común
- Guardar valores o estados de puntos específicos en intervalos regulares.

**TABLA N° 4.10 Funciones Frezee**

Código	Tipo de Trama	Acción	Respuesta
7	Inmediate Frezee	Copia objetos especificados para un Congelamiento buffer	Responde con estados de operación puntos de estado. Note que los datos no son retornandos
8	Inmediate Frezee – no ack	Copia objetos especificados para un Congelamiento buffer	No responde a ser enviado
	Frezee and clear	Copia objetos especificados para un Congelamiento buffer, luego limpia los objetos.	Responde con estados de operación puntos de estado. Note que los datos no son retornandos
9	Frezee and clear – no ack	Copia objetos especificados para un Congelamiento buffer, luego limpia los objetos.	No responde al mensaje enviado

10	Freeze with time	Copia objetos especificados para un Congelamiento buffer en el tiempo especificado y después en intervalos especificados	Responde con estados de operación puntos de estado. Note que los datos no son retornados
11	Freeze with time- No Ack	Copia objetos especificados para un Congelamiento buffer en el tiempo especificado y después en intervalos especificados	No responde al mensaje enviado

La Tabla N° 4.11 muestra las funciones de control de aplicación, cuya definición es la siguiente:

El Cold Restart es un completo reinicio de la estación secundaria, como si haya sido desenergizada y luego energizada.

El Warm Restart puede ser usado para detener la aplicación DNP3 pero no necesariamente reiniciar otros programas de aplicación. Típicamente es usado para inicializar su configuración y limpiar los eventos almacenados en los buffers.

Inicializar datos por defecto puede por ejemplo configurar Setpoints y limpiar contadores. Los objetos de datos específicos a ser inicializados son identificados en las consultas pero no los valores por defecto. Estos son almacenados localmente en la Estación secundaria como datos de lectura fija o como parámetros en memoria no volátil.

**TABLA N°4.11 Funciones de control de aplicación**

<b>Función Code</b>	<b>Tipo de Trama</b>	<b>Acción</b>	<b>Respuesta</b>
13	Cold restart	Reinicio aplicación en el final de secuencia de comunicaron	Responde con tiempo hasta Estación Remota availability following
14	Warm restart	Reinicio parcial en el final de secuencia de aplicación	Responde con tiempo hasta Estación Remota availvality following
15	Inicializar datos por defecto	Inicializar datos específicos para iniciar datos o parámetros por defecto	Responder con el estado de operación
16	Inicializar aplicacion	Inicializar aplicaciones especificas	Responder con el estado de operación
17	Iniciar aplicación	Iniciar aplicaciones especificas	Responder con el estado de

			operación
18	Parar aplicacion	Parar aplicaciones especificas	Responder con el estado de operación

La Tabla N° 4.12 muestra los códigos de configuración de funciones es el estado de parámetros y configuración que determinan el comportamiento de la Estación.

**TABLA N° 4.12 Configuración de Funciones**

<b>Función Code</b>	<b>Tipo de Trama</b>	<b>Acción</b>	<b>Respuesta</b>
19	Guardar configuración	Guardar la configuración especificada en memoria no volátil	Respuesta con el tiempo de disponibilidad de estación
20	Habilita mensajes no solicitados	Habilita reporte espontáneo de objetos de datos especificados	Responde con ele estado de operación
21	Deshabilita mensajes no solicitados	Deshabilita reporte espontáneo de objetos de datos especificados	Responde con ele estado de operación
22	Asigna clases	Asigna clases a objetos de datos especificados	Responde con ele estado de operación

La función de medición de retardo es usado para realizar sincronización inmediata mediante escritura al reloj de la estación secundaria. Esto es usado en enlaces seriales asíncronos debido a que el tiempo de transmisión es significativo en comparación a la resolución de un milisegundo del reloj. La estación secundaria mide el tiempo en milisegundos, que toma la respuesta del mensaje, esto es el tiempo desde el ingreso del mensaje hasta el envío de la respuesta a la Estación Master. La estación master sustrae este tiempo del tiempo de respuesta, para determinar el tiempo transcurrido durante la comunicación.

La función de almacenamiento de tiempo actual es usado cuando se ejecuta la escritura de tiempo sobre una red LAN. En este caso la transmisión ocurre instantáneamente, y no es necesario el tiempo de respuesta. En ambos las Estaciones Master y secundaria almacenan el valor actual del tiempo de sus propios reloj cuando el mensaje es enviado.

Seguidamente, la master envía su tiempo almacenado a la estación secundaria, el cual

calcula el error de tiempo de la diferencia entre los valores almacenados. La Tabla N° 4.13 muestra los códigos de función de sincronización.

**TABLA N° 4.13 Función de sincronización de tiempo**

<b>Código</b>	<b>Tipo de Trama</b>	<b>Acción</b>	<b>Respuesta</b>
23	Medición de Retardo	Permite medir el retardo en la ruta entre la Estaciones Master y la Secundaria . El valor determinado es usado como un valor desviación (offset) cuando es configurado el tiempo de sistema en la estación secundaria	Mensaje responde con retardo de tiempo de recepción y respuesta
24	Almacenamiento de tiempo actual	La Estación Secundaria almacena el tiempo de su reloj al termino de la entrada del mensaje	Responde con el estado

Las funciones de archivo proporcionan operaciones con configuración de archivos y otros archivos en los dispositivos remotos. Algunos dispositivos pueden implementar características de seguridad para controlar acceso a sus archivos cuando sean necesarios, por lo tanto requiere un procedimiento de autenticación. La tabla N° 4.14 muestra los códigos de funciones de archivo.

**TABLA N° 4.14 Funciones de Archivo**

<b>Código</b>	<b>Tipo de Trama</b>	<b>Acción</b>	<b>Respuesta</b>
25	Abrir archivo	El archivo requerido es bloqueado para prevenir el uso por otros procesos.	Responde con archivo de estados (Grupo de Objeto 70, variación 4)
26	Cerrar Archivo	El archivo es cerrado y disponible para uso por otros procesos	Responde con archivo de estados (Grupo de Objeto 70, variación 4)
27	Borrar Archivo	EL archivo requerido es borrado, siempre que no sea abierto. Si esta abierto el comando no es ejecutado	Responde con archivo de estados (Grupo de Objeto 70, variación 4)
28	Obtener archivo	Proporciona información de archivo: Tipo, tamaño, tiempo de creación y permisos.	Responde con objeto descriptor de archivo (Grupo de Objeto 70, variación 7).
29	Autenticación	Solicita clave de autenticación	Responde con Objeto

		desde la estación secundaria.	Autenticador (Grupo de Objeto 70, variación 2).
30	Rechazo	Inmediatamente abandona una transferencia de archivos en progreso y cierra el archivo sin guardar cambios	Responde con archivo de estados (Grupo de Objeto 70, variación 4)

### b) Códigos de Función de Respuesta

**TABLA N° 4.15 Función de sincronización de tiempo**

Código	Tipo de Trama	Acción	Respuesta
0	Confirmación	Confirmación de Fragmento de mensaje. Usados por respuestas y consultas	No requiere respuesta
129	Respuesta	Respuesta a solicitudes	Estación Master responderá con confirmación si Bit CON=1
130	Mensaje no solicitado	Mensajes no solicitados desde estaciones secundarias	Estación Master responderá con confirmación si Bit CON=1

### Indicadores Internos

El campo de indicadores internos (IIN) es un doble octeto contiguo al campo de códigos de función en todas las respuestas. Es mediante los indicadores internos que los estados de las Estaciones Secundarias son reportados a la Estación Master. Cada bit en el campo tiene un específico significado. La descripción detallada del significado de cada bit son incluidas en las Tablas 4.16 y 4.17.

**TABLA N° 4.16 Significado de bits del Primer Byte**

<b>Bit</b>	<b>Significado</b>	<b>Notas</b>
0	Mensaje recibido por todas las estaciones	Bit0=1, cuando una dirección del rango FFF0-FFFF es recibida., y Bit0=0 después de la siguiente respuesta.
1	Disponibilidad de datos clase 1	Indica que datos de clases especificadas están disponibles.
2	Disponibilidad de datos clase 2	
3	Disponibilidad de datos clase 3	
4	Solicitud de sincronización de tiempo	Después de un reinicio , Bit4=1; y Bit4=0 luego de la sincronización.
5	Puntos en local	Cuando uno o más puntos están en modo local y por lo tanto no pueden ser controlados remotamente.
6	Falla de dispositivo	Usado cuando una condición anormal esta presente.
7	Reinicio de dispositivo	Bit7=1 cuando se reinicia la aplicación de usuario, y Bit7=0 cuando la master desactiva directamente

**TABLA N° 4.17 Significado de bits del Segundo Byte**

Bit	Significado	Notas
0	Código de función no implementada	No disponible
1	Objetos solicitados no conocidos	No hay objetos en las cales especificadas
2	Parámetros invalidos	Parámetros o campos de datos fuera de rango
3	Buffer desbordado (overflow)	Desbordamiento de Buffers de Eventos o de otra aplicaciones
3	Operación en progreso	Esta operación esta ejecutándose
5	Configuración corrupta	Indicador de un problema especifico. La master tendrá que descargar una nueva configuración
6	Reservado	Siempre retorna 0
7	Reservado	Siempre retorna 0

### c) Librería de Objetos de Datos

En DNP3 La información de control y los datos son formados en el nivel de aplicación mediante objetos de datos. Cada objeto esta definido por un número de grupo y un número de variación (campo de 8 bits).

La TABLA N° 4.16 ilustra los grupos de objetos organizados en rangos.

**TABLA N° 4.18 Grupos de Objetos**

Bit	Significado
0-9	Objetos de entradas binarias
10-19	Objetos de salidas binarias
20-29	Objetos contadores
30-39	Objetos de entradas analógicas
40-49	Objetos de salidas analógicas
50-59	Objetos de tiempo
60-69	Objetos de clases
70-79	Objetos de archivos
80-89	Objetos de aplicación
100+	Objetos numéricos alternativos

La TABLA N° 4.19 presentan la variación de los grupos de objetos de datos.

- Los objetos de entradas binarias representan el estado de una entrada física o una entrada por software tal como un flag.
- Las entradas binarias de bit simples están siempre empaquetados en un Octeto (8-bits)
- Las posiciones de bits no usados son rellenados con ceros.
- Los elementos de flan de eventos contienen la misma información que el flan estático.
- Los objetos eventos pueden ser usados para guardar eventos, o para actualizar base de datos usando el modo de operación inactivo cuando suceden cambios.
- El time Tagging usa el tiempo local en los dispositivos.
- Tiempo relativo es precedido con un objeto de tiempo común en el mensaje y proporciona un medio de transmisión a un numero de time stamps de modo eficiente.

**TABLA N° 4.19 Objetos de Entradas Binarias**

Grupo	Var	Tipo	Descripción	Estructura
01	01	Estático	Entrada binaria (Bit Simple)	
	02	Estático	Entrada binaria con estado	Flag 1
02	01	Evento	Cambio de entrada binaria sin tiempo	Flag 1
	02	Evento	Cambio de entrada binaria con tiempo	Flag 1,;tiempo
	03	Evento	Cambio de entrada binaria con tiempo relativo	Flag; Tiempo relativo

La Tabla N° 4.20 muestra los objetos de salidas binarias.

- Las salidas de control pueden ser por software (flags) o hardware (salidas físicas).
- Las salidas binarias son controladas con OG 10V01
- Los estados de las salidas binarias son retornados con OG 10V02
- El control de bloques de reles proporcionan un número de opciones de control incluyendo, pulse on, Pulse off, latch on, latch off.
- El control de bloques de reles pueden también ser usados para proporcionar control sobre combinaciones Select/Trip/Close.
- El bloque de patrón de control realiza acciones control a un número de puntos simultáneamente. Los puntos son seleccionados usando la mascara patrón.

**TABLA N° 4.20 Objetos de Salidas Binarias**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
10	01	Estático	Salida binaria (Bit Simple)	Packed Binary
	02	Estático	Estados de salidas Binarias	Flag 2
12	01	Estático	Control de bloques de salidos por rele	Código de control; contador; On time; Off time; código de estado.
	02	Estático	Patrón de bloques de control	Código de control; contador; On time; Off time, código de estado.
	03	Estático	Mascara de patrón	Encapsulado Binario

**TABLA N° 4.21 Objetos de Entradas analógicas**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
30	01	Estático	Entrada analógica 32 bits	Flag 4; I32
	02	Estático	Entrada analógica 16 Bits	Flag 4; I16
	03	Estático	Entrada analógica 32 bits sin flag	I32
	04	Estático	Entrada analógica 16 Bits sin flag	I16
	05	Estático	Entrada analógica en punto flotante corto	Flag 4; FLT32
	06	Estático	Entrada analógica en punto flotante largo	Flag 4; FLT64
31	01	Estático Congelado	Entrada analógica congelada (Frozen) 32 bits	Flag 4; I32
	02	Estático Congelado	Entrada analógica congelada (Frozen) 16 bits	Flag 4; I16
	03	Estático Congelado	Entrada analógica congelada (Frozen) 32 bits con tiempo	Flag 4; I32;;time
	04	Estático Congelado	Entrada analógica congelada (Frozen)16 bits con tiempo	Flag 4; I164;time
	05	Estático Congelado	Entrada analógica congelada (Frozen)32 bits sin tiempo	I32
	06	Estático Congelado	Entrada analógica congelada (Frozen) 16 bits sin tiempo	I16
	07	Estático Congelado	Entrada analógica congelada (Frozen) en punto flotante (Floating short)	Flag 4; FLT32
	08	Estático Congelado	Entrada analógica congelada en punto flotante (Floating long)	Flag 4; FLT64
32	01	Evento	Evento entrada analógica 32 bits sin tiempo	Flag 4; I32
	02	Evento	Evento entrada analógica 16 bits sin tiempo	Flag 4; I16

	03	Evento	Evento entrada analógica 32 bits con tiempo	Flag 4; I32;;time
	04	Evento	Evento entrada analógica 16 bits con tiempo	Flag 4; I16;time
	05	Evento	Evento entrada analógica en punto flotante (Floating short)	Flag 4; FLT32
	06	Evento	Evento entrada analógica en punto flotante (Floating long)	Flag 4; FLT64
	07	Evento	Evento entrada analógica en punto flotante (Floating short) con tiempo	Flag 4; FLT32;time
	08	Evento	Evento entrada analógica en punto flotante (Floating long) Con tiempo	Flag 4; FLT64;time
33	01	Evento congelado	Evento analógico congelado (Frozen) 32 Bits sin tiempo	Flag 4; FLT32
	02	Evento congelado	Evento analógico congelado (Frozen) 16 Bits sin tiempo	Flag 4; FLT64
	03	Evento congelado	Evento analógico congelado (Frozen) 32 Bits con tiempo	Flag 4; I32;;time
	04	Evento congelado	Evento analógico congelado (Frozen) 16 Bits con tiempo	Flag 4; I16;time
	05	Evento congelado	Evento entrada analógica congelado (Frozen) en punto flotante (Floating short)	Flag 4; FLT32
	06	Evento congelado	Evento entrada analógica congelado (Frozen) en punto flotante (Floating long)	Flag 4; FLT64
	07	Evento congelado	Evento entrada analógica congelado (Frozen) en punto flotante (Floating short) con tiempo	Flag 4; I32;;time
	08	Evento congelado	Evento entrada analógica congelado (Frozen) en punto flotante (Floating long) con tiempo	Flag 4; I16;time
34	01	Estático*	Objeto banda inerte (deadband ) reporte de entrada analógica 16-Bits	UI16
	02	Estático*	Objeto banda inerte (deadband ) reporte de entrada analógica 32-Bits	UI32
	03	Estático*	Objeto banda inerte (deadband ) reporte de entrada analógica en punto flotante.	FLT32

- Los objetos de entradas analógicas proporciona el valor de punto analógico a través de hardware o software.

- Los objetos de datos analógicos congelados representan el valor del punto en el tiempo del comando de congelamiento.
- Los objetos de cambios analógicos son generados cuando el valor de los cambios de un valor actual previamente reportado superan que el deadband configurado.
- Los objetos de eventos analógicos congelados son usados cuando un valor congelado es reportado como un evento.
- El grupo de objetos de variación 34 son para lectura o escritura de valores de deadband asociados con la generación de eventos de los puntos analógicos.

**TABLA N° 4.22 Objetos de Salidas Analógicas**

Grupo	Var	Tipo	Descripción	Estructura
40	01	Estático	Estados de salidas analógicas 32 bits	Flag 5; I32
	02	Estático	Estados de salidas analógicas 16 bits	Flag 5; I16
	03	Estático	Estados de salidas analógicas punto flotante (Short Floating)	Flag 5; FLT32
	04	Estático	Estados de salidas analógicas punto flotante (Long Floating)	Flag 5; FLT64
41	01	Estático	Bloque de salidas analógicas 32 bits	I32; Cod. de estado
	02	Estático	Bloque de salidas analógicas 16 bits	I16; Cod. de estado
	03	Estático	Bloque de salidas analógicas en punto flotante (Short Flotaing)	FLT32; Cod. estado
	04	Estático	Bloque de salidas analógicas 16 bits (Long Flotaing)	FLT64; Cod. estado

- Los objetos de estados de salidas analógicas representan el valor actual de la salida.
- Los objetos de bloques de salidas analógicas son usados para controlar los valores de las salidas analógicas. Estos contienen los valores finales, es decir, valores escalados antes de ser aplicado a la salida actual.

**TABLA N° 4.23 Objetos de Fecha y Hora**

Grupo	Var	Tipo	Descripción	Estructura
50	01		Fecha y Hora	Hora
	02		Fecha y hora con intervalo	Hora; T32
51	01		Fecha y hora CTO	Hora
	02		Fecha y hora no sincronizada CTO	Hora
52	01		Retardo de hora	UI16
	02		Retardo de hora fina	UI16

- El objeto de fecha y hora esta representado por un entero 48 bits sin signo (48 bits unsigned)
- La fecha y hora con objeto de intervalo puede ser usado para proporcionar un inicio de hora y un intervalo de repetición.

- El objeto de fecha y hora CTO (tiempo común de ocurrencia) es usado con otros objetos que contienen referencias de tiempo relativo y pueden conjuntamente ser utilizados para determinar el tiempo absoluto.
- La fecha y hora no sincronizada es guardada en una Estación Secundaria, donde la hora actual no ha sido actualizada por la Estación Master.
- El retardo de hora puede ingresado en segundos y horas (0 – 65535 s, y hasta 18 horas).
- El retardo fino puede ser ingresado en milisegundos y segundos (0-65535 ms; y hasta 65 segundos).

**TABLA N° 4.24 Objetos de Clases**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
40	01	No	Datos clase 0	No aplicable,
	02	usado	Datos clase 0	
	03		Datos clase 0	
	04		Datos clase 0	

Los objetos clases son diferentes a todos los objetos previamente descritos por que estos son usados en los mensajes de solicitud para llamar a los objetos de una clase específica. Estos no transportan información y por esta razón no tienen una estructura de información. Clase es un atributo que puede ser asignado a los elementos de información, incluyendo tipos de objetos, variaciones específicas o alguna combinación de estas, y puede ser utilizado para implementar un sistema de prioridades. Los niveles de prioridad indicados por DNP3 son las siguientes.

Clase	Prioridad
1	Alta
2	Media
3	Baja
4	Sin prioridad

**TABLA N° 4.25 Objetos de archivos**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
70	01		Identificador de archivo	Formato libre
80	01		Indicadores internos	
81	01		Objeto de almacenamiento	
82	01		Perfil de dispositivo	
83	01		Objeto de registro privado	
	02	Estático	Descripción de objeto de registro privado	

- El objeto identificador de archivo es un objeto de formato libre que es enviado en un mensaje de solicitud, y es utilizado para transferir grandes bloques de datos que no forman parte de otros objetos de datos definidos. Esto es adecuado para manejar archivos de configuración para dispositivos remotos.

**TABLA N° 4.26 Objetos de Dispositivos**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
80	01		Indicadores internos	Encapsulado binario
81	01		Objeto de almacenamiento	
82	01		Perfil de dispositivo	
83	01		Objeto de registro privado	
	02	Estático	Descripción de objeto de registro privado	

Los indicadores internos son flags dependientes de los dispositivos utilizados para transmitir el estado de una estación secundaria. Estos indicadores son diferentes a los bits del campo del doble-byte (INN) en la cabecera del mensaje de aplicación para los mensajes de respuesta.

Objeto de almacenamiento proporciona el estado de los buffers, colas (consultas), u otras áreas de almacenamiento de la estación secundaria. Las referencias de grupos y variaciones son proporcionadas para objetos de datos que representan un área particular de almacenamiento. La interpretación de los bits de estado es dependiente del dispositivo y están especificados en el perfil del dispositivo.

El objeto Perfil de dispositivo esta dirigido para proporcionar un mecanismo de configuración dinámica de una Estación Master para aceptar un nuevo dispositivo.

El perfil de dispositivo es enviado por una estación secundaria cuando recibe un mensaje de solicitud que no puede interpretar. También, la Estación Secundaria puede ser configurada para enviar su perfil al inicio. El receptor del mensaje una Estación master puede podrá reconfigurar dinámicamente su base de datos para la Estación secundaria de modo que las comunicación a nivel de aplicación puedan funcionar correctamente.

El objeto de perfil de datos proporciona la siguiente información:

- Funciones soportadas por el dispositivo
- Lista de objetos soportados
- Cantidad de objetos
- Muestra de cabeceras de objetos

La estructura del objeto de datos es:

- Una cadena de 64 bits para representación de los códigos de función 0-63
- Un número binario de 16 bits que proporciona el número de cabeceras objetos
- Una secuencia de N objetos datos.

Objeto de registro privado (PRO) proporcionado para las estructuras específicas de los fabricantes. Sin restricción son ubicados en el contenido en el campo de datos de los objetos a discreción del fabricante.

El Objeto descriptor de objetos re registro privado proporciona una descripción del contenido de los objetos de datos PRO. La documentación del DNP3 debería ser usado para obtener información detallada.

**TABLA N° 4.27 Definición del Objeto de Aplicación**

<b>Grupo</b>	<b>Var</b>	<b>Tipo</b>	<b>Descripción</b>	<b>Estructura</b>
90	01		Identificar de aplicación	No Aplicable

El objeto de identificación de aplicación es usado para representar una aplicación o la operación del sistema en la Estación Secundaria.

### 4.5.2.6 Objetos Numéricos

**TABLA N° 4.28 Objetos Numéricos**

Grupo	Var	Tipo	Descripción	Estructura
100	01		Punto flotante corto (Short floating)	Flag 4; Unidades, valor definido
	02		Punto flotante largo (long floating)	Flag 4; Unidades, valor definido
	03		Punto flotante extendido	Flag 4; Unidades, valor definido
101	01		Código decimal binario pequeño	4xBCD
	02		Código decimal binario medio	8xBCD
	03		Código decimal binario largo	16xBCD

Los objetos de datos numéricos son usados para transmitir el valor de la información numérica calculada o real. Cada objeto incluye un flag (un octeto), código de unidad (un octeto), y si valor en su formato definido. Los números en punto flotante están de acuerdo con el estándar IEE-754 para representación de números en punto flotante.

La estructura de Flag es la siguiente.

7	6	5	4	3	2	1	0
---	---	---	---	---	---	---	---

Bit	Interpretación
0	En línea
1	Reinicio
2	Perdida comunicación
3	Dato forzado remotamente
4	Dato forzado localmente
5	Rango excedido
6	Check de referencias
7	Reservado

La documentación DNP3 proporciona la asignación de los siguientes códigos de unidad.

**TABLA N° 4.29 Asignación de códigos de Unidad DNP3**

0	Voltios Pico-pico	10	Frecuencia
1	Amperios pico-pico	11	Frecuencia rad/sec (w)
2	Voltios RMS	12	Temperatura C
3	Amperios RMS	13	Temperatura F
4	Potencia Real kW	14	Temperatura K
5	Potencia Aparente kVA	15	Fuerza in Neutons N
6	Potencia Reactiva Kva.	16	Masa kg
7	Energia kWh	17	Aceleración m/s <sup>2</sup>
8	Potencia Imaginaria kVARh	18	Presion N/m <sup>2</sup>
9	Factor de Potencia	19	Torque Neuton-metros

#### 4.6 Niveles de Sub Sets

Par obtener interoperatividad entre diferentes versiones de un protocolo de fabricantes es necesario asegurar que toda la implementación de fabricantes soportan los mismos objetos de datos y funciones. Sin embargo no resulta eficiente por que un pequeño IED podría requerir un pequeño subset de objetos de datos disponibles, mientras que un RTU concentrador de varios IEDs puede necesitar mucho más objetos. Estas ediciones están dirigidas a través de la definición de niveles de subset

Actualmente existen tres niveles definidos en DNP3. Estos están designados en el formato del protocolo de capa de aplicación.

Los niveles de aplicación son descritos en términos de las funciones principales definidos por cada nivel.

##### 4.6.1 Definición de Subset Nivel 1

Funciones de esclavo nivel 1

- lectura de objeto de clases
- Lectura de objetos de de datos de salidas analógicas y salidas binarias.
- Control de Operaciones para objetos de salidas analógicas y salidas binarias.
- Escritura para reiniciar el bit indicador interno.
- Reinicio en frío
- Medición de retardo
- Escritura de tiempo

### Funciones Master nivel 1

- Eventos y entradas binarias
- Eventos contadores y contadores
- Eventos y entradas analógicas
- Estados de salidas analógicas y binarias

El master nivel 1 debe muchos objetos para tener la capacidad de comunicarse con varios dispositivos esclavos, por lo que necesitara un gran arreglo de funciones. Un esclavo nivel 1 no requiere generarlos.

#### 4.6.2 Definición de Sub-Set Nivel 2

Funciones de esclavo nivel 2 adicional al nivel 1

- Acepta solicitud de congelamiento en objetos contadores binarios
- Solicitudes de lectura para variación 0 (todas las variaciones) para algunos objetos.
- Solicitudes de lectura para variaciones 1,2, y 3 de objetos de cambios binarios.
- Pueden responder a solicitudes de congelamiento de objetos contadores.
- Pueden enviar respuestas no solicitadas conteniendo datos estáticos.
- Las funciones Master Nivel 2 son las mismas que del nivel 1

#### 4.6.3 Definición de Sub-Set Nivel 3

Funciones de nivel 3 adicional a los niveles 1 y 2

- El esclavo procesara solicitudes de datos para varios objetos específicos y variaciones.
- Habilita o deshabilita respuestas no solicitadas por clases (clase1, clase2, y clase 3) y asigna dinámicamente clases a objetos de datos.

El documento del perfil del dispositivo es un instrumento del DNP3 para la interoperatividad entre dispositivos y sistemas. Este es un documento esta referido principalmente al nivel de aplicación y enlace de datos y debe ser proporcionado por el fabricante del dispositivo o sistema en conformidad con el estándar DNP3.

El documento del perfil de dispositivo consta de las siguientes secciones:

- Perfil del dispositivo
- Tabla de implementación
- Lista de puntos (opcional)

El Perfil de dispositivo contiene las siguientes partes:

- Identificación del fabricante y dispositivo
- Niveles soportados por el dispositivo
- Función del dispositivo

Para asegurar la interoperatividad de un sistema DNP con todos sus componentes y partes, incluyendo Master, RTUs y IEDs, es necesario examinar la documentación del perfil para cada dispositivo.

El **ANEXO C** muestra un ejemplo de la documentación del perfil DNP de nivel 2 de un dispositivo del Fabricante General Electric.

#### **4.7 Recomendaciones y Reglas de Implementación**

En esta sección se resume las reglas y recomendaciones difundida por el documento de definición de Subset DNP3.

##### **4.7.1 Eventos y clases de datos**

En DNP el método más simple de referenciar datos en las solicitudes es llamar objetos por clases y es fundamental asumir que el nivel mas bajo dependa del uso de las llamadas por clases para obtener muchos objetos. Esto sugiere que todos los dispositivos tengan sus datos estáticos asignados a la clase 0, y todos los eventos asignados a una de las otras clases.

a) Los dispositivos nivel 3 deben permitir a una estación master habilitar o deshabilitar reporte de eventos para un punto, para ello deberá asignar al punto clases de datos requeridas 1, 2, o 3., pero no clase 0. La clase 0 es asignada por defecto solo a los puntos de datos estáticos.

b) Los dispositivos clases 1 y 2 no requieren habilitar o deshabilitar reporte de eventos por la master. Para estos dispositivos es necesario la asignación de variación por defecto. Esto significa que el dispositivo esclavo debe enviar la variación por defecto y debe permitir ser configurado.

c) El dispositivo esclavo debe preservar el orden de secuencia de eventos para que cuando una solicitud de datos llama por múltiples clases, los eventos no deben ser enviados por grupos si no por la secuencia de ocurrencia.

d) Las siguientes acciones deben suceder cuando un dispositivo es iniciado.

- En el dispositivo iniciado el bit IIN=1

- Si es configurado para respuestas no solicitadas, debe enviar una en el inicio.

- Esta respuesta puede no contener datos o todos los datos estáticos
  - Esta respuesta puede también contener datos de eventos no reportados.
- e) Es recomendable que si un dispositivo no reporta todos sus datos estáticos en el inicio, el Master debería inmediatamente solicitar todos los datos estáticos y eventos.
- f) Las Respuestas no solicitadas son soportados:
- La documentación del perfil deberá indicar que objetos y funciones puede usar este modo de operación.
  - EL uso de respuestas no solicitadas podrá ser configurada en OFF
  - El Marte debe poder dinámicamente deshabilitar usando un una solicitud de deshabilitación (código de función 21)

#### **4.7.2 Operación de Salidas Binarias**

Todos los dispositivos esclavos deberán realizar operaciones en bloques de salidas por relé. Todos los dispositivos deberán realizar todos los códigos de función de salidas y tipos de control ejemplo Select/Operate, y pulse ON.

Usar solicitudes de escrituras binarias no es recomendable por que no hay realimentación del suceso de la operación. El método recomendable es usar control de bloques de salidas por relé.

Si es utilizada escritura directa entonces una realimentación de un estado binario debería ser usado.

#### **4.8 Pruebas de Conformidad**

EL DNP tiene procedimientos detallados de procedimientos de pruebas de certificación de conformidad detallados especificados y conservados por el grupo de usuarios DNP3. Es importante indicar que los procedimientos de certificación están enfocados en los mínimos requerimientos para la implementación en los IEDs más que en el nivel de SCADA master. Si bien, estos procedimientos aseguran la conformidad e interoperatividad de dispositivos certificados para el nivel 1 o nivel 2, esto no asegura las características y funciones en estos niveles.

La especificación del protocolo esta esclarecido por los procedimientos de certificación definidos en la siguiente documentación.

- Capa de enlace de datos DNP versión 3.00
- Funciones de transporte DNP versión 3.00`

## **CAPITULO V**

### **COMUNICACIÓN DNP 3.0 A TRAVÉS DE UNA RED GPRS PARA UN SISTEMA DE DISTRIBUCION DE AGUA POTABLE**

#### **5.1 Introducción**

La empresa de servicio de distribución de Agua Potable Sedapal con la finalidad de mejorar su servicio utiliza sistemas de control y supervisión de sus Estaciones Remotas distribuidas en la red de distribución de agua potable.

Las Estaciones Remotas ERs estan equipadas con sensores hidráulicos, analizadores de energía, equipos de respaldo de suministro eléctrico, y equipos de automatización que permiten su control y supervisión.

La Estación Maestra SCADA es el centro de operaciones donde se recibe y procesa toda la información enviada por los equipos de automatización de las ERs a través de un sistema de comunicaciones de radio en banda licenciada.

#### **5.2 Antecedentes**

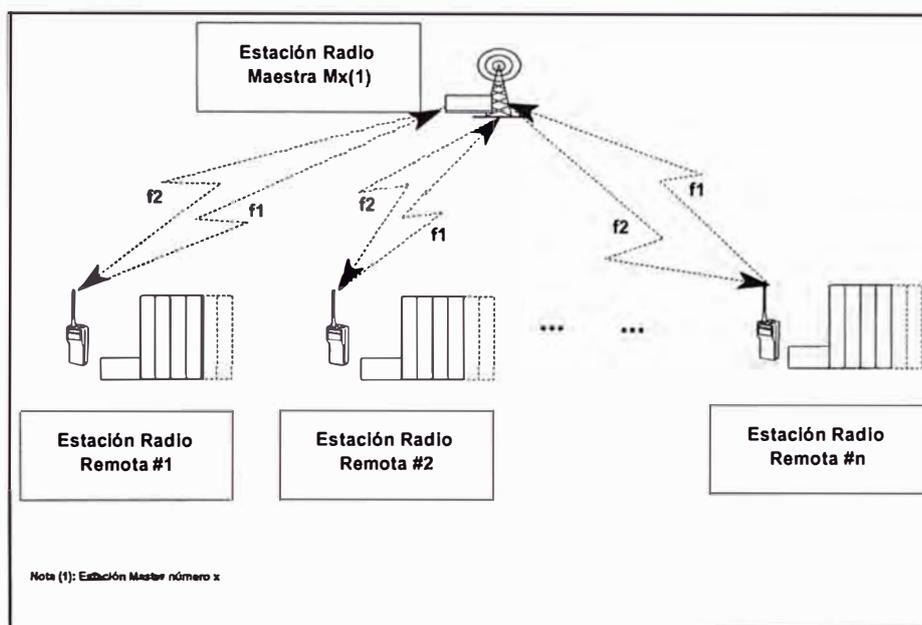
El proyecto de Comunicación DNP3 a través de una Red GPRS surgió ante la necesidad de mejorar la comunicación y contar con una nueva alternativa de comunicación entre el Centro de Control y las Estaciones remotas (Pozos, Reservorios, Cámaras de Rebombeo, Cámaras de Regulación) controladas y monitoreados por PLCs instalados en campo. El sistema SCADA anterior utiliza el protocolo de comunicaciones MODBUS, el cual por su diseño nativo carece de un esquema de reporte por excepción y del tiempo que se le agrega a cada cambio de estado en el momento en que ocurrió el evento (timestamp). Además, el esquema de comunicación bajo este protocolo se basa únicamente en el de interrogaciones constantes del dispositivo maestro a los dispositivos esclavos en intervalos de tiempo definidos esto obligo a buscar una nueva alternativa para obtener mayor rapidez en la recepción de la información de campo.

El sistema de comunicaciones existente está constituida por un conjunto de grupos punto-multipunto (celdas), cada uno de ellos gobernado por una Estación Radio Maestra y con

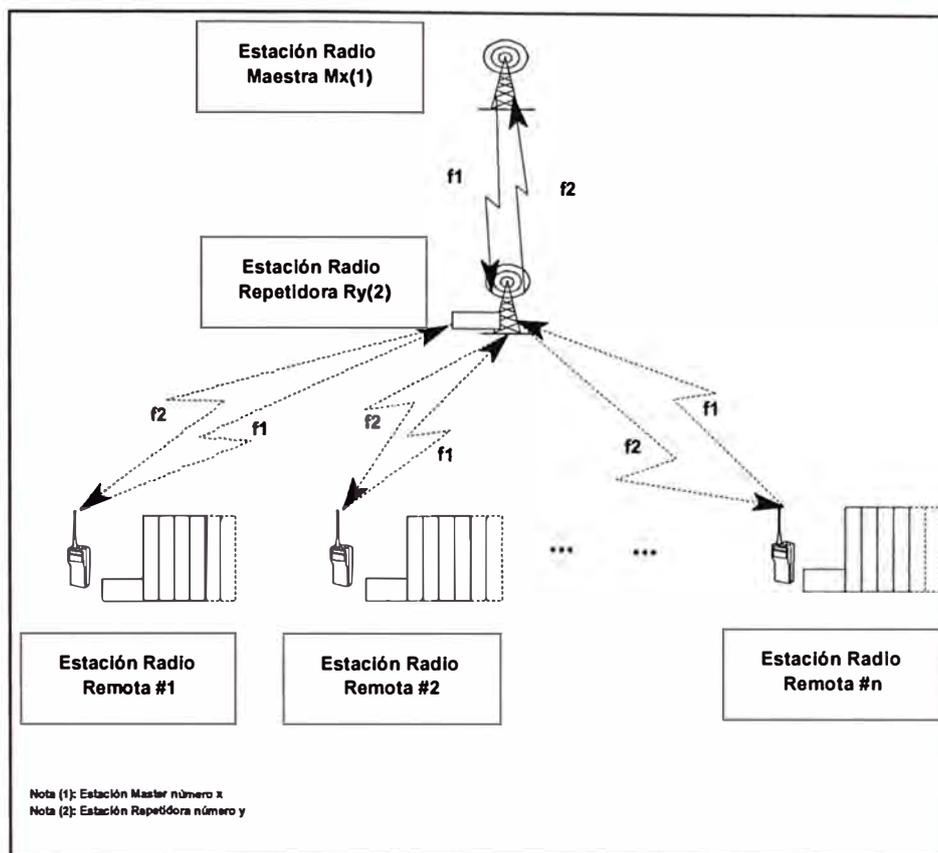
varias Estaciones Radio Remotas. En algunas de estas celdas se utilizarán radios repetidoras para enlazar las Radios Master con las Radios Remotas.

Cada grupo o celda forma una zona de comunicaciones de datos independiente bajo el protocolo Master-Esclavo Modbus.

EL sistema de comunicaciones esta conformado por una combinación de celdas tienen alguna de las dos topologías que se presentan a continuación:



**Fig. 5.1 Celda con cobertura directa desde Radio Maestra**



**Fig. 5.2 Celda con cobertura desde Radio Repetidora**

**Tabla 5.1: Características de Red**

<b>Características de red</b>	<b>Descripción</b>
Tipo de red	Red formada por ocho (8) celdas radio, funcionando cada una de ellas a dos frecuencias. Modo de comunicación half-duplex y funcionando bajo un esquema de polling, aceptando mensajes no solicitados
Plan de frecuencias	Frecuencias (f1, f2) entre 400 y 512 MHz, una para transmisión y otra para recepción, por lo que en total se requieren 8 pares de frecuencias (16 frecuencias).
Tipo de emisión	Modulación FSK a 9.600 bps.
Protocolo	Propietario (Modicon Modbus), Master-Slave, con la funcionalidad Master temporal para que los emplazamientos remotos puedan emitir mensajes no solicitados.
Equipos de Radio	Radios Master: MDS 4710 de Adaptive Broadband Radios Repetidores: MDS 4790 de Adaptive Broadband Radios Remotas: MDS 4790 de Adaptive Broadband

### **5.3 Descripción y Justificación del Sistema Implementado**

El nuevo Sistema de Automatización y Telecontrol de las instalaciones de las redes primarias de distribución de agua potable de Lima metropolitana permite la operación y control de los equipos de las redes hidráulicas de producción y distribución ubicados parcialmente en el área de los distritos de Vitarte y Puente Piedra. Dichos equipos se distribuyen en estaciones remotas de distintos tipos según función y tipología:

- Bombes
- Entradas a Sector
- Reservorios
- Pozos
- Válvulas de Control

El nuevo sistema de control y supervisión permite la operación desde tres centros de control, el principal (CCP) situado en la planta de La Atarjea, y dos Centros de Control Zonales (CCZ) en los Centros de Servicio de Ate Vitarte y Comas, conduciendo los datos en tiempo real de las estaciones remotas y conduciendo los comandos originados en los centros de control hasta las estaciones remotas.

El control está distribuido entre:

- Elementos de control local, tanto controles manuales desde armarios eléctricos de mando como controles gestionados por programas de PLC.
- Supervisión y operación global, con gestión centralizada en servidores SCADA y de Base de datos y con operadores responsables de centros de servicios que abarcan grupos de estaciones de control local.

Para completar la funcionalidad del sistema, se utiliza la tecnología celular GPRS y protocolo DNP3 para establecer el enlace de las ERs con el Centro Principal de Control de La Atarjea.

Este nuevo esquema de comunicaciones con la plataforma GPRS debe controlar el manejo del ancho de banda es decir el uso de canales para disminuir los costos del servicio pero sin perder la rapidez de recepción de la información de campo; de esta forma se necesitaba un esquema en el cual los dispositivos esclavos reportaran espontáneamente la ocurrencia de eventos sin necesidad de interrogarlos constantemente.

Estas características básicas y muy importantes, se encuentran presentes en el protocolo de comunicaciones DNP 3.0, las cuales permiten que el operador del sistema, sea capaz de enterarse de los eventos en un tiempo muy cercano al tiempo de ocurrencia, y conocer con precisión cual fue el primer evento en generarse, lo que permite realizar análisis mas fidedignos en caso de fallas y además tiene la versatilidad de soportar el reporte de datos mediante interrogaciones o espontáneamente.

#### **5.4 Descripción del Sistema de Comunicación GPRS y Protocolo DNP 3**

GPRS son las siglas de General Packet Radio System, Sistema General de Transmisión de Datos mediante Paquetes de Información.

El protocolo GPRS es un protocolo de nivel tres, transparente para todas las entidades de red comprendidas entre el modem y el nodo de red más cercano; las entidades entre las que se establece una conexión a este nivel están localizadas en el modem y en el nodo de red.

Este protocolo soporta tanto el intercambio de informaciones de control como de paquetes PDP-PDU (Packet Data Protocol - Protocol Data Unit) entre el modem y el nodo de red al que éste está conectado (los PDP-PDU están, encapsulados en las tramas GPRS).

Al contrario que el servicio de transferencia de datos con modalidad de conmutación de circuito, en el que cada conexión establecida se dedica sólo al usuario que la ha solicitado, el servicio GPRS permite la transmisión de paquetes en modalidad link by link, es decir, los paquetes de información se encaminan en fases separadas a través de los diversos nodos de soporte del servicio, denominados GSN (Gateway Support Node).

Así, una vez que un paquete ha sido transmitido por el interfaz de radio, se vuelven a liberar los canales, que así pueden ser utilizados por algún otro usuario.

El estándar GPRS tiene una serie de ventajas respecto a generaciones anteriores de comunicación, estas ventajas son:

**Costo:** En GPRS el sistema de facturación empleado no va en función del tiempo de conexión, sino en función de la información descargada por el usuario. Esta forma de facturación permite que la conexión sea más prolongada, ya que al usuario sólo se le factura en función de los datos que haya usado. De hecho una de las características del GPRS es la de ser un sistema “always on” (siempre conectado), similar a ADSL en las conexiones a Internet terrestres, ya que el usuario siempre tiene disponible la información.

**Rapidez:** Con GPRS el acceso a Internet o a una Intranet puede contarse a una velocidad promedio de 40 Kbps

**Eficacia:** La ganancia en eficacia con GPRS no sólo se produce por el óptimo aprovechamiento de la red, sino también porque se abre la puerta a nuevas posibilidades tales como el envío de datos a mayor velocidad que con redes anteriores.

**Seguridad y fiabilidad en la transferencia de la información:** GPRS permite la detección robusta de errores y la capacidad de corrección, lo que asegura que los datos sean transmitidos en forma segura y completa.

El sistema celular GPRS con estándares de TCP/IP y UDP/IP en combinación con el protocolo DNP3 en aplicaciones de sistemas de telecontrol ofrece las siguientes ventajas:

- Comunicación por excepción y reporte de mensajes no solicitados.
- Velocidad de transmisión de datos optima para datos de telemetría y control.
- No requiere el uso de antenas directivas de fácil instalación.
- El Costo del servicio GPRS depende de la cantidad de datos que se transmiten y Reciben por Terminal de datos.
- El protocolo DNP 3.0 permite direccionar más de 65000 dispositivos con direcciones diferentes.
- La segmentación en múltiples tramas en el mensaje de respuesta para disminuir los errores y la pérdida de datos, y el envío de mensajes sin solicitud previa (Mensajes No Solicitados).

## **5.5 Arquitectura del Sistema de Comunicaciones**

### **a) Enlace equipos de automatización PLCs – Convertidor de Protocolo - Modem GPRS.**

En cada ER se dispone de un Convertidor de protocolo Modbus/DNP que recopila la información del PLC mediante una conexión serial RS232 vía protocolo ModBus RTU, y envía la información en protocolo DNP3 hacia el CCP de Sedapal.

En el Convertidor de protocolo DNP3 se configura el modo de reporte espontáneo para optimizar el uso de los canales de comunicaciones de la Red Celular GPRS. Para establecer esta configuración se realizó un cálculo aproximado del volumen de datos mensual conforme se indica en el numeral 5.5.1.

### **b) Enlace equipos Modem GPRS – Red GPRS**

Los módems se enlazan a la red celular GPRS para realiza el enrutamiento de los datos correspondientes a cada ER con la dirección IP de cada modem remoto y dirección IP destino (Servidor SCADA), evitando así la difusión masiva de paquetes de datos a todas las ERs.

### **c) Enlace a la red GPRS – CCP SEDAPAL**

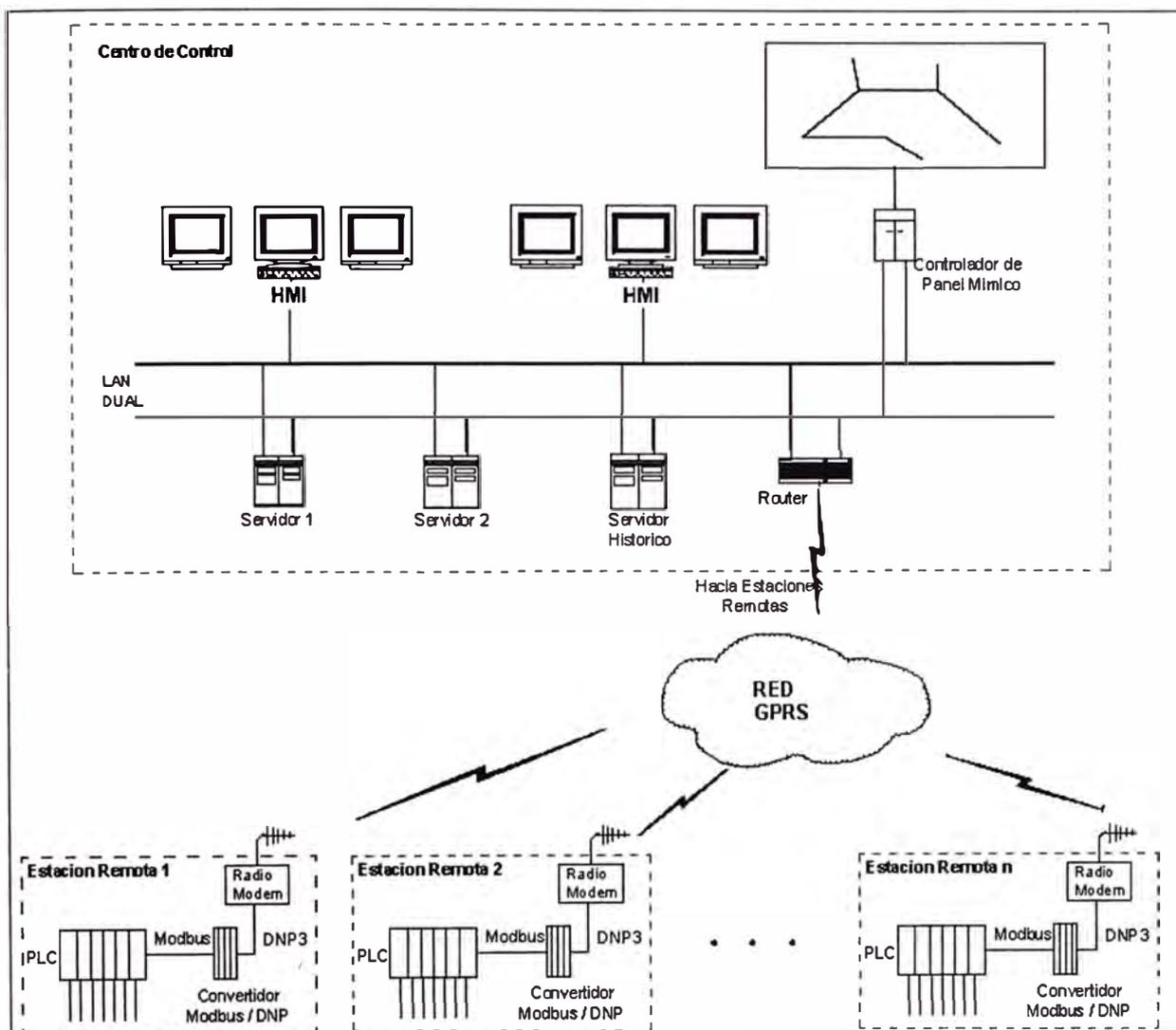
La Información SCADA de todas las ERs es canalizada por un enlace de banda ancha de capacidad E1 (2.048Mbps) hasta el Cerro Santa Rosa de la Atarjea-Sedapal. Este enlace es proporcionado por el Proveedor de Comunicaciones GPRS.

La interconexión entre la red del proveedor de comunicaciones en el cerro Santa Rosa conexión y la Red LAN del CCP de Sedapal es mediante un enlace de Fibra Óptica Ethernet.

### **d) Enlaces de Microondas entre el CCP de La Atarjea y los Centros de Servicio Comas y Vitarte.**

Se utiliza la red de Microondas existente entre el CCP de La Atarjea y los Centros de Servicio Comas y Vitarte para conectar sus nuevas Estaciones de Operación con los servidores SCADA. Este enlace permitirá la transmisión de datos de los Servidores SCADA hacia dichas Estaciones de Operación para presentadas mediante la interfaz grafica.

La Fig. 5.1 Muestra la arquitectura de un sistema SCADA utilizando el protocolo de comunicación DNP3 a través de la red GPRS.



**Fig. 5.1. Arquitectura Sistema SCADA**

Tabla 5.2: Características de Red GPRS en el Proyecto

Características de red	Descripción
Tipo de red	Red formada por (17) islas, cada isla agrupa los datos de un grupo de Estaciones Remotas, y mediante un MODEM GPRS en la Estación principal de cada isla se transmite los datos al CCP.
Plan de frecuencias	Frecuencias licenciada para el servicio GSM 1900MHz
Protocolo	Estándar DNP3, Master-Slave, con la funcionalidad de reporte espontáneo para que los emplazamientos remotos puedan emitir mensajes no solicitados.
Equipos de Radio	Modem GPRS Airlink: G3211 clase 8

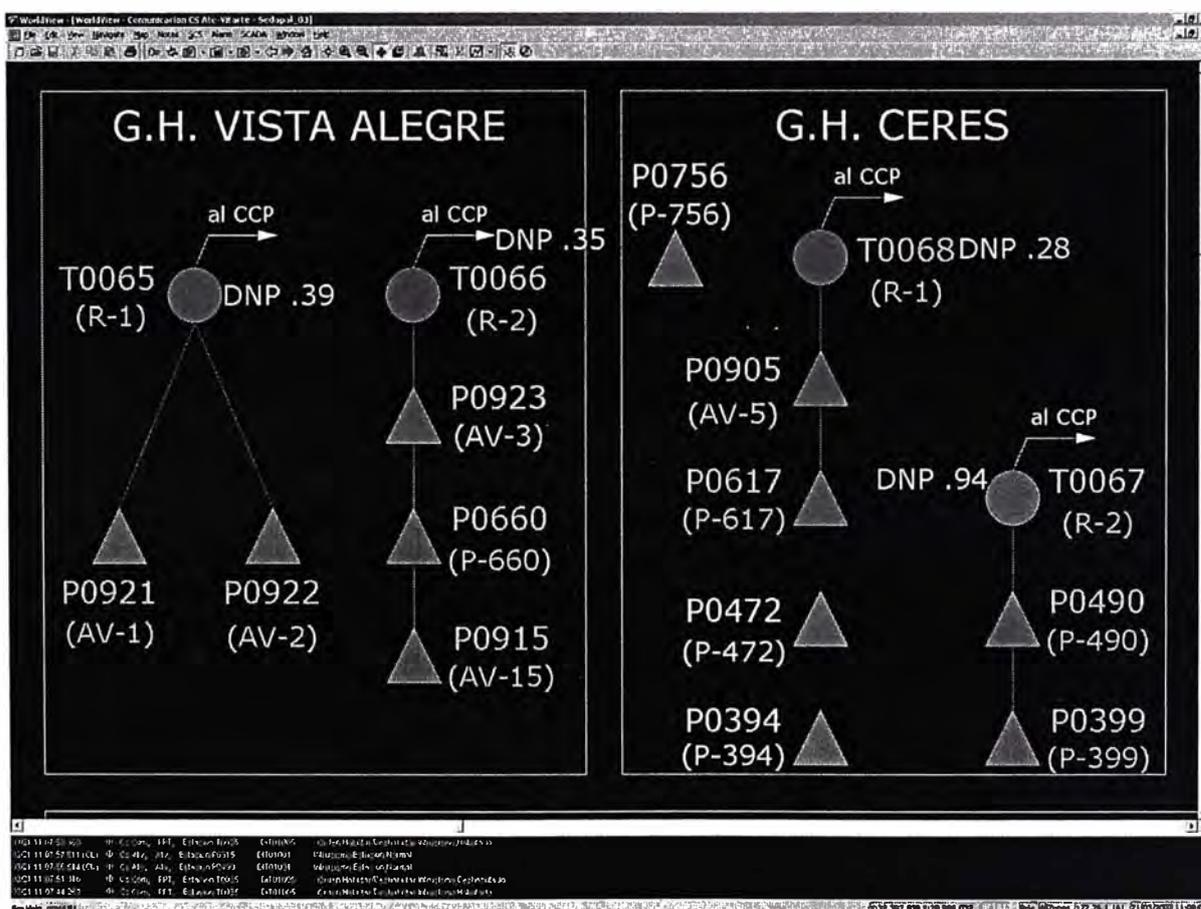


Figura 5.2: Configuración de la Topología de Islas o Grupo de Estaciones Remotas

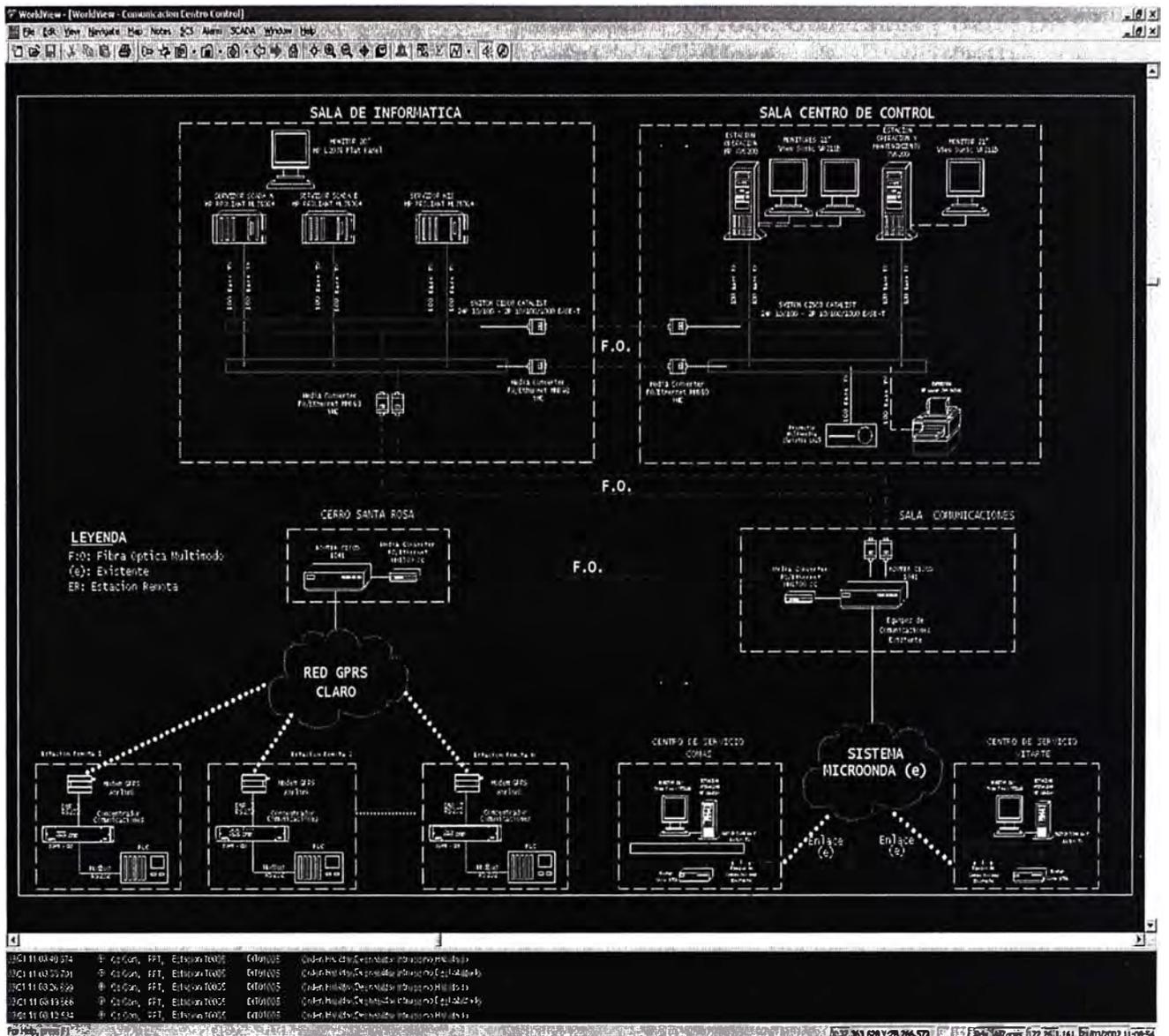


Figura 5.3: Arquitectura General del Sistema SCADA

### 5.5.1 Resultados del Cálculo del Volumen de Datos por la Red GPRS.

Para el cálculo del volumen de datos enviados y recibidos con DNP3 por Estación Remota se utilizó el aplicativo Ethernet y el analizador de protocolos ASE2000. El resultado obtenido se cotejó con el resultado del sistema de Facturación (Billing) del proveedor del servicio obteniéndose un margen de alrededor error de 3%.

En la Tabla 5.2 Resume el cálculo del número totales de MB con DNP3 para tres tipos de Estación Remota.

Tabla 5.2

Tipo Estación	Variables		Periodo de Encuesta (min)	Nro de Eventos Prom. Generados /Hora	Total de Datos DNP3 (MB)
	Estados	Analógicos			
Pozo	67	51	5	20	3.8
Reservorio	36	45	10	20	3.3
Bombeo	76	83	15	20	5.1

También se realizó el cálculo del Volumen de Datos usando Protocolo Modbus para las mismas estaciones remotas obteniéndose en total 10.7MB con una frecuencia de consultas (polling) de 30 Segundos.

### 5.6 Beneficios y Facilidades del Sistema

Actualmente la implementación de esta forma de comunicación incluyendo el DNP con Respuestas No Solicitadas en la plataforma GPRS ha traído una variedad de beneficios tanto operativos como económicos que no se tenían con el protocolo MODBUS entre los cuales tenemos:

- La nueva arquitectura del sistema de comunicaciones permite tener menores tiempos en la actualización de la información de campo en el sistema SCADA.
- EL Servicio GPRS ofrece ventajas económicas en relación al sistema de comunicación en banda licenciada por tener un costo razonable en la facturación mensual por Estación Remota, además evita gastos operativos en mantenimiento, estudios de factibilidad, uso de repetidoras, costos de canon que demandan todo sistema en banda de frecuencia licenciada.
- Respuesta rápida de los eventos que ocurren en campo sin la necesidad de interrogar por ellos. El reporte de eventos por parte de los equipos ubicados en campo se redujo a segundos supervisando varias Estaciones en comparación con la comunicación MODBUS en que el reporte de datos era en el orden mayor a los 5 minutos debido a que se debía configurar el tiempo de interrogaciones mayor a este valor para reducir el costo GPRS.
- Se pudo incrementar el número de puntos a supervisar por Estación debido que la cantidad de Bytes transmitidos y recibidos se redujo substancialmente.
- El conteo de Bytes transmitidos/recibidos en el canal GPRS de acuerdo con la facturación de la empresa suministradora del servicio arrojó un resultado promedio de 5.1 MBytes en el peor de los casos, alrededor de 6.6 MBytes menos de los que se tiene

si la comunicación sería con MODBUS, lo que condujo a una reducción de los costos de alrededor de 50% esto se puede ver en la tabla 5.4.

**TABLA N° 5.4**

CF con IGV	CF sin IGV	Unidades libres		Tarifa adic. Sin IGV.		Tarifa adic. Con IGV	
		MB	Kb	Kb adic.	MB adic.	Kb adic.	MB adic.
S/. 35.00	29.41	5	5120	0.006721	6.882353	0.007998	8.19
S/. 70.00	58.82	11	11264	0.006557	6.714286	0.007803	7.99
S/. 100.00	84.03	18	18432	0.006385	6.537815	0.007598	7.78

(\*) para los casos que se requiera conexión ILIMITADA se considerará S/. 140.00 nuevos soles.

- Fácil configuración y mantenimiento del protocolo DNP3 facilitando a que el usuario del equipo convertidor de protocolo pueda hacer el mantenimiento de los mismos con la mínima ayuda de la empresa integradora disminuyendo así los costos por servicio de mantenimiento de los equipos.
- Facilidad de hacer mantenimiento remoto teniendo una PC, conectado a la red del Centro de Control o un módem GPRS configurado para monitorear los otros módems, y el software de configuración amigable y disponible en Internet, disminuyendo igualmente los costos de mantenimiento al ser el mismo usuario el que la realiza.

## CONCLUSIONES

- 1 La importancia de los estándares en los sistemas SCADA permite la interoperatividad entre sistemas y dispositivos de distintos fabricantes, esto beneficia al usuario porque no dependerá de un solo suministrador de sistemas.
- 2 Sus características de protocolo abierto y seguro lo convierten al DNP3 en un protocolo fuertemente aceptado por muchos fabricantes de dispositivos y sistemas especialmente en la industria eléctrica.
- 3 Las exigencias del grupo de usuarios DNP para la aceptación y aprobación del protocolo DNP3 garantizan la funcionalidad, interoperatividad entre sistemas y dispositivos y la constante evolución del protocolo para adaptarse a las nuevas tendencias en comunicaciones.
- 4 La comunicación DNP 3.0 utilizando Respuestas no Solicitadas a través de una red GPRS reduce considerablemente los costos de éste servicio, a su vez la combinación del DNP 3.0 y GPRS involucra al protocolo de comunicaciones más confiable y avanzado en el área de automatización con una red inalámbrica muy segura que tiene bajo costo y facilidad en la instalación y mantenimiento.
- 5 Entre otros beneficios de esta combinación entre DNP y GPRS se tiene la gran velocidad de transmisión, una disminución considerable de errores en los datos, gran versatilidad para adaptarse a los equipos de automatización que comuniquen DNP 3.0.
- 6 EL Servicio GPRS ofrece ventajas económicas en relación al sistema de comunicación en banda licenciada evitando así gastos operativos en mantenimiento, estudios de factibilidad, uso de costosas repetidoras, costos de canon que demandan todo sistema en banda de frecuencia licenciada. Sin embargo, el sistema de comunicación esta sujeto al grado de confiabilidad y disponibilidad que ofrece la empresa que ofrece el servicio de comunicaciones GPRS.

## **ANEXOS**

**ANEXO A**  
**TERMINOLOGIA**

**Tabla A.1 Terminología**

Item	Termino	Descripcion
1	<b>Chatter Filter</b>	A facility that s used to disable a digital input point if the number of state changes of that point during a defined time interval is excessively high
2	<b>Chatter Filter</b>	A facility that s used to disable a digital input point if the number of state changes of that point during a defined time interval is excessively high
3	<b>Clear Time</b>	The amount of time that the select relay will operate after the master trip or close has operated.
4	<b>Control Arm Time-out</b>	The maximum amount of time that a device will wait to receive an execute command after receiving an arm command.
5	<b>Debounce Period</b>	The amount of time for which the state of a digital input point shall be detected in a valid “on” or “off” condition before it is considered to be in that position
6	<b>Diagnostics</b>	Programs automatically executed in an IED, at predetermined intervals, to check the health of the device.
7	<b>Double-point Accumulator</b>	.1): A pair of digital input points that can assume four different states. States 1 and 2 may be described as NORMAL or VALID states, and states 3 and 4 may be described as ABNORMAL or INVALID states. Purpose is to detect and count complete changes of state (transitions), while ignoring any incomplete transitions.
8	<b>Form A Counters</b>	A single-point type of digital input that counts rising-edge changes of state (or transitions).
9	<b>Form C Counters</b>	A pair of digital inputs that counts the transitions from one valid state to the next valid state, while ignoring any transitions to invalid states
10	<b>Form A</b>	Counts rising edge transitions
11	<b>Form C</b>	2 inputs, counts when both change to the opposite state (1 on, 1 off).
12	<b>Host Name</b>	On an IP network, an arbitrary name used as an alias for a network device’s address
13	<b>Host Table</b>	A list of all Host Names of all IP network devices that is maintained by each device on the network
14	<b>Lock-out Period</b>	A parameter that defines the length of time that a device or point will be disabled from operation after exceeding a pre-defined error condition
15	<b>PING</b>	Acronym for Packet Internet Groper, a utility that can test the “reachability” of destinations on an IP network. It uses an ICMP echo request, and waits for its reply.
16		

17	<b>Pseudo Points</b>	System data points generated internally by a software application. They often represent the results of a calculation, or the internal state of a process
18	<b>Recloser</b>	Abbreviated name for automatic circuit recloser
19	<b>Scan (interrogation)</b>	The process by which a data acquisition system interrogates RTUs for points of data. See also polling (data request).
20	<b>Scan cycle</b>	The time in seconds required to obtain a collection of data (e.g. all data from one RTU, all data from all RTUs, or all data of a particular type from all RTUs)
21	<b>Scan Enable</b>	A feature that allows or disallows a particular input point to be scanned
22	<b>Select Before Operate</b>	Two-part command sequence for high communications security and hardware verification before the control is actually executed.
23	<b>Software Debouncing</b>	A method used to determine whether a digital input has actually changed state, or whether a perceived change of state was actually contact bounce or other line
24	<b>Latency</b>	The time between when sensor outputs are present at the physical interface of a measuring device until its value is available to the first user or program
25	<b>Accuracy</b>	The difference between the actual value of a measurement and the indicated value of the measurement. Accuracy is usually expressed in terms of percentage deviation from a reference value, commonly full scale of the measuring device and less commonly the actual value at the input. Note that accuracy for power measurements must be expressed with a applicable power factor range. ( Real power measured at less than 10% power factor or reactive power measured at greater than 90% power factor tend to have significant errors) Note also that if the “measuring device” is a current transformer, its full scale rating may be significantly larger than the displayed value (e.g., a 3000 ampere 0.3% CT measuring a 300 ampere load current). In this case, its accuracy is $0.3 \% \times 3000$ or $\pm 90$ amps, so the display of a 300 amp load is actually $300 \pm 90$ amps or $\pm 30\%$ of the measured value
26	<b>Update Periodicity</b>	The unit time between updates, sometimes expressed as the rate at which a measurement is updated (frequency)
27	<b>Time Skew</b>	The elapsed time between when the first value in a set of measurements is taken until the last value of the same set of measurements is taken. The data set may consist of measurements made in a close proximity, as within a single substation, or across a large geographic area as in the flow measurements for a large transmission network
28	<b>Resolution</b>	The smallest increment of a value that can be resolved, often expressed as percent of full scale. It is better expressed in engineering units of the measured value. A displayed value (printed or on a CRT) should be no more precise than its resolution
29	<b>Availability</b>	The measure of time a parameter measurement is available to users and algorithms. It is customary to express Availability in percentage

		of uptime plus downtime, usually as 99.xxx where xxx is an expressed fraction of a percentage point. It is sometimes more useful to express unavailability as a maximum period of time during which the variable is unavailable, e.g. 4 hrs per month. Availability = $\text{uptime}/(\text{uptime} + \text{downtime})$ .
30	<b>Unavailability</b>	The ratios of downtime to uptime, or $\text{downtime}/(\text{uptime} + \text{downtime})$
31	<b>Single point/multiple point</b>	Control of a single point versus global control of multiple points

**ANEXO B**  
**TABLAS DE REQUERIMIENTOS BÁSICOS DE EVALUACIÓN DE**  
**PERFORMANCE PARA UNA RED DE TRANSMISIÓN**

TABLA N° B.1 Typical Measurement Services

Enterprise / Function	Measured element	Typical Measurement Performance Requirements					
		Update Periodicity (Sec)	Accuracy (%)	Availability (hrs/mo)	Latency (Sec)	Resolution (%)	Time skew (sec)
<b>Tier 1</b>							
Substation Operator Indications	Voltage, Bus	5	0.3	4	1	0.1	1
Switching and Tagging	Voltage, Line	5	0.3	4	1	0.1	1
End element control	Real & Reactive Power, Line	10	1.0	4	5	0.2	1
Low priority alarm	Real & Reactive Power, Equip	10	1.0	4	5	0.2	1
High priority alarm	Current, Line	5	0.3	4	1	0.1	1
System restoration	Current, Equip	5	0.3	4	1	0.1	1
	Frequency/Phase Angle	10	1.0	4	5	0.2	1
	Position, Regulator/valve	10	1.0	4	5	0.2	1
	Ancillary value	10	1.0	4	5	0.2	1
<b>Tier 2</b>							
Non-System Operator Enterprise User Indication	Voltage, Bus	15	0.3	24	10	0.1	1
System Planning	Voltage, Line	15	0.3	24	10	0.1	1
	Real & Reactive Power, Line	30	1.0	24	30	0.2	1
	Real & Reactive Power, Equip	30	1.0	24	30	0.2	1
	Current, Line	15	0.3	24	30	0.1	1
	Current, Equip	15	0.3	24	30	0.1	1
	Frequency/Phase Angle	30	1.0	24	30	0.2	1
	Position, Regulator/valve	30	1.0	24	30	0.2	1
	Ancillary value	30	1.0	24	30	0.2	1
<b>Tier 3</b>							
Auto Gen Control	Voltage, Bus	2	0.3	2	1	0.1	1
Auto restoration	Voltage, Line	2	0.3	2	1	0.1	1
Sectionalizing	Real & Reactive Power, Line	2	1.0	2	1	0.2	1
	Real & Reactive Power, Equip	2	1.0	2	1	0.2	1
	Current, Line	2	0.3	2	1	0.1	1
	Current, Equip	2	0.3	2	1	0.1	1
	Frequency/Phase Angle	2	1.0	2	1	0.2	1
	Position, Regulator/valve	10	1.0	2	1	0.2	1
	Ancillary value	10	1.0	2	5	0.2	1
<b>Tier 4</b>							
State Estimation	Voltage, Bus	15	0.3	8	30	0.1	1
Operator Load Flow	Voltage, Line	15	0.3	8	30	0.1	1

		Typical Measurement Performance Requirements					
Enterprise / Function	Measured element	Update Periodicity (Sec)	Accuracy (%)	Availability (hrs/mo)	Latency (Sec)	Resolution (%)	Time skew (sec)
Optimal Power Flow	Real & Reactive Power, Line	15	3.0	8	30	0.2	1
Contingency Analysis	Real & Reactive Power, Equip	15	3.0	8	30	0.2	1
Security Surveillance	Current, Line	15	3.0	8	30	0.1	1
	Current, Equip	15	3.0	8	30	0.1	1
	Frequency/Phase Angle	30	3.0	8	30	0.2	1
	Position, Regulator/valve	30	1.0	8	30	0.2	1
	Ancillary value	30	1.0	8	30	0.2	1
<b>Tier 5</b>							
Power Quality	Voltage, Bus						
Intra-Substation Phasor Measurements	Voltage, Line						
Inter-substation/utility Phasor measurements	Real & Reactive Power, Line						
Substation Events	Real & Reactive Power, Equip						
System Events	Current, Line						
	Current, Equip						
	Frequency/Phase Angle						
	Position, Regulator/valve						
	Ancillary value						
<b>Tier 6</b>							
Device configuration data	Configuration Files						
GIS data	Mapping Files						
Electric system topology	Archive Files						
Condition monitoring							
Archive							
Disturbance/Fault data							
<b>Tier 7</b>							
substation/system time reference							

TABLA N° B.2 Typical Status Monitoring Performance Requirements

Enterprise / Function	Measured element	Typical Monitoring Performance Requirements					
		Update Periodicity (Sec)	Accuracy (%)	Availability (hrs/mo)	Latency (Sec)	Resolution (%)	Time skew (sec)
<b>Tier 1</b>							
Substation Operator Indications	breaker trip, fire,	2	99.9	4.0	0.5	0.1	0.1
Switching and Tagging	Substation HMI control	2	99.9	4.0	0.5	0.1	0.1
End element control		2	99.9	4.0	0.5	0.1	0.1
Substation algorithm		0.5	99.99	4.0	0.5	0.1	0.1
<b>Tier 2</b>							
Non-System Operator Enterprise User Indication		5					
<b>Security Surveillance</b>							
Low priority alarm	doors, gates, water on floor,	5 - 10	99	12	60	1	N/A
High priority alarm	breaker trip, fire,	2 - 5	99	1	2	0.001	N/A
Substation Sequence of Events	device state, time of state change,	OO	TS	8	20	0.001	0.0001
System Sequence of Events	device state, time of state change,	OO	TS	99	20	0.001	0.0001
<b>NOTES</b> 1—OO On occurrence 2—TS de-bounce logic, time stamp							

**TABLA N° B.3 Example Control Services Performance Requirements**

Enterprise / Function	Typical Control Performance Requirements						
	Measured element	Execution Time (Sec)	Accuracy %	Unavailability (Hrs/mo)	Latency (sec)	Single Point / Multiple Point	Feedback Sequence
<b>Tier 1</b>							
Substation Operator Control	Circuit breaker, capacitor switcher	2	99.99	4.0		Single	SBO
Auto-sectionalizing	Substation or Field device	2	99.99	4.0		Multiple	None
Generation Dispatch		2	99.9	4.0		Multiple	None
Substation algorithm		0.5	99.99	4.0			
<b>Tier 2</b>							
Non-System Operator Enterprise User		15		24		Single	
Low priority control	Pumps, lighting	15	99	12		Single	

TABLA N° B.4 Example Ancillary Performance Requirements

Function	Example	Typical Ancillary Performance Requirements						
		Update Periodicity	Execution Time	Accuracy %	Unavailability(Hrs/mo)	Latency (Sec)	Resolution (Sec)	Time skew (Sec)
<b>Tier 1</b>								
Substation Operator Reports		N/A	20 sec		4.0			
Non-System Operator Enterprise User Reports		N/A	200 sec		4.0			
State Estimation		5	2 sec		4.0			
Operator Load Flow		OD	0.5 sec		4.0			
<b>Tier 2</b>								
Optimal Power Flow		OD	2 sec		24			
Contingency Analysis		15	15 min		24			
<b>Tier 3</b>								
Device configuration data		OD	15 sec		24			
Electric system topology		OD	15 sec		24			
System planning		N/A	15 sec		12			
Condition monitoring		N/A	30 min					
Archive		N/A	30 min					
Disturbance/Fault data		N/A	5 min					
NOTE—OD: On demand								



**ANEXO C**  
**DOCUMENTACIÓN DEL PERFIL DNP DE UN DISPOSITIVO DE GENERAL**  
**ELECTRIC.**

## DNP Communications

### DNP 3.0 Device Profile Document

The communications port configured as a DNP slave port must support the full set of features listed in the Level 2 DNP V3.00 Implementation (DNP-L2) described in Chapter 2 of the subset definitions. See the DNP protocol website at <http://www.dnp.org> for details

<b>DNP 3.0: DEVICE PROFILE DOCUMENT</b>			
Vendor Name: General Electric Multilin Inc.			
Device Name: 750/760 Feeder Management Relay			
Highest DNP Level Supported: For Requests: Level 2 For Responses: Level 2		Device Function: <input type="checkbox"/> Master <input checked="" type="checkbox"/> Slave	
Notable objects, functions, and/or qualifiers supported in addition to the Highest DNP Levels Supported (the complete list is described in the attached table): Binary Input (Object 1, variations 1 and 2) Binary Output (Object 10, variation 2) Analog Input (Object 30, variations 1, 2, 3, and 4) Analog Input Change (Object 32, variations 1, 2, 3, and 4) Warm Restart (Function Code 14)			
Maximum Data Link Frame Size (octets): Transmitted: 292 Received: 292		Maximum Application Fragment Size (octets): Transmitted: 2048 Received: 2048	
Maximum Data Link Re-tries: <input type="checkbox"/> None <input type="checkbox"/> Fixed <input checked="" type="checkbox"/> Configurable (note 1)		Maximum Application Layer Re-tries: <input checked="" type="checkbox"/> None <input type="checkbox"/> Configurable	
Requires Data Link Layer Confirmation: <input type="checkbox"/> Never <input type="checkbox"/> Always <input type="checkbox"/> Sometimes <input checked="" type="checkbox"/> Configurable (note 1)			
Requires Application Layer Confirmation: <input type="checkbox"/> Never <input type="checkbox"/> Always <input checked="" type="checkbox"/> When reporting Event Data <input type="checkbox"/> When sending multi-fragment responses <input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable			
Timeouts while waiting for:			
Data Link Confirm	<input type="checkbox"/> None	<input type="checkbox"/> Fixed	<input type="checkbox"/> Variable <input checked="" type="checkbox"/> Configurable
Complete Appl. Fragment	<input checked="" type="checkbox"/> None	<input type="checkbox"/> Fixed	<input type="checkbox"/> Variable <input type="checkbox"/> Configurable
Application Confirm	<input checked="" type="checkbox"/> None	<input type="checkbox"/> Fixed	<input type="checkbox"/> Variable <input type="checkbox"/> Configurable
(fixed value is 5000 milliseconds)			
Complete Appl. Response	<input checked="" type="checkbox"/> None	<input type="checkbox"/> Fixed	<input type="checkbox"/> Variable <input type="checkbox"/> Configurable
Others: (None)			
Executes Control Operations:			
Write Binary Outputs	<input checked="" type="checkbox"/> Never	<input type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Select/Operate	<input type="checkbox"/> Never	<input checked="" type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Direct Operate	<input type="checkbox"/> Never	<input checked="" type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Direct Operate: No Ack	<input type="checkbox"/> Never	<input checked="" type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Count > 1	<input checked="" type="checkbox"/> Never	<input type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Pulse On	<input type="checkbox"/> Never	<input type="checkbox"/> Always	<input checked="" type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Pulse Off	<input checked="" type="checkbox"/> Never	<input type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Latch On	<input type="checkbox"/> Never	<input type="checkbox"/> Always	<input checked="" type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Latch Off	<input type="checkbox"/> Never	<input type="checkbox"/> Always	<input checked="" type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Trip/Close	<input type="checkbox"/> Never	<input type="checkbox"/> Always	<input checked="" type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
See Binary / Control Relay Output on page 77 for explanation of the above.			
Queue	<input checked="" type="checkbox"/> Never	<input type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable
Clear Queue	<input checked="" type="checkbox"/> Never	<input type="checkbox"/> Always	<input type="checkbox"/> Sometimes <input type="checkbox"/> Configurable

DNP 3.0: DEVICE PROFILE DOCUMENT (Continued)	
Reports Binary Input Change Events when no specific variations requested: <input type="checkbox"/> Never <input checked="" type="checkbox"/> Only time-tagged <input type="checkbox"/> Only non-time-tagged <input type="checkbox"/> Configurable to send both, one or the other	Reports time-tagged Binary Input Change Events when no specific variation requested: <input type="checkbox"/> Never <input checked="" type="checkbox"/> Binary Input Change With Time <input type="checkbox"/> Binary Input Change With Relative Time <input type="checkbox"/> Configurable
Sends Unsolicited Responses: <input checked="" type="checkbox"/> Never <input type="checkbox"/> Configurable <input type="checkbox"/> Only certain objects <input type="checkbox"/> Sometimes <input type="checkbox"/> ENABLE/DISABLE UNSOLICITED Function codes supported	Sends Static Data in Unsolicited Responses: <input checked="" type="checkbox"/> Never <input type="checkbox"/> When Device Restarts <input type="checkbox"/> When Status Flags Change
Default Counter Object/Variation: <input checked="" type="checkbox"/> No Counters Reported <input type="checkbox"/> Configurable <input type="checkbox"/> Default Object / Default Variation <input type="checkbox"/> Point-by-point list attached	Counters Roll Over at: <input checked="" type="checkbox"/> No Counters Reported <input type="checkbox"/> Configurable <input type="checkbox"/> 16 Bits <input type="checkbox"/> 32 Bits <input type="checkbox"/> Other Value <input type="checkbox"/> Point-by-point list attached
Sends Multi-Fragment Responses: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

Note 1: The data link layer confirmation mode, confirmation time-out, and number of retries are all configurable. Refer to the *DNP Configuration* section in Chapter 5 of the Instruction manual for more details.

## DNP Implementation

The table below gives a list of all objects recognized and returned by the relay. Additional information is provided on the following pages including a list of the default variations returned for each object and lists of defined point numbers for each object.

### Implementation Table Notes:

1. For this object, the quantity specified in the request must be exactly 1 as there is only one instance of this object defined in the relay.
2. All static input data known to the relay is returned in response to a request for Class 0. This includes all objects of type 1 (Binary Input), type 10 (Binary Output) and type 30 (Analog Input).
3. The point tables for Binary Input and Analog Input objects contain a field which defines to which event class the corresponding static data has been assigned.
4. For this object, the qualifier code must specify an index of 7 only.

## DNP Communications

Table 9: DNP Implementation Table

Object			Request		Response	
Obj	Var	Description	Func Codes	Qual Codes (Hex)	Func Codes	Qual Codes (Hex)
1	0	Binary Input - All Variations	1	06		
1	1	Binary Input	1	00, 01, 06	129	00, 01
1	2	Binary Input With Status (Note 6)	1	00, 01, 06	129	00, 01
2	0	Binary Input Change - All Variations	1	06, 07, 08		
2	1	Binary Input Change Without Time	1	06, 07, 08	129	17, 28
2	2	Binary Input Change With Time	1	06, 07, 08	129	17, 28
10	0	Binary Output - All Variations	1	06		
10	2	Binary Output Status	1	00, 01, 06	129	00, 01
12	1	Control Relay Output Block	3, 4, 5, 6	17, 28	129	17, 28
30	0	Analog Input - All Variations	1	06		
30	1	32-Bit Analog Input With Flag	1	00, 01, 06	129	00, 01
30	2	16-Bit Analog Input With Flag	1	00, 01, 06	129	00, 01
30	3	32-Bit Analog Input Without Flag	1	00, 01, 06	129	00, 01
30	4	16-Bit Analog Input Without Flag	1	00, 01, 06	129	00, 01
32	0	Analog Input Change - All Variations	1	06, 07, 08		
32	1	32-Bit Analog Input Change without Time	1	06, 07, 08	129	17, 28
32	2	16-Bit Analog Input Change without Time	1	06, 07, 08	129	17, 28
32	3	32-Bit Analog Input Change with Time	1	06, 07, 08	129	17, 28
32	4	16-Bit Analog Input Change with Time	1	06, 07, 08	129	17, 28
50	1	Time and Date	1, 2	07 (Note 1)	129	07
60	1	Class 0 Data (Note 2)	1	06	129	
60	2	Class 1 Data (Note 3)	1	06, 07, 08	129	
60	3	Class 2 Data (Note 3)	1	06, 07, 08	129	
60	4	Class 3 Data (Note 3)	1	06, 07, 08	129	
80	1	Internal Indications	2	00 (Note 4)	129	
		No object - Cold Start	13			
		No object - Warm Start (Note 5)	14			
		No object - Delay Measurement	23			

1, 2, 3, 4, 5, 6: see the IMPLEMENTATION TABLE NOTES above.

The following table specifies the default variation for all objects returned by the relay. These are the variations that will be returned for the object in a response when no specific variation is specified in a request.

Object	Description	Default Variation
1	Binary Input - Single Bit	1
2	Binary Input Change With Time	2
10	Binary Output Status	2
30	16-Bit Analog Input Without Flag	4
32	16-Bit Analog Input Change Without Time	2

## DNP Point Lists

### Binary Input / Binary Input Change

The point list for Binary Input (Object 01) and Binary Input Change (Object 02) is shown below.

**Table 10: Binary Inputs DNP Points**

Index	Description	Event Class
0	Relay In Service	Class 1
1	Trip Condition(s) Active	Class 1
2	Alarm Condition(s) Active	Class 1
3	Protection Picked Up	Class 1
4	Setpoint Group 1 Active	Class 1
5	Setpoint Group 2 Active	Class 1
6	Setpoint Group 3 Active	Class 1
7	Setpoint Group 4 Active	Class 1
8	Breaker Is Open	Class 1
9	Breaker Is Closed	Class 1
10	Reclosure Enabled <sup>1</sup>	Class 1
11	Reclosure Disabled <sup>1</sup>	Class 1
12	Reclosure In Progress <sup>1</sup>	Class 1
13	Reclosure Locked Out <sup>1</sup>	Class 1
14	Local Mode Active	Class 1
15	Diagnostic Message(s) Active	Class 1
16	Major Internal Failure	Class 1
17	Minor Internal Failure	Class 1
18	Testing Mode Active	Class 1
19	Contact Input 1 Closed	Class 1
20	Contact Input 2 Closed	Class 1
21	Contact Input 3 Closed	Class 1
22	Contact Input 4 Closed	Class 1
23	Contact Input 5 Closed	Class 1
24	Contact Input 6 Closed	Class 1
25	Contact Input 7 Closed	Class 1
26	Contact Input 8 Closed	Class 1
27	Contact Input 9 Closed	Class 1
28	Contact Input 10 Closed	Class 1
29	Contact Input 11 Closed	Class 1
30	Contact Input 12 Closed	Class 1
31	Contact Input 13 Closed	Class 1
32	Contact Input 14 Closed	Class 1
33	Setpoint Access Jumper Present	Class 1
34	Coil Monitor 1 Circuit Closed	Class 1
35	Coil Monitor 2 Circuit Closed	Class 1
36	Relay 1 Trip Operated	Class 1
37	Relay 2 Close Operated	Class 1
38	Relay 3 Auxiliary Operated	Class 1

**Table 10: Binary Inputs DNP Points**

<b>Index</b>	<b>Description</b>	<b>Event Class</b>
39	Relay 4 Auxiliary Operated	Class 1
40	Relay 5 Auxiliary Operated	Class 1
41	Relay 6 Auxiliary Operated	Class 1
42	Relay 7 Auxiliary Operated	Class 1
43	Relay 8 Service Operated	Class 1

**Notes:**

1. Any detected change in the state of any point will cause the generation of an event object.
2. An event object will be generated as a result of any change in any point.

- The "Breaker Control" point (23) will only accept a "Trip" or "Close" value. A value of "Trip" will activate the "Breaker Open" function. Similarly, a value of "Close" will activate the "Breaker Close" function.
  - All operations not defined above are invalid and will be rejected.
3. The *On Time* and *Off Time* fields are ignored. A "Pulse On" Code takes effect immediately when received, therefore timing is irrelevant.
  4. The *Status* field in the response will reflect the success or failure of the control attempt thus:
    - A Status of "Request Accepted" (0) will be returned if the command was accepted.
    - A Status of "Request not Accepted due to Formatting Errors" (3) will be returned if the Control Code field was incorrectly formatted or an invalid Code was present in the command.
    - A Status of "Control Operation not Supported for this Point" (4) will be returned if an attempt was made to operate the "Open Breaker" (1), "Close Breaker" (2) or "Breaker Control" (23) points and the relay is in local mode (this status is indicated by Object 1, Point 14).

Setting or clearing a Virtual Input will always succeed, however an operate of the Reset, Open Breaker, Close Breaker or Breaker Control points may fail (even if the command is accepted) due to other inputs or conditions (e.g., blocks) existing at the time. To verify the success or failure of an operate of these points it is necessary that the associated Binary Input(s) be examined after the control attempt is performed.

When using object 10 to read the status of a Binary Output, a read of points 0 through 2 and 23 will always return zero. For other points, the current state of the corresponding Virtual Input will be returned.

### Analog Input / Analog Input Change

In the following table, the entry in the "Format" column indicates that the format of the associated data point can be determined by looking up the entry in the Memory Map Data Formats table. For example, an "F1" format is described in that table as a (16-bit) unsigned value without any decimal places. Therefore, the value read should be interpreted in this manner.

The point list for Analog Input (Object 30) and Analog Input Change (Object 32) is shown below. Refer to the notes following the table for additional details.

**Table 12: Analog Inputs DNP Points (Sheet 1 of 5)**

Index when Point Mapping is:		Format	Description	Event Class Assigned
Disabled	Enabled			
n/a	0	-	User Map Value 1	
n/a	1	-	User Map Value 2	
↓	↓	↓	↓	
n/a	118	-	User Map Value 119	
n/a	119	-	User Map Value 120	
0	120	F49	Phase Time Overcurrent 1	Class 1
1	121	F49	Phase Instantaneous Overcurrent 1	Class 1
2	122	F49	Phase Instantaneous Overcurrent 2	Class 1
3	123	F49	Ground Time Overcurrent	Class 1
4	124	F49	Ground Instantaneous Overcurrent	Class 1
5	125	F49	Neutral Time Overcurrent 1	Class 1
6	126	F49	Neutral Time Overcurrent 2	Class 1
7	127	F49	Neutral Instantaneous Overcurrent 1	Class 1
8	128	F49	Neutral Instantaneous Overcurrent 2	Class 1

**Binary / Control Relay  
Output**

The point list for Binary Output (Object 10) and Control Relay Output (Object 12) is shown below.

**Table 11: Binary Outputs DNP Points**

Index	Description
0	Reset
1	Open Breaker
2	Close Breaker
3	Virtual Input 1
4	Virtual Input 2
5	Virtual Input 3
6	Virtual Input 4
7	Virtual Input 5
8	Virtual Input 6
9	Virtual Input 7
10	Virtual Input 8
11	Virtual Input 9
12	Virtual Input 10
13	Virtual Input 11
14	Virtual Input 12
15	Virtual Input 13
16	Virtual Input 14
17	Virtual Input 15
18	Virtual Input 16
19	Virtual Input 17
20	Virtual Input 18
21	Virtual Input 19
22	Virtual Input 20
23	Breaker Control

The following restrictions should be observed when using object 12 to control the points listed in the above table.

1. The *Count* field is checked first. If it is zero, the command will be accepted but no action will be taken. If this field is non-zero, the command will be executed exactly once regardless of its value.
2. The *Control Code* field of object 12 is then inspected:
  - The Queue, and Clear sub-fields are ignored.
  - If the Code sub-field is NUL, then the command will be accepted without any action being taken.
  - A Code sub-field of "Pulse On" (1) is valid only for points 0 through 2. This is used to activate the function (e.g., Reset) associated with the point.
  - A Code sub-field of "Pulse On" (1) in combination with a value in the Trip/Close sub-field form a "Trip" or "Close" value. A "Trip" value consists of a "Pulse On" (1) in the Code sub-field and a 2 in the Trip/Close sub-field. This results in a value of 81 (hex) in the Control Code field. A "Close" value consists of a "Pulse On" (1) in the Code sub-field and a 1 in the Trip/Close sub-field. This results in a value of 41 (hex) in the Control Code field.
  - A Code sub-field of "Latch On" (3) or "Latch Off" (4) is valid for all virtual input points (i.e., points 3 through 22). This is used to set the associated Virtual Input on ("Latch On") or off ("Latch Off"). As well, a "Close" value in the Control Code field will cause the virtual input to be turned on while a "Trip" value in this field will cause the virtual input to be turned off.

Table 12: Analog Inputs DNP Points (Sheet 2 of 5)

Index when Point Mapping is:		Format	Description	Event Class Assigned
Disabled	Enabled			
9	129	F49	Phase Directional Is Reverse	Class 1
10	130	F49	Neutral Directional Is Reverse	Class 1
11	131	F49	Manual Close Blocking	Class 1
12	132	F49	Cold Load Pickup Blocking	Class 1
13	133	F49	Bus Undervoltage 1	Class 1
14	134	F49	Bus Undervoltage 2	Class 1
15	135	F49	Line Undervoltage 3	Class 1
16	136	F49	Line Undervoltage 4	Class 1
17	137	F49	Overvoltage 1	Class 1
18	138	F49	Overvoltage 2	Class 1
19	139	F49	Underfrequency 1	Class 1
20	140	F49	Underfrequency 2	Class 1
21	141	F49	Phase Current Level	Class 1
22	142	F49	Neutral Current Level	Class 1
23	143	F49	Power Factor 1	Class 1
24	144	F49	Power Factor 2	Class 1
25	145	F49	Synchrocheck Block (Not In Sync)	Class 1
26	146	F49	Current Demand	Class 1
27	147	F49	Real Power Demand	Class 1
28	148	F49	Reactive Power Demand	Class 1
29	149	F49	Apparent Power Demand	Class 1
30	150	F49	Analog Input Threshold 1	Class 1
31	151	F49	Analog Input Threshold 2	Class 1
32	152	F49	Analog Input Rate of Change 1	Class 1
33	153	F49	Analog Input Rate of Change 2	Class 1
34	154	F49	Overfrequency	Class 1
35	155	F49	Trip Counter	Class 1
36	156	F49	Arcing Current	Class 1
37	157	F49	VT Failure	Class 1
38	158	F49	Breaker Failure	Class 1
39	159	F49	Breaker Operation Failure	Class 1
40	160	F49	Trip Coil Monitor	Class 1
41	161	F49	Close Coil Monitor	Class 1
42	162	F49	User Input A	Class 1
43	163	F49	User Input B	Class 1
44	164	F49	User Input C	Class 1
45	165	F49	User Input D	Class 1
46	166	F49	User Input E	Class 1
47	167	F49	User Input F	Class 1
48	168	F49	User Input G	Class 1
49	169	F49	User Input H	Class 1
50	170	F49	Negative Sequence Instantaneous Overcurrent	Class 1
51	171	F49	Negative Sequence Time Overcurrent	Class 1
52	172	F49	Negative Sequence Overvoltage	Class 1
53	173	F49	Undervoltage Restoration	Class 1

Table 12: Analog Inputs DNP Points (Sheet 3 of 5)

Index when Point Mapping is:		Format	Description	Event Class Assigned	
Disabled	Enabled				
	54	174	F49	Underfrequency Restoration	Class 1
	55	175	F49	Phase Time Overcurrent 2	Class 1
	56	176	F49	Frequency Decay	Class 1
	57	177	F49	Negative Sequence Directional Is Reverse	Class 1
	58	178	F49	Sensitive Ground Instantaneous Overcurrent	Class 1
	59	179	F49	Sensitive Ground Time Overcurrent	Class 1
	60	180	F49	Sensitive Ground Directional Is Reverse	Class 1
	61	181	F1	Phase A RMS Current (see Note 3)	Class 2
	62	182	F1	Phase B RMS Current (see Note 3)	Class 2
	63	183	F1	Phase C RMS Current (see Note 3)	Class 2
	64	184	F1	Percent Of Load-To-Trip (see Note 3)	Class 2
	65	185	F1	Ground Current (see Note 3)	Class 2
	66	186	F3	Phase A-Neutral RMS Voltage (see Note 3)	Class 2
	67	187	F3	Phase B-Neutral RMS Voltage (see Note 3)	Class 2
	68	188	F3	Phase C-Neutral RMS Voltage (see Note 3)	Class 2
	69	189	F3	Phase A-Phase B RMS Voltage (see Note 3)	Class 2
	70	190	F3	Phase B-Phase C RMS Voltage (see Note 3)	Class 2
	71	191	F3	Phase C-Phase A RMS Voltage (see Note 3)	Class 2
	72	192	F3	Sensitive Ground Current (see Note 3)	Class 2
	73	193	F1	Average Current (see Note 3)	Class 2
	74	194	F3	Average Line Voltage (see Note 3)	Class 2
	75	195	F3	Average Phase Voltage (see Note 3)	Class 2
	76	196	F1	Neutral Current (see Note 3)	Class 2
	77	197	F86	3 $\phi$ Real Power (see Note 3)	Class 2
	78	198	F86	3 $\phi$ Reactive Power (see Note 3)	Class 2
	79	199	F86	3 $\phi$ Apparent Power (see Note 3)	Class 2
	80	200	F6	3 $\phi$ Power Factor (see Note 3)	Class 2
	81	201	F3	System Frequency (see Note 4)	Class 2
	82	202	F1	Analog Input (see Note 3)	Class 2
	83	203	F23	Date Of Last Trip (upper 16 Bits, see Note 1)	Class 1
	84	204	F23	Date Of Last Trip (lower 16 Bits, see Note 1)	Class 1
	85	205	F22	Time Of Last Trip (upper 16 Bits, see Note 1)	Class 1
	86	206	F22	Time Of Last Trip (lower 16 Bits, see Note 1)	Class 1
	87	207	F24	Cause Of Last Trip	Class 1
	88	208	F1	Last Trip Phase A RMS Current	Class 1
	89	209	F1	Last Trip Phase B RMS Current	Class 1
	90	210	F1	Last Trip Phase C RMS Current	Class 1
	91	211	F1	Last Trip Ground Current	Class 1
	92	212	F3	Last Trip Sensitive Ground Current	Class 1
	93	213	F3	Last Trip A-N (A-B) RMS Voltage	Class 1
	94	214	F3	Last Trip B-N (B-C) RMS Voltage	Class 1
	95	215	F3	Last Trip C-N (C-A) RMS Voltage	Class 1
	96	216	F3	Last Trip System Frequency	Class 1
	97	217	F1	Last Trip Analog Input	Class 1
	98	218	F1	Last Trip Neutral Current	Class 1
	99	219	F23	Date Of Fault 1 (Upper 16 Bits - See Note 1)	Class 3

Table 12: Analog Inputs DNP Points (Sheet 4 of 5)

Index when Point Mapping is:		Format	Description	Event Class Assigned	
Disabled	Enabled				
	100	220	F23	Date Of Fault 1 (Lower 16 Bits - See Note 1)	Class 3
	101	221	F22	Time Of Fault 1 (Upper 16 Bits - See Note 1)	Class 3
	102	222	F22	Time Of Fault 1 (Lower 16 Bits - See Note 1)	Class 3
	103	223	F76	Type Of Fault 1	Class 3
	104	224	F52	Distance To Fault 1	Class 3
	105	225	F53	Line Z1 To Fault 1 (Magnitude)	Class 3
	106	226	F23	Date Of Fault 2 (Upper 16 Bits - See Note 1)	
	107	227	F23	Date Of Fault 2 (Lower 16 Bits - See Note 1)	
	108	228	F22	Time Of Fault 2 (Upper 16 Bits - See Note 1)	
	109	229	F22	Time Of Fault 2 (Lower 16 Bits - See Note 1)	
	110	230	F76	Type Of Fault 2	
	111	231	F52	Distance To Fault 2	
	112	232	F53	Line Z1 To Fault 2 (Magnitude)	
	113	233	F23	Date Of Fault 3 (Upper 16 Bits - See Note 1)	
	114	234	F23	Date Of Fault 3 (Lower 16 Bits - See Note 1)	
	115	235	F22	Time Of Fault 3 (Upper 16 Bits - See Note 1)	
	116	236	F22	Time Of Fault 3 (Lower 16 Bits - See Note 1)	
	117	237	F76	Type Of Fault 3	
	118	238	F52	Distance To Fault 3	
	119	239	F53	Line Z1 To Fault 3 (Magnitude)	
	120	240	F23	Date Of Fault 4 (Upper 16 Bits - See Note 1)	
	121	241	F23	Date Of Fault 4 (Lower 16 Bits - See Note 1)	
	122	242	F22	Time Of Fault 4 (Upper 16 Bits - See Note 1)	
	123	243	F22	Time Of Fault 4 (Lower 16 Bits - See Note 1)	
	124	244	F76	Type Of Fault 4	
	125	245	F52	Distance To Fault 4	
	126	246	F53	Line Z1 To Fault 4 (Magnitude)	
	127	247	F23	Date Of Fault 5 (Upper 16 Bits - See Note 1)	
	128	248	F23	Date Of Fault 5 (Lower 16 Bits - See Note 1)	
	129	249	F22	Time Of Fault 5 (Upper 16 Bits - See Note 1)	
	130	250	F22	Time Of Fault 5 (Lower 16 Bits - See Note 1)	
	131	251	F76	Type Of Fault 5	
	132	252	F52	Distance To Fault 5	
	133	253	F53	Line Z1 To Fault 5 (Magnitude)	
	134	254	F23	Date Of Fault 6 (Upper 16 Bits - See Note 1)	
	135	255	F23	Date Of Fault 6 (Lower 16 Bits - See Note 1)	
	136	256	F22	Time Of Fault 6 (Upper 16 Bits - See Note 1)	
	137	257	F22	Time Of Fault 6 (Lower 16 Bits - See Note 1)	
	138	258	F76	Type Of Fault 6	
	139	259	F52	Distance To Fault 6	
	140	260	F53	Line Z1 To Fault 6 (Magnitude)	
	141	261	F23	Date Of Fault 7 (Upper 16 Bits - See Note 1)	
	142	262	F23	Date Of Fault 7 (Lower 16 Bits - See Note 1)	
	143	263	F22	Time Of Fault 7 (Upper 16 Bits - See Note 1)	
	144	264	F22	Time Of Fault 7 (Lower 16 Bits - See Note 1)	
	145	265	F76	Type Of Fault 7	

Table 12: Analog Inputs DNP Points (Sheet 5 of 5)

Index when Point Mapping Is:		Format	Description	Event Class Assigned
Disabled	Enabled			
146	266	F52	Distance To Fault 7	
147	267	F53	Line Z1 To Fault 7 (Magnitude)	
148	268	F23	Date Of Fault 8 (Upper 16 Bits - See Note 1)	
149	269	F23	Date Of Fault 8 (Lower 16 Bits - See Note 1)	
150	270	F22	Time Of Fault 8 (Upper 16 Bits - See Note 1)	
151	271	F22	Time Of Fault 8 (Lower 16 Bits - See Note 1)	
152	272	F76	Type Of Fault 8	
153	273	F52	Distance To Fault 8	
154	274	F53	Line Z1 To Fault 8 (Magnitude)	
155	275	F23	Date Of Fault 9 (Upper 16 Bits - See Note 1)	
156	276	F23	Date Of Fault 9 (Lower 16 Bits - See Note 1)	
157	277	F22	Time Of Fault 9 (Upper 16 Bits - See Note 1)	
158	278	F22	Time Of Fault 9 (Lower 16 Bits - See Note 1)	
159	279	F76	Type Of Fault 9	
160	280	F52	Distance To Fault 9	
161	281	F53	Line Z1 To Fault 9 (Magnitude)	
162	282	F23	Date Of Fault 10 (Upper 16 Bits - See Note 1)	
163	283	F23	Date Of Fault 10 (Lower 16 Bits - See Note 1)	
164	284	F22	Time Of Fault 10 (Upper 16 Bits - See Note 1)	
165	285	F22	Time Of Fault 10 (Lower 16 Bits - See Note 1)	
166	286	F76	Type Of Fault 10	
167	287	F52	Distance To Fault 10	
168	288	F53	Line Z1 To Fault 10 (Magnitude)	
169	289	F49	Reserved for MOD 008	Class 1
170	290	F49	Neutral Displacement	Class 1
171	291	F49	Ground Directional is Reverse	Class 1
172	292	F49	Reserved For MOD 010	Class 1
173	293	F49	User Input I	Class 1
174	294	F49	User Input J	Class 1
175	295	F49	User Input K	Class 1
176	296	F49	User Input L	Class 1
177	297	F49	User Input M	Class 1
178	298	F49	User Input N	Class 1
179	299	F49	User Input O	Class 1
180	300	F49	User Input P	Class 1
181	301	F49	User Input Q	Class 1
182	302	F49	User Input R	Class 1
183	303	F49	User Input S	Class 1
184	304	F49	User Input T	Class 1
185	305	F49	Autoreclose Rate Supervision	Class 1
186	306	F49	Restricted Earth Fault	Class 1
187	307	F1	Auto Ranging Power / Energy Multiplier	Class 2
188	308	F3	Neutral Voltage (see Note 3)	Class 2
189	309	F3	Last Trip Neutral Voltage	Class 1

**ANEXO D**  
**CONTENIDO DE PROCEDIMIENTOS DE CERTIFICACIÓN**

**TABLA N° D.1 Procedimientos de Certificación**

Section	Title	Description
1	Overview	Describes purpose of test as specifically ensure compliance with Level of the Subset definitions
2	Notes	General Test requirements and assumptions
3	Definitions	Includes: General Definitions Definitions of INN bit meanings Error response shows by I12 bits Definitions about change objects
4	References documents	Defined to be: Basic Four Subnet Definitions
5	Pretest Review Device Profile Review Equipment Review Wiring Diagrams	This Defines the pre-test desktop review requirements these ensure the device Profile documentations is conforming, it indicates conformance, and that device is testable
6	Link Layer Reset Link and passive confirm support Test Link Request Link Status Test Retries DIR AND FCV Bits Data Link Rejects Invalid Frames	Test Link Layer  The Section specifies for each function under test: <ul style="list-style-type: none"> <li>- Desired behaviour</li> <li>- Test procedure</li> </ul>
7	Transport Layer	Test Transport Layer functionality. The section specifies: <ul style="list-style-type: none"> <li>- Desired behaviour</li> <li>- Test procedure</li> </ul>
8	Application Layer <ul style="list-style-type: none"> <li>- Binary Output status</li> <li>- Binary outputs</li> <li>- Analog Outputs status</li> <li>- Analog Outputs</li> <li>- Test Retries</li> <li>- Class Data</li> <li>- Indications</li> <li>- Time</li> <li>- Cold Restart</li> <li>- Application Layer Fragmentation</li> <li>- Multidrop Support</li> <li>- Unsolicited Responses</li> <li>- Collision Avoidance</li> </ul> Additional sections for Level 2 <ul style="list-style-type: none"> <li>- Binary Inputs</li> <li>- Binary Input change</li> <li>- Common time of occurrence</li> <li>- Binary Counters</li> <li>- Binary Counters, Event</li> <li>- Analog Input</li> <li>- Analog change Event</li> <li>- Multiple Read Request</li> </ul>	Tests Application layer functionality  The Section specifies for each function under test:  The Section specifies for each function under test: <ul style="list-style-type: none"> <li>- Desired behaviour</li> <li>- Test procedure</li> </ul>

## **BIBLIOGRAFÍA**

1. IEEE Recommended Practice for Master/Remote Supervisory Control and Acquisition (SCADA) Communications. Standards 1993.
2. IEEE Standard Definition, Specification and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control. IEEE Standards, 1994.
3. Gordon Clarke and Deon Reynders. "Modern SCADA Protocols" Ed. Elsevire, 2004.
4. Stuart A. Boyer. "Supervisory Control And data Acquisition" Ed. ISA, 2004.
5. Paper "DNP3 Protocol Premier" Wrote by Ken Cutis. Jun 2000