UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROTOCOLO DE COMUNICACIÓN PARA SISTEMAS DE TRANSPORTE INTELIGENTE

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

ROCIO JESUS ANDIA RUIZ

PROMOCIÓN
2003 - I

LIMA – PERÚ
2006

PROTOCOLO DE COMUNICACIÓN PARA SISTEMAS DE TRANSPORTE INTELIGENTE

SUMARIO

Estos Protocolos de Comunicación para Sistemas de Transporte Inteligente están basados en la familia de normas de comunicaciones de Comunicación de Transporte Nacional para Sistemas de Transporte Inteligente (NTCIP: Nacional Transportation Communication for Intelligent Transport System Protocols).

Se va a hacer un breve resumen de cada capítulo expuesto en este informe:

Capítulo I: Definición de Sistemas de Transporte Inteligente y Beneficios del NTCIP

Este capítulo define los conceptos del Sistema de transporte inteligente, del NTCIP, sus beneficios y tipos de sistemas soportados por el mismo.

Capítulo II: Niveles de Comunicación y Protocolos usados en Sistemas de Transporte Inteligente

Este capítulo va a comparar los niveles de comunicación con el modelo OSI, los tipos de protocolos que existen en esta familia, y algunos ejemplos para entender las definiciones de los mismos.

Capítulo III: Definición de Protocolos

Este capítulo es una descripción de los diferentes protocolos usados en Sistemas de Transporte Inteligente.

Capítulo IV: Requerimientos y Alternativas

Este capítulo presenta los requerimientos y alternativas para la implementación de una Central de Tráfico.

Capítulo V: Ejemplo de Implementaciones NTCIP

Este capítulo describe ejemplos para cada tipo de protocolos usados en NTCIP.

INDICE

PROLOGO

Un protocolo de comunicaciones es un conjunto de reglas de como los mensajes y los elementos de la data son codificados y transmitidos entre dispositivos electrónicos, el equipo de cada Terminal de la transmisión de la data debe usar el mismo protocolo para una comunicación satisfactoria. Los protocolos son como el lenguaje humano que tienen un alfabeto, vocabulario, reglas gramaticales usadas por cualquier persona que hable ese lenguaje.

Se sabe que cada proveedor de dispositivos de control de tráfico y software usados en los sistemas de gestión de transporte son desarrollados con un protocolo propietario diferente para las comunicaciones de la data. Esto requiere de proyectos de integración extensiva para mezclar equipos y software en el mismo sistema y poder comunicarse entre sistemas operados por agencias adjuntas. Estos protocolos de comunicación para Sistemas de Transporte Inteligente aquí descritos en este informe, proveen normas comunes que pueden ser usados por todos los fabricantes y desarrolladores de sistemas para ayudar a superar estas diferencias.

Estos protocolos pertenecen a una familia de comunicaciones estándares para la transmisión de datos y mensajes entre los dispositivos de control usados en los Sistemas de Transporte Inteligente. Un ejemplo de cómo un sistema está basado en la operación de controladores de microprocesadores que controlan y monitorean a una ciudad a través de los semáforos. La computadora puede enviar instrucciones a los controladores de tráfico para cambiar los tiempos de ciclo o de cada fase de acuerdo a las condiciones de tránsito y éstos pueden enviar a la vez el estado actual del flujo de tráfico a la computadora.

En otro ejemplo, dos sistemas de gestión de tránsito pueden necesitar intercambiar información en tiempo real acerca de la ubicación de los vehículos. Esto permite a cada sistema saber en forma inmediata cuando un vehículo está corriendo mas de lo permitido. Los pasajeros pueden ser notificados con anticipación y en forma automática, y el Centro de Gestión de Tráfico Local puede ser automáticamente pedido de dar prioridad a las señales de tráfico para los vehículos de tránsito.

CAPITULO I

DEFINICION DE SISTEMAS DE TRANSPORTE INTELIGENTE Y BENEFICIOS DEL NTCIP

1.1 Introducción:

Los Protocolos de Comunicación para Sistemas de Transporte Inteligente (ITS Intelligent Transport System), son usados para controlar en forma remota las vías de tránsito y otros dispositivos de gestión de transporte.

Este define los protocolos y perfiles de comunicación de datos, el cual habilita las aplicaciones para interactuar y lograr una funcionalidad deseada.

Algunos protocolos de esta familia ya han sido aprobadas, y otros están en proceso de aprobación. Además, esta aplicación continúa creciendo en la comunidad del transporte, puesto que la necesidad lo hará incrementar más.

El propósito de estos protocolos es que como la comunidad del Transporte ha necesitado por mucho tiempo un sistema de transporte que pueda ser estructurado usando dispositivos y componentes que fuese ***intercambiables*** e ***interoperables***. Es por esta razón que esta familia de protocolos este siendo incluido y especificado en muchos nuevos desarrollos de sistemas.

El término ***interoperabilidad*** refleja la habilidad de múltiples dispositivos, con frecuencia de diferentes modelos, para que puedan trabajar juntos como un solo sistema para el mismo propósito. Un ejemplo de interoperabilidad es, el control de tráfico y los mensajes dinámicos que comparten un solo canal de comunicación en el caso de comunicaciones Centro – a – Campo.

El término ***intercambiabilidad*** esta definido como la capacidad de intercambiar dispositivos del mismo tipo en un mismo canal de comunicación y tienen esos dispositivos que interactuar con otros dispositivos del mismo tipo usando las funciones estandards en las cuales están basadas. Un ejemplo de intercambiabilidad es un control de tráfico que provienen de diferentes procedencias pueden interactuar con cada control de tráfico que provee la coordinación a lo largo de una autopista o carretera.

El tema de los protocolos de comunicación para ITS, es un desafío, aún para el personal con amplia experiencia en estas materias. En este caso, el nivel de dificultad es muy alto, puesto que es una familia de normas diseñado para reunir las necesidades de la comunicación de varios activos inmovilizados de los Centros de Gestión de Tráfico y Dispositivos de Carretera.

Un Protocolo de Comunicación es una serie de reglas de cómo los mensajes y los elementos de datos son codificados y transmitidos entre dispositivos electrónicos. El equipo de cada transmisior de datos debe usar el mismo protocolo para comunicarse satisfactoriamente. El protocolo es casi como el lenguaje humano que tiene un alfabeto, vocabulario y reglas de gramática usado por cualquier persona para hablar ese lenguaje.

Históricamente, cada fabricante de dispositivos de control y software usados en el sistema de gestión de datos, desarrolló o adoptó diferentes protocolos propietarios para la comunicación de datos. Este proyecto de integración extensiva sirve para combinar los equipos y software de diferentes fabricantes en el mismo sistema y comunicarse entre sistemas operados por diferentes agencias.

El **NTCIP** (Protocolo de Comunicación de Transporte Nacional para ITS - National Transportation Comunication for ITS Protocol) es una familia de normas de comunicaciones para la transmisión de datos y mensajes entre dispositivos de control usados en ITS. Un ejemplo de esto es una computadora que monitorea y controla la operación del controlador de tráfico basado en microprocesadores el cual controla los semáforos de una ciudad. La computadora puede enviar instrucciones a los controladores de tráfico para cambiar los tiempos de las señales de acuerdo a las condiciones de tráfico, y el controlador de la intersección envia la información de estado y el flujo del tráfico a la computadora.

Estos protocolos tiene la intención de ser usado en todo tipo de sistemas de gestión de acuerdo al ambiente del transporte, incluyendo las autopistas, semáforos, tránsito, gestión de emergencia, información del viajero y archivamiento de datos. Además, la comunicación puede ser alámbrica o inalámbrica entre la computadora de diferentes sistemas o diferentes Centros de Gestión, y entre una computadora y los dispositivos de gestión de tránsito.

1.1.1 ¿Qué es el Sistema de Transporte Inteligente (ITS)?

Los Sistemas de Transporte Inteligente, conocidos también como ITS, son tecnologías que incluyen electrónica avanzada, comunicaciones y sistemas informáticos para aumentar la eficiencia y seguridad del transporte por carretera. Conocidas originalmente como IVHS (iniciales de *Intelligent Vehicle/Highway Systems,* Sistemas

inteligentes de automóviles y autopistas), proporcionan intercambio de información en tiempo real entre los conductores y las vías de tránsito, de ahí los términos "automóviles inteligentes" o "autopistas inteligentes". Como las tecnologías se han expandido para incluir al transporte público y vehículos comerciales, este rango de tecnologías ha terminado por llamarse sistema de transporte inteligente. Con el tiempo, los conductores tendrán acceso a la última información acerca de las condiciones de circulación (incluyendo atascos y accidentes), selecciones de rutas, direcciones de destino poco familiares y es posible que hasta control automatizado del vehículo.

La gestión o administración de la circulación es un área en la que se están utilizando sistemas avanzados de electrónica para mejorar el control del tráfico. En algunas ciudades, la circulación de las principales carreteras se controlan mediante cámaras de vídeo, radares o sensores en la propia carretera. Un sistema de computadora central analiza la información. Si la circulación está congestionada o atascada, el flujo de circulación mejora de modo automático ajustando los intervalos de señales de tráfico, controlando el flujo de circulación en las carreteras de acceso a las ciudades o proporcionando información a los conductores mediante señales electrónicas a lo largo de las carreteras.

Las tecnologías de control automatizado de vehículos se están desarrollando para mejorar la seguridad en carretera. Estos dispositivos, situados a bordo del vehículo, pueden avisar al conductor para impedir un peligro determinado o, en una emergencia, corregir sus acciones. Se ha adaptado un sistema de radar para uso en los autobuses de escuela de manera que detecten a una persona cerca del vehículo y alerten al conductor. También se están estudiando los sensores de infrarrojos y otros métodos de mejora visual para incrementar la seguridad en la circulación nocturna o en condiciones climáticas adversas. El proyecto de sistema de transporte inteligente más ambicioso es la autopista automatizada, donde los vehículos podrán viajar a grandes velocidades pero en cortos intervalos, mediante el uso del radar incorporado, la posición del vehículo y los sensores del motor, que actúan sobre los sistemas de aceleración y de frenado, y de conexiones informatizadas entre los vehículos.

Está muy claro que construir más carreteras no es la solución a los problemas del transporte. Mediante el uso de equipos informáticos y dispositivos de comunicación, la infraestructura de transporte (sistemas de carretera y los vehículos que los usan) puede pasar a ser más inteligente, y por lo tanto, reducir los atascos, disminuir las emisiones de los vehículos en tráfico, reducir el tiempo de viaje, aumentar la capacidad de las

carreteras existentes y hacer más seguros los desplazamientos por carretera. Los ITS pueden ser definidos como el matrimonio entre los avances en tecnologías de información y sistemas de comunicación con los vehículos y redes de caminos que forman parte del sistema de transporte. Son inteligentes debido a que proveen de información oportuna tanto a usuarios como a operadores. Utilizando estas tecnologías en conjunto con el sistema de transporte es posible salvar vidas, ahorrar tiempo y dinero.

Dentro de los autos, los sistemas ITS ayudan a los conductores a circular evitando los lugares congestionados y los accidentes. En buses y trenes, estos permiten a los operadores optimizar la operación y ofrecer a los pasajeros la compra automática de boletos e información en tiempo real. En la red de caminos, los sistemas ITS coordinados con las señales de tráfico pueden detectar y ayudar en el manejo de incidentes mostrando información, y dando consejos o instrucciones a los conductores. Entre otras funciones, a continuación se presenta una descripción más detallada de todas las posibilidades que ofrecen las ITS.

Una importante aplicación de las ITS es el Control de Tráfico: Las ITS permiten recolectar los peajes eficientemente y minimizar las demoras que implican, con lo que se reduce la congestión. Además el monitoreo continuo de ciertas áreas presenta un gran beneficio a los operadores y tomadores de decisiones los que pueden llevar a un mejor control sobre número y tipo de vehículo que pasa por cierta ruta en un período dado y así tener mayor cantidad de información disponible, de manera rápida y confiable para definir políticas de desarrollo e inversión.

1.1.2 ¿Que es NTCIP y Porque necesitamos usarlo?

El NTCIP, es una familia de datos y protocolos de comunicación que han sido diseñados para acomodar las diversas necesidades de varios subsistemas y servicios de usuarios de la Arquitectura Nacional ITS. El NTCIP tiene la intención de manejar estas necesidades en dos áreas: Centro a Centro (Center – to – Center C2C) y Centro a Campo (Center – to - Field C2F).

El NTCIP difiere de la práctica pasada de protocolos de gestión de transporte, en la que no existía un solo protocolo de comunicación diseñado para este propósito. Más bien, éste consiste de una familia entera de protocolos que cubren el espectro de los protocolos orden/respuesta Punto – Punto simple para muchas técnicas orientada de objetos sofisticados. Esto es debido a muchas razones: la diversidad de las aplicaciones dentro del cual NTCIP será como el tipo y la cantidad de datos a ser transferidos, la criticidad de los datos de tiempos transferidos, los costos aceptables de la infraestructura de comunicación y la criticidad de los datos de seguridad y la integridad del mismo.

Primero se va a definir dos términos: **interoperabilidad** e **intercambiabilidad.** El término *interoperabilidad* refleja la habilidad de múltiples dispositivos, con frecuencia de diferentes tipos, trabajando como un único sistema para un propósito en común. Por ejemplo, usar el mismo canal de comunicación para interconectar un sistema de gestión con controladores de tráfico, señales de mensaje dinámico, controles de video de vigilancia y otros dispositivos que reflejan un real mundo de ejemplo de interoperabilidad. El término *intercambiabilidad* generalmente refleja la habilidad de usar diversas marcas de un dispositivo en un mismo canal de comunicación, acompañando la habilidad de intercambiarlos en campo.

El Acto de Equidad de Transporte (TEA: Transportation Equity Act) para el siglo 21, conocido como "TEA – 21", requiere que los proyectos deben ser conforme con la Arquitectura Nacional ITS.

La Ingeniería da acceso al diseño de proyectos que emplea un proceso iterativo para desarrollar el concepto de operaciones, necesidades y requerimientos, diseño, construcción, testeo, evaluación y desarrollo de la implementación. Un enfoque del mismo requiere que el equipo del proyecto considere todas las fases de un ciclo de vida del sistema que proviene del momento de la concepción del sistema hasta su instalación. Esto significa que se toma todas las consideraciones de los estados de planeamiento, obtención del diseño, despliegue, operaciones, mantenimiento, aumento o expansión y el retiro de los sistemas y/o subsistemas. Este enfoque también requiere:

- Identificar las alternativas para cada paso del diseño y construcción del sistema.
- Evaluar los requerimientos y los diseños de impacto para cada alternativa basada en costos, consideraciones políticas y técnicas, y necesidades de los clientes.
- Considerar que riesgos existen durante el proceso y plan para su gestión.

1.2 Beneficios del NTCIP:

El NTCIP ofrece el incremento y las opciones para las agencias de operación de sistemas de gestión de transporte. Esto remueve barreras para las interagencias de coordinación y permite a los equipos de diferentes modelos y procedencias de fabricación ser mezclados en una misma línea de comunicación. Por estas razones, las agencias de operaciones se beneficiarán con el NTCIP.

1.2.1 Evitar la temprana obsolescencia:

Es posible operar una mezcla de dispositivos NTCIP y dispositivos que no tienen este protocolo en el mismo sistema aunque no en la misma línea de comunicación. Una

agencia de operación puede asegurar que su equipo permanezca útil y compatible por mucho tiempo con el soporte de NTCIP en todas las adquisiciones futuras y mejoramientos de los sistemas de gestión de transporte. Esto incluiría la adquisición de software, controladores de tráfico maestros para cualquier tipo de control de tráfico o dispositivo de monitoreo.

1.2.2 Proveer la elección del Proveedor:

Una vez que una agencia tenga un sistema central, puede adquirir otros sistemas, dispositivos de campo o software que provenga de un fabricante que ofrezca productos conforme a las normas NTCIP que pueda comunicarse con ese sistema. Puede ser el caso que solamente productos que proviene de la misma fábrica estará apto para usar totalmente la riqueza de las características con el software o el controlador que son de fabricación específica, pero la funcionalidad básica estará disponible sin importar el fabricante, provistos de los documentos necesarios para especificar las características obligatorias y opcionales que soporta los requerimientos funcionales de la agencia. Sin embargo, el NTCIP lo hará mas fácil para una agencia que cambia gradualmente su software, controladores de tráfico y otros dispositivos de campo que vienen de uno u otro fabricante, o en parte para añadir simplemente múltiples dispositivos de otros fabricantes a sus sistemas en el futuro.

Naturalmente, una agencia tiene que considerar no sólo los aspectos inherentes de interoperabilidad / intercambiabilidad del NTCIP, pero también el asunto como el stock para reemplazar las partes, el cual será diferente de proveedor a proveedor, y la base del conocimiento de los técnicos del ITS quien tendría que convertir en forma familiar con otros productos de los fabricantes.

1.2.3 Habilitar la coordinación entre diferentes Agencias:

El NTCIP permite a las agencias intercambiar información (con autorización) de las órdenes básicas que habilite a cualquier agencia para monitorear las condiciones de los otros sistemas de las agencias, y para implementar las respuestas coordinadas a los incidentes y otros cambios en condiciones de campo cuando se requiera.

Tal como el intercambio de la data y la respuesta coordinada que pueden ser implementadas. Una agencia puede monitorear, y dar las órdenes básicas, si está autorizado, a operar los dispositivos de campo por otra agencia; la coordinación de las aplicaciones potenciales entre agencias incluye:

- Coordinación a la transferencia de tiempos a un Centro de Tránsito compartido.

- Coordinación de los semáforos que cruzan los límites jurisdiccionales.
- Proveer prioridad a los semáforos a ser seleccionados, por ejemplo, tránsito vehicular.
- Proveer información en tiempo real a un centro de información al viajero.
- Monitoreo de los volúmenes de tráfico en otras agencias.
- Coordinación de la operación en una autopista con un semáforo adyacente
- Destinar un mensaje de advertencia de una señal dinámica de mensaje a la otra agencia.

1.3 Uso de una Red de Comunicaciones para Todo Propósito:

La comunicación en red es generalmente uno de los mas caros componentes de un sistema de gestión de transporte. El NTCIP permite un sistema de gestión para comunicarse con una variedad de modelos de dispositivos en el mismo canal de comunicación, asegura una máxima flexibilidad en el futuro para el uso de una mayor inversión.

El NTCIP permite a un sistema de gestión comunicarse con una variedad de dispositivos en un mismo canal de comunicación. Por ejemplo, con la añadidura de un software de aplicación apropiada en el sistema, una señal de mensaje dinámico puede ser instalado cerca de una intersección señalizada, y la computadora puede comunicarse con el controlador usando la línea de comunicación que esta en el controlador de tráfico. La red de comunicaciones es uno de los componentes más costosos en un sistema de gestión de transporte.

1.4 Tipos de Sistemas y Dispositivos Soportados por NTCIP:

El NTCIP define una familia de protocolos de comunicaciones de datos de transporte específico que soporta la mayoría de los tipos de los sistemas de computadoras y dispositivos de campo usados en la gestión de transporte. Las aplicaciones son generalmente dividido en dos categorías:

- C 2 F : Centro a Campo (Center to Field)
- C 2 C : Centro a Centro (Center to Center)

El primero, normalmente incluye dispositivos de campo, comunicándose con un software de gestión a una central de tráfico. Las aplicaciones C 2 C usualmente incluye las comunicaciones computador – computador, donde estos pueden estar en el mismo cuarto, en los centros de gestión operados por agencias cercanas. El rol que cumple el NTCIP esta ilustrado aquí:

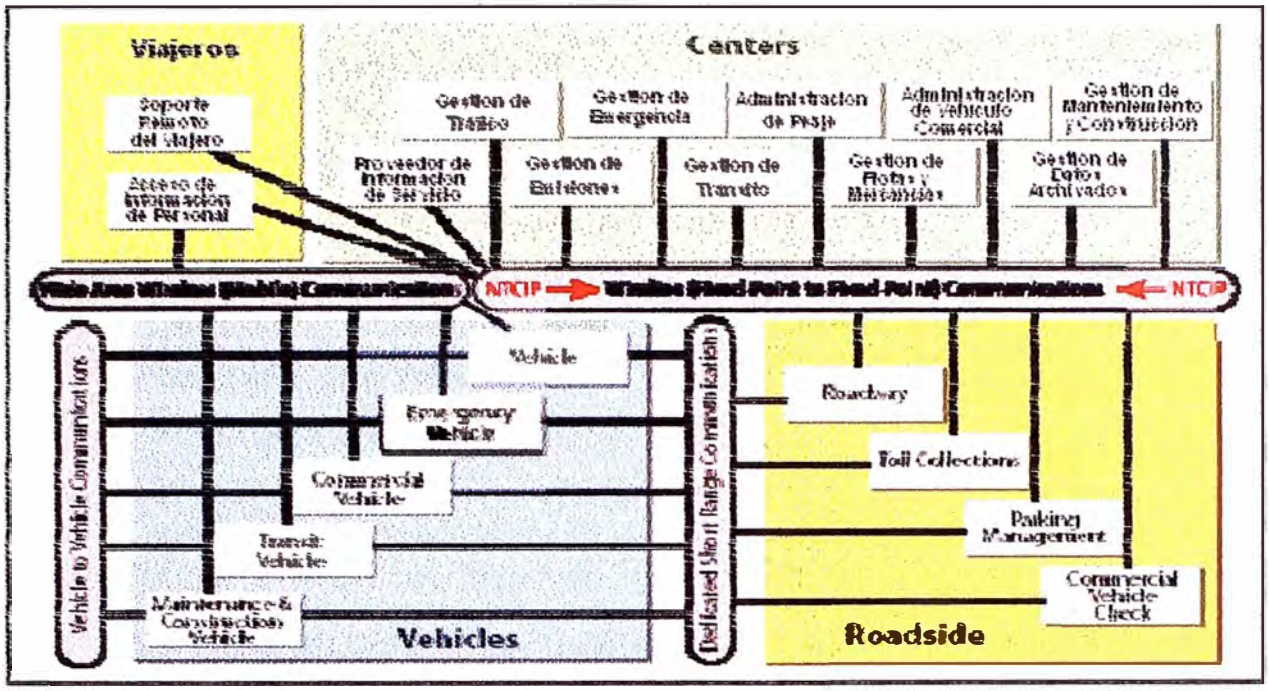

Figura 1.1: NTCIP y la Arquitectura Nacional del ITS

Para ambas aplicaciones C2F y C2C, el NTCIP soporta los sistemas y dispositivos usados en tráfico, tránsito, gestión de emergencia, información al viajero y sistemas de planeamiento / archivamiento de la data. La Figura 1.1 ilustra como varios sistemas de gestión de transporte y dispositivos pueden ser integrados usando NTCIP.

Nota: Algunas computadoras involucradas en comunicaciones C2C puede ser localizado en el campo, por ejemplo: kioscos, controladores de tráfico maestros, controladores avanzados. Los protocolos de comunicación C2C y C2F del NTCIP tienen opciones para soportar enlaces de comunicación dial-up.

- ***Centro a Campo (C2F)***
  - Señales de Mensaje Dinámico.
  - Semáforos.
  - Controladores Maestros (sistemas de lazo cerrado)
  - Dispositivos de Monitoreo y Recolección de Datos, tal como un contador de tráfico, estaciones de clasificadores de tráfico.
  - Controladores y sensores a bordo.
  - Sensores de ambiente.
  - Medidores de desnivel.
  - Detectores de vehículos.
  - Cámaras de circuito cerrado de televisión (solo el control de cámara).

- Video switches.
- Control de alumbrado de carreteras.

- ***Centro a Centro (C2C)***
  - Gestión de Tráfico (autopista, calles, urbano / rural)
  - Gestión de Tránsito (bus / tren / otros)
  - Gestión de Incidentes.
  - Gestión de Emergencia.
  - Gestión de Parqueo.
  - Información para los Viajeros (todos los modos).
  - Regulación de Operaciones de Vehículo Comercial.

Muchas aplicaciones de NTCIP están relacionados con las comunicaciones en tiempo real e involucrados con las transmisiones continuas / automáticas de datos o comandos. También soporta transmisiones humano a remoto de la máquina/sistema. Los datos pueden también ser enviados usando otras normas de comunicaciones, especialmente e-mail y los protocolos de transferencia de archivos desarrollados para Internet.

CAPITULO II

NIVELES DE COMUNICACIÓN Y PROTOCOLOS USADOS EN SISTEMAS DE TRANSPORTE INTELIGENTE

2.1 Los Niveles de Comunicación NTCIP:

El NTCIP usa un enfoque modular o en capas para las comunicaciones estándares, similar al enfoque adoptado por el Internet y la Organización Internacional de Normas (ISO). En general, las comunicaciones de datos entre dos computadoras u otros dispositivos electrónicos pueden ser consideradas para las siguientes capas primarias, llamadas "NIVELES" en NTCIP y distinguirlos de ellos por ISO y el Internet.

A través de una combinación de capas de las normas de comunicaciones existentes y algunas normas desarrollados específicamente para ITS, el NTCIP provee una familia de protocolos de comunicaciones que sirven a las necesidades comunes en la Gestión de Transporte ITS. Los Niveles en NTCIP son:

- **Nivel de Información NTCIP:** Las normas de Información definen el significado de datos y mensajes y generalmente acordar con la información de ITS (más que información acerca de la comunicación en red). Esto es similar para definir una lista de frases y diccionarios dentro de un lenguaje. Estas normas son sobre el modelo tradicional de las siete capas ISO. El nivel de información representa la funcionalidad del sistema a ser implementado.

- **Nivel de Aplicación NTCIP:** Las normas de Aplicación definen las reglas y procedimientos para el intercambio de la información de datos. Las reglas pueden incluir definiciones de una gramática propia y una sintaxis de un único acuerdo, tan bien como la secuencia de acuerdos permitidos. Esto es similar a la combinación de palabras y frases para formar una oración, y definir las reglas para acordar el intercambio de información. Estas normas son aproximadamente al equivalente de las capas de Sesión, Presentación y Aplicación del modelo OSI.

- **Nivel de Transporte NTCIP:** Las normas de Transporte define las reglas y procedimientos para intercambiar los datos de Aplicación entre el punto "A" y el punto "X" en una red, incluyendo cualquier funcion de Gestión de Ruta, Mensaje des-ensamblada / re-ensamblada y Red necesaria. Esto es similar a las reglas y procedimientos usados por la compañía de teléfonos al conectar dos teléfonos localizados remotamente. Las normas del nivel de Transporte son aproximadamente equivalente a las capas de Transporte y Red del modelo OSI.

- **Nivel de Red NTCIP:** Las normas de subred define las reglas y procedimientos para intercambiar los datos entre dos dispositivos "adyacentes" sobre algunos medios de comunicaciones. Esto es equivalente a las reglas usadas por la compañía de teléfonos al intercambiar los datos de un enlace celular vs. Las reglas usadas para intercambiar los datos sobre un cable de par trenzado. Estas normas son aproximadamente equivalente a las capas de Enlace de datos y Físico del modelo OSI.

- **Nivel de Planta NTCIP:** El nivel de Planta es mostrado en la estructura del NTCIP solamente como para de proveer un punto de referencia a ese aprendizaje acerca de las normas de comunicaciones NTCIP. El nivel de Planta incluye la infraestructura de comunicaciones sobre el cual las normas de comunicaciones de NTCIP son para ser usados y tendrán un impacto directo en la selección de un Nivel de Red para usar sobre la infraestructura de comunicaciones seleccionadas. Las normas NTCIP no prescriben cualquier tipo de medio de comunicación sobre otra. En muchos casos, se tendrá una idea de qué medios de comunicación estaremos usando en la implementación de un sistema en el diseño de una fase.

La mayoría de las normas en los niveles más bajos son normas disponibles comercialmente existentes usados en la industria de telecomunicaciones y no son desarrollados únicamente por NTCIP, aunque con frecuencia, el NTCIP especifica el cual las sub-opciones con esas normas son usados. La mayoría de las normas de ITS son encontrados en los dos primeros niveles (nivel de información y nivel de Aplicación), mostrados en el figura 2.1 y 2.2. Cada pila del protocolo NTCIP involucra una mezcla de normas, con al menos uno de cada nivel.

2.1.1 Mapeo de la Capa OSI al Nivel NTCIP:

Con los diversos requerimientos del NTCIP, no es sorprendente que veamos en el modelo de referencia OSI para ayudarnos a definir la estructura para esta nueva familia de normas. Aunque los protocolos de comunicación OSI no son ampliamente usados, el modelo de las capas permanece. El modelo OSI rompe el proceso de comunicación dentro de siete capas bien definidas. Cada capa tiene un propósito definido, generalmente independientemente de las capas adyacentes. Este gráfico muestra como los Niveles de Planta, de Subred, Transporte, Aplicación e Información de l NTCIP está indirectamente relacionado al modelo OSI.

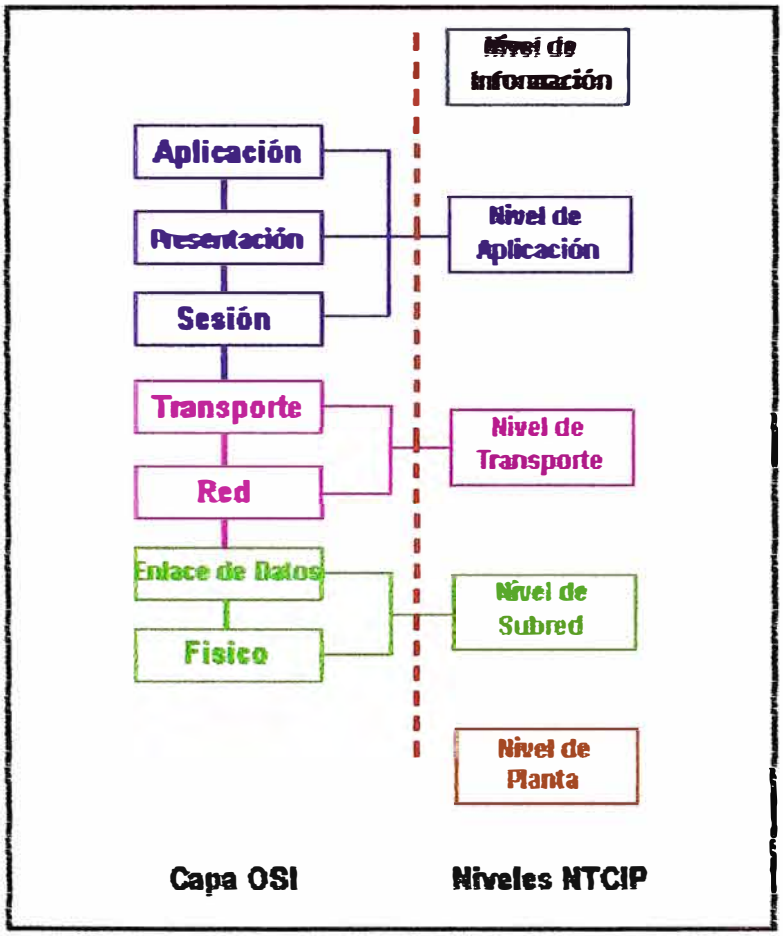

Figura 2.1 : Comparación de la Capa ISO y los Niveles NTCIP

2.1.2 Estructura del NTCIP:

Cuando las opciones están disponibles con los protocolos modulares, las opciones pueden ser diagramadas en una estructura ("framework"). Aquí se muestra la estructura para NTCIP.

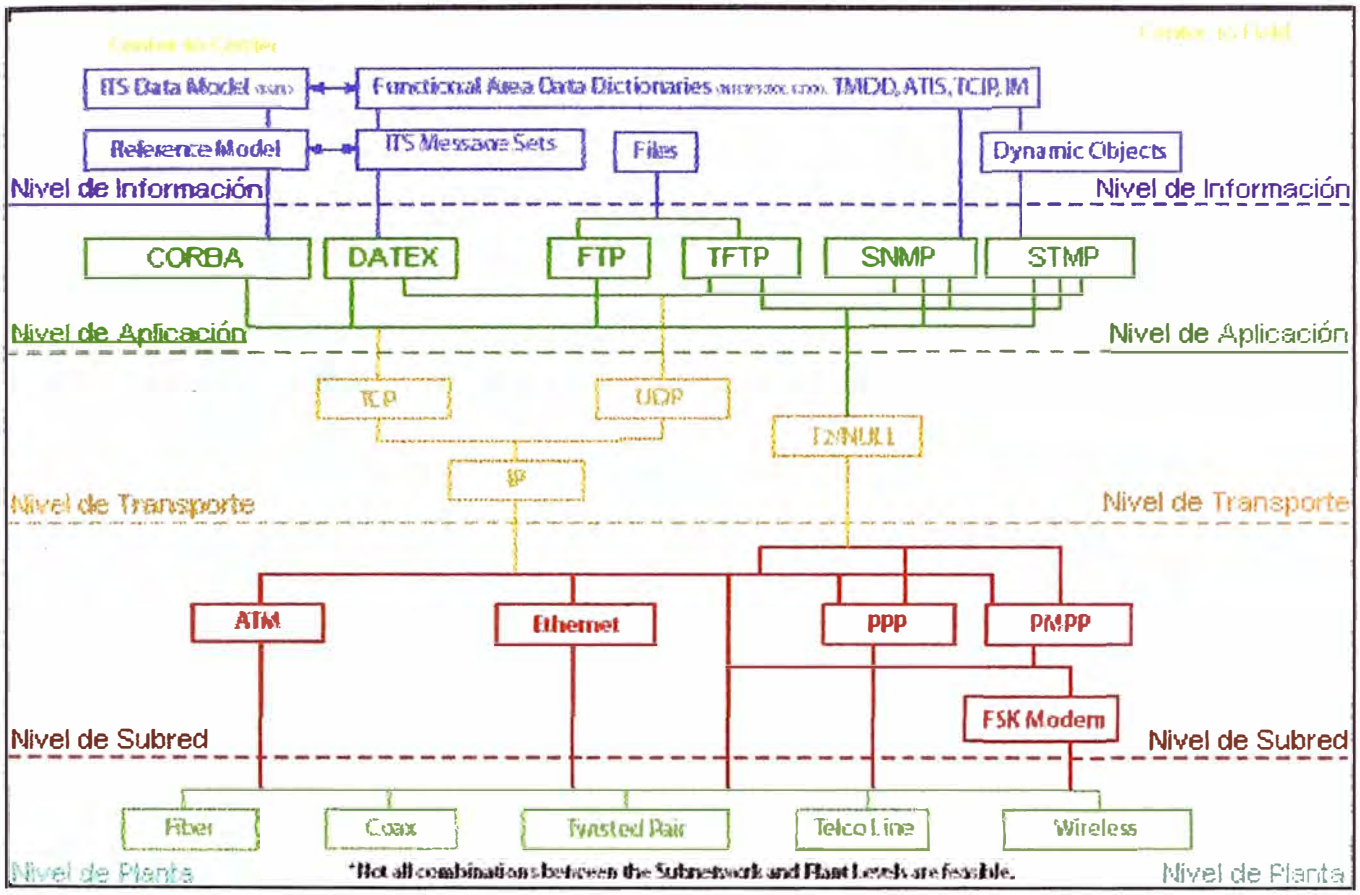

Figura 2.2: Estructura de las Normas NTCIP

En la figura 2.2 se muestra los diferentes protocolos que pueden ser escogidos de cada nivel (cajas), de los cuales, unos son compatibles (las líneas que conectan las cajas). Sin embargo, no todas las configuraciones compatibles preparan el sentido, y hay elecciones exclusivas. Por ejemplo, el funcionamiento SNMP sobre TCP/IP no es típicamente dado en la industria de la Tecnología de la información.

Una transmisión de mensaje particular puede usar al menos un protocolo de cada nivel de la estructura del NTCIP. Las series de protocolos usados en la transmisión del mensaje es llamado "Pila de Protocolo". Otras normas NTCIP definen dos cajas de los protocolos en un nivel en la trama.

Es posible que para un par de dispositivos electrónicos intercambien mensajes usando una pila y otros mensajes usando una diferente pila, aún, cuando las pilas difieran en uno o dos niveles o sub-niveles. En la figura 2.3, las líneas que conectan las normas en diferentes niveles muestran las normas opcionales de cada nivel. Si hay una línea continua (sin que se revierta la dirección) de una norma a otra, entonces son compatibles y pueden ser usados juntos como parte de una pila de protocolo.

Los niveles mostrados en la estructura son algo diferente de las capas de la pila de comunicación definidos por el modelo OSI y otras organizaciones. La pila del NTCIP se extiende más allá de las comunicaciones que incluyen interfaces y datos de información a la infraestructura de comunicaciones físicas. Los niveles y terminologías usados en NTCIP fueron escogidos por su simplicidad y fácil entendimiento para los usuarios y aplicaciones típicas en la industria del transporte.

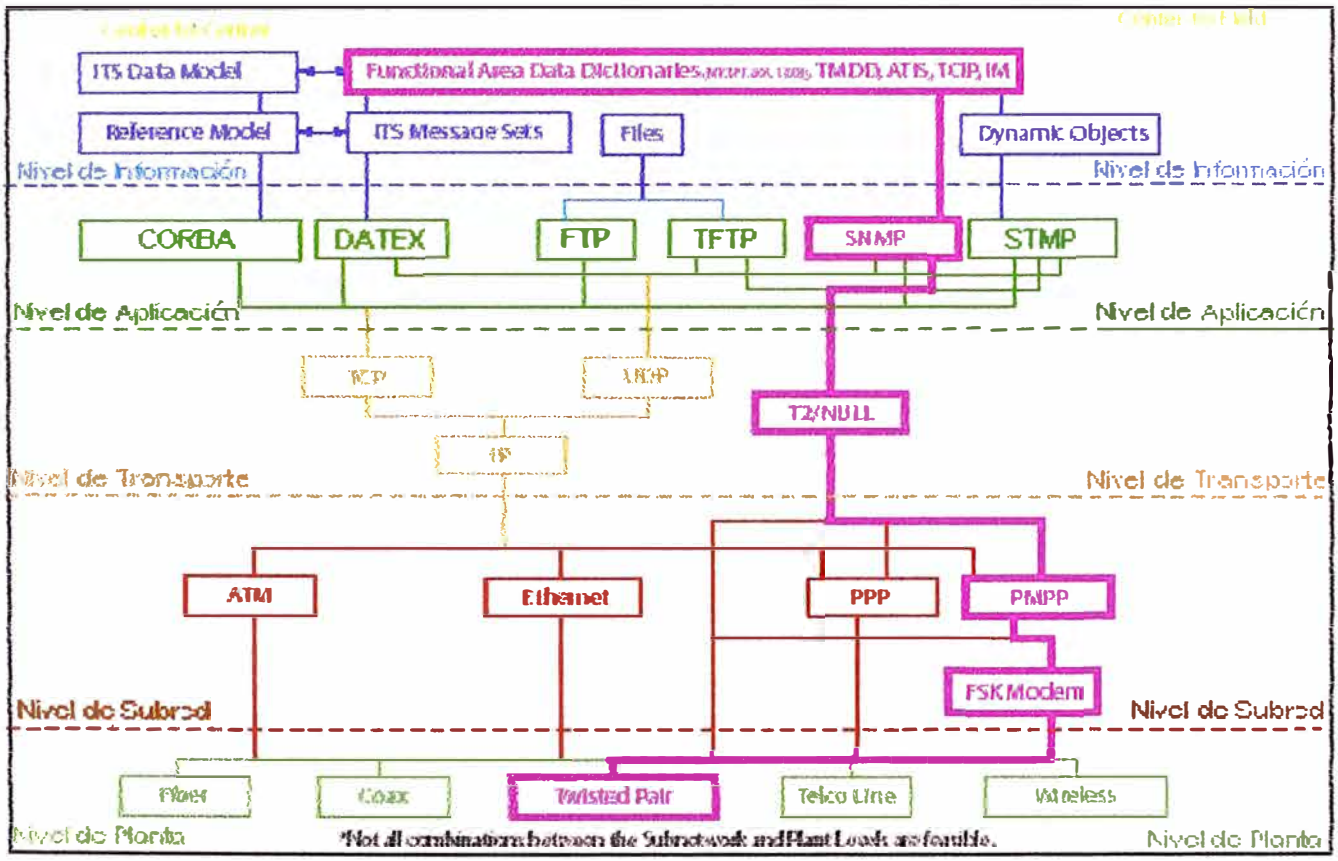

Figura 2.3: Ejemplo de la Pila Center - to - Field

2.2 Pilas de Protocolos y Normas NTCIP:

Las primeras normas NTCIP fueron desarrolladas para aplicaciones Centro a Campo (C2F). Esto involucra una *nueva* norma en el nivel de Aplicación llamado Protocolo de Gestión de Transporte Simple (*Simple Transportation Management Protocol* – STMP), una *nueva* norma en el nivel de Transporte llamado *Transportation Transport Profile* (T2 o T2/Null), y muchos conjuntos de los elementos de la data de la *nueva* norma llamado "definiciones de objetos" en el Nivel de Información. El desarrollo inicial del protocolo C2F también involucra tres normas existentes:

- Protocolo Punto a Punto (PPP).
- La personalización de la norma HDLC (High-level Data Link Control), en el nivel de Subred, conocido como Protocolo Punto – Multipunto, y
- El Protocolo de Gestión de Red Simple (SNMP) para el Nivel de Aplicación.

Las normas en el Nivel de Aplicación que el NTCIP ha definido, son brevemente descritas como sigue:

- ***Protocolo de Gestión de Red Simple (Simple Network Management Protocol - SNMP)*** – Las pilas basadas en SNMP proveen un simple, pero ineficiente ancho de banda, los protocolos para aplicaciones de C2F, basados en los protocolo de Internet del mismo nombre (SNMP). Es apropiado sólo para redes con un alto ancho de banda, o bajos volúmenes de mensajes. El SNMP ha sido diseñado por la comunidad del Internet para funcionar sobre UDP/IP, pero puede ser forzado a funcionar sobre TCP/IP o T2/Null.

- ***Protocolo de Gestión de Transporte Simple (Simple Transportation Management Protocol - STMP)*** - Fue desarrollada específicamente para el uso en la industria del transporte. Es una extensión de SNMP que permite mensajes de C2F a ser enviados más eficientemente usando objetos robots dinámicos. Los stacks basados en este protocolo son apropiados para redes con bajo ancho de banda y altos volúmenes de mensajes, incluyendo los sistemas de tráfico donde una computadora central está directamente conectada a los dispositivos de campo, sin la necesidad de rutear la información a través de algún otro dispositivo tal como controlador maestro colocado en la calle en un sistema de lazo cerrado. El STMP ha sido diseñado para funcionar sobre T2/Null desde que este soporta enlaces de bajo ancho de banda, pero puede también ser usado sobre UDP/IP o TCP/IP si el ancho de banda es apropiado.

- ***(Nuevo) Protocolo de Mensaje Reparado Simple (Simple Fixed Message Protocol - SFMP)*** – Una necesidad ha sido expresada para tener un protocolo eficiente de ancho de banda para dispositivos de campo, como controladores de cámara de circuito cerrado. El NTCIP está desarrollando SFMP para reunir esta necesidad. Desde que el SFMP no está aun completada. Aún no está incluida en la estructura del NTCIP.

- ***Intercambio de Datos (Data Exchange - DATEX)*** – DATEX provee un propósito general para el protocolo de intercambio de datos. Usa mensajes pre-definidos transmitidos por la base de los protocolos de Internet (TCP/IP y UDP/IP) en una red punto – punto. La norma base en el Nivel de Aplicación en la norma OSI, desarrollado por el grupo de trabajo NTCIP llamado DATEX-ASN.

- ***Arquitectura del Corredor del Pedido del Objeto Comun (Common Object Request Broker Architecture - CORBA)*** – CORBA es un protocolo de comunicación C2C basado en la norma de la industria de la computación del mismo nombre. Para los sistemas de objetos orientados, este habilita un alto grado de integración y algunos servicios no provistos por DATEX, pero no es apropiado para aplicaciones en tiempo real y sistemas acoplados aproximadamente.

Las normas que pueden ser usadas en cada uno de estas categorías de las pilas de protocolos son mostrados en figura 2.3.

Dos dispositivos electrónicos servirán mejor para comunicar la intercambiabilidad con otro dispositivo, si usan la misma pila de protocolo, el mismo diccionario de datos y mensajes del Nivel de Información, e implementar las mismas opciones deseadas definidas en cada una de estos protocolos y normas bases primarias, de soporte seleccionadas.

2.3 Protocolos Centro a Campo (Center – To – Field C2F):

El NTCIP provee tres opciones de protocolo del Nivel de Aplicación relacionadas para las comunicaciones C2F: El SNMP, STMP, SFMP de Internet, los cuales están ahora en desarrollo. Estos protocolos base usan el paradigma get / set-messaging usado en el SNMP. Estas opciones usan la misma base de elementos de datos, como están definidos en la serie de publicaciones de NTCIP 1200. Ellos difieren en el nivel de complejidad para implementar y los tipos de servicios ofrecidos en el resumen de servicios ofrecidos y requerimientos de implementación mostrados en Tabla 2.1 y figura 2.4.

Tabla 2.1: Comparación del SNMP y STMP

	SNMP	STMP	SFMP
¿Puede enviar algún elemento de la base de datos?	SI	SI	
Eficiencia del Ancho de Banda – inversa del paquete de cabecera.	Peor	Mejor (usando objetos dinámicos)	Bajo Desarrollo
Soporta ruteamiento y dial-up.	Opciones	Opciones	
Set de Mensajes	Soportado	Limitado a 13	
Fácil de implementación	Fácil	Difícil	

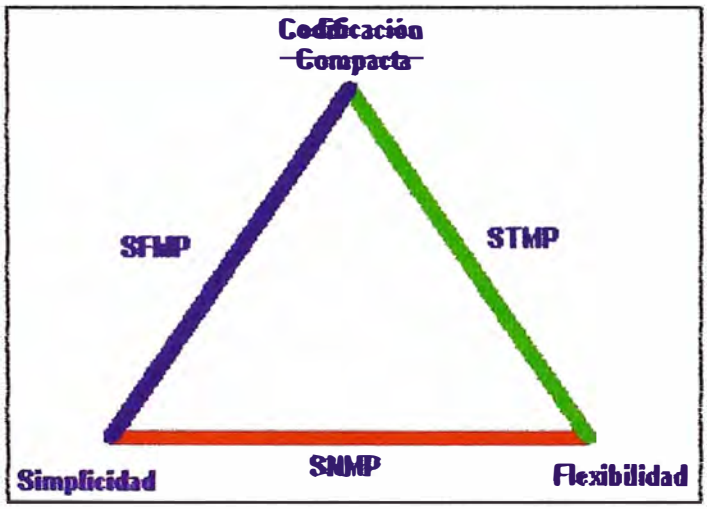

Figura 2.4: Protocolos C2F

El STMP es la opción de mayor ancho de banda eficiente apropiado e incluye un alto soporte de SNMP para las demandas de mensajes infrecuentes. Esto incluye al SNMP como un subconjunto, que cualquier sistema de gestión que implemente el STMP puede también comunicarse con un dispositivo que soporte sólo SNMP. Esto también requiere el uso de SNMP para definir objetos dinámicos. Los mensajes ocasionales requieren seguridad adicional que puede ser enviado usando SNMP. La gran ventaja de STMP es su soporte para objetos dinámicos, el cual, cuando se combina con un esquema de codificación más eficiente, se reduce dramáticamente el paquete relacionado al SNMP. Los objetos dinámicos también habilitan a los usuarios a definir los

mensajes de los clientes que están compuestos de cualquier número de elementos de datos individuales. Sin embargo, estos elementos de datos tendrán que ser definidos en la computadora central y los dispositivos de campo de modo que se trabaje adecuadamente. El STMP es la opción más flexible y de mayor ancho de banda.

Los dispositivos que usan cualquier protocolo de red particular puede compartir la misma línea de comunicación con otros dispositivos usando el mismo protocolo de red. No importa si los dispositivos tienen diferentes proveedores o son dispositivos totalmente diferentes, por ejemplo, un semáforo y una señal de mensaje dinámico. Cada dispositivo tiene asignado una dirección que es única en esa línea o canal. El sistema de gestión puede comunicarse con sólo uno de los dispositivos al mismo tiempo enviando un mensaje direccionado al dispositivo. Sin embargo, cuando se usa Protocolo Punto – Multipunto, la gestión del sistema puede comunicarse con sólo uno de los dispositivos en la línea o canal al mismo tiempo. Como una función de SNMP y STMP, los dispositivos pueden sólo enviar un mensaje al sistema de gestión cuando se requiera.

Los protocolos C2F pueden ser usados en los sistemas de gestión de cualquier configuración o complejidad. El protocolo TCP/UDP IP transporta las normas que son implementadas, luego el soporte para el enrutamiento del mensaje a través de hub's de comunicación o dispositivos de campo que están inherentemente incluidos.

El enlace de comunicación puede usar cualquier tipo de medio, tal como un cable par trenzado, cable coaxial, fibra óptica, o radio, por ejemplo: banda angosta, espectro, microondas. Los multiplexores pueden ser usados para combinar canales múltiples en un enlace troncal. Teóricamente, una tasa de transmisión de datos en el rango de 1200 a 19 200 bps. El único requerimiento que asume esa comunicación es un half-duplex, y que el tiempo de transmisión, incluye alguna demora en los dispositivos de relevo intermedio, y el tiempo de respuesta en el dispositivo final, sea razonable y dentro de las tolerancias necesitadas para permitir a todos los dispositivos a comunicarse dentro del tiempo requerido. Estos usuarios operacionales ejecutan los requerimientos, junto con la tasa de bits, tasa de sondeo y cantidad de información a ser transmitidos, determinan la máxima viabilidad de números de dispositivos en cada canal de comunicación.

El Protocolo de Gestión de Transporte (TMP) es una composición de tres protocolos distintos todos provistos de servicios cercanamente idénticos, pero diseñado para reunir los diferentes intercambios de datos y procesamiento de requerimientos. Los tres componentes de los protocolos son como sigue:

a. Simple Network Management Protocol (SNMP), versión 1.
b. Simple Fixed Message Protocol (SFMP).

c. Simple Transportation Management Protocol (STMP)

El TMP fue cuidadosamente diseñado para proveer el 100% de interoperabilidad con las normas de Internet SNMP, pero extiende esta estructura del protocolo para proveer requerimientos adicionales del ambiente del transporte. Mientras el SNMP reúna los requerimientos de flexibilidad y simplicidad de la industria del transporte, esto produce una codificación muy fecunda que no reúne los requerimientos funcionales de la existencia de la infraestructura de la comunicación. Como resultado, el esfuerzo del NTCIP produjo dos protocolos adicionales que produce una codificación mucho más compacta en el costo de la simplicidad o flexibilidad.

2.3.1 Composición del Protocolo de Gestión de Transporte (TMP)

El término TMP se refiere a la construcción de los datos que permite a los tres protocolos coexistir mientras usan el mismo protocolo identificador. Esto fue logrado debido al hecho de que todos mensajes SNMP comienzan con un byte inicial de 0x30. así, la construcción TMP ha sido diseñado para usar el valor de este primer byte para identificar el cual el protocolo esta siendo referido. El valor de 0x30 identifica un mensaje SNMP. Ambos mensajes SFMP y SNMP usan el nibble de orden más alto. El nibble de bajo orden es luego usado para identificar si el mensaje es un mensaje reparado, o uno de los 13 objetos dinámicos. El mapeo específico del primer valor del byte es definido en la tabla 2-2.

Tabla 2-2: Mapeo del Protocolo TMP

PROTOCOLO	VALOR
SNMP-Todos los mensajes SNMP (incluyendo TRAPS)	0x30
SFMP-Get Request	0x80
SFMP-Set Request	0x90
SFMP-Set No Reply	0xA0
SFMP-Get Response	0xC0
SFMP-Set Response	0xD0
SFMP-Error Response	0xE0
SMP-Trap (Reservado para futura definición)	0xF0
STMP-Get Request (Para 13 objetos dinámicos)	0x81 - 0x8D
STMP-Set Request (Para 13 objetos dinámicos)	0x91 - 0x9D
STMP-Set No Reply (Para 13 objetos dinámicos)	0xA1 - 0xAD
STMP-Get Next (Para 13 objetos dinámicos)	0xB1 - 0xBD
STMP-Get Response (Para 13 objetos dinámicos)	0C1 - 0xCD
STMP-Set Response (Para 13 objetos dinámicos)	0xD1 - 0xDD
STMP-Error Response (Para 13 objetos dinámicos)	0xE1 - 0xED
Reservado por compatibilidad con TP-T2	0x31
Reservado por compatibilidad con TP-T2	0x41

Reservado	0x00 - 0x29
Reservado	0x32 - 0x40
Reservado	0x42 - 0x7F
Reservado	0x8E - 0x8F
Reservado	0x9E - 0x9F
Reservado	0xAE - 0xB0
Reservado	0xBE - 0xBF
Reservado	0xCE - 0xCF
Reservado	0xDE - 0xDF
Reservado	0xEE - 0xEF
Reservado	0xF1 - 0xFF

Cuando la decodificación, el TMP transmite el dato entero, incluyendo el primer byte, para corregir el componente del protocolo. Cuando la decodificación, el TMP simplemente transmite el dato entero a la capa más baja sin cambiar la codificación del componente del protocolo.

a. Procesamiento Simultáneo

Una estación de gestión debe tomar dentro de una cuenta del natural procesamiento de la lista vinculante variable de TMP. En TMP, todos los objetos contenidos en un solo paquete de datos del conjunto de pedidos aparecen para ser reunidos en sus nuevos valores simultáneamente. Además, una estación de gestión no deberá combinar un cambio de estado pedido con un pedido de un conjunto de una instancia de valor asociado con el cambio de estado. Si una operación es intentado, la operación puede no ser correctamente procesado. Por ejemplo, usando un solo conjunto de comandos para cambiar ambos el estado y contenido de un objeto dinámico puede tener resultados impredecibles.

b. Lógica Identificación de Protocolo

La estructura del mapeo definido en la tabla 2-2 está basado en los siguientes principios generales representados en la figura 2.5:

** Si el primer byte es 0x30, el mensaje es un mensaje SNMP.

** Si el orden mas alto del bit del primer byte es puesto, el valor del primer byte es más grande que o igual a 0x80, el mensaje es también STMP o SNMP definido por lo siguiente:

- Si el nibble de bajo orden del primer byte es igual a 0, el mensaje es SFMP.
- Si el nibble de orden bajo del primer byte está entre 1 y 13 (0xD) inclusive y el nibble de orden alto del primer byte no es 15 (0xF), el mensaje es STMP.

- De lo contrario el mensaje no está definido.

** De lo contrario el mensaje no está definido.

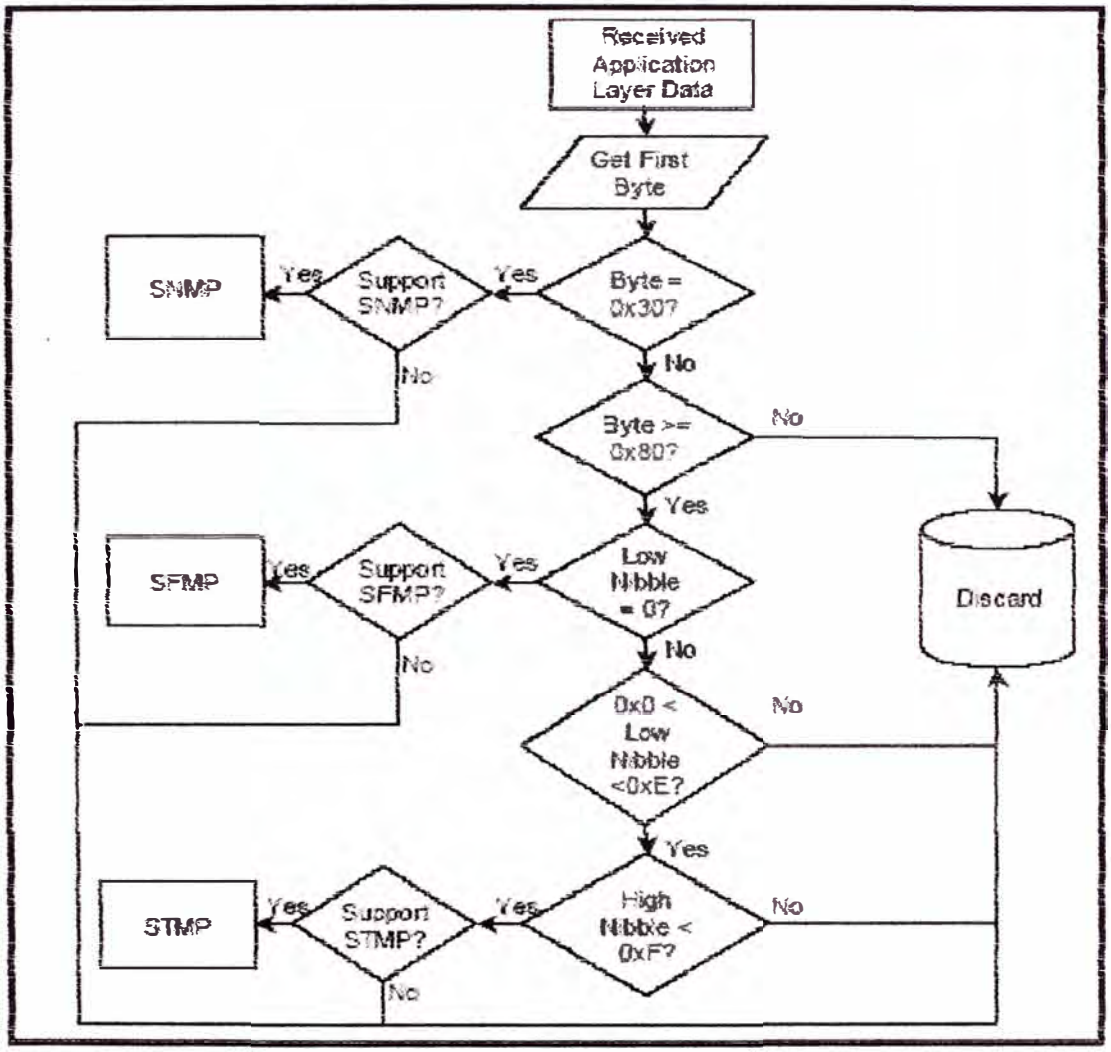

Figura 2.5: Proceso para determinar componente del Protocolo

2.3.2 Protocolo de Gestión de Red Simple (Simple Network Management Protocol - SNMP)

El SNMP es una norma mayor desarrollada por la Internet Engineering Task Force (IETF). El NTCIP seleccionó este protocolo para uso en la industria ITS debido a su amplio uso dentro de la comunidad del internet, la flexibilidad que éste provee a las estaciones de gestión para definir sus propios contenidos de los mensajes, y la simplicidad del protocolo. Mientras había preocupaciones acerca de la codificación que el SNMP impuso en las comunicaciones de datos, se decidió que el protocolo debía proveer un conjunto esencial de protocolos funcionales que puede ser desarrollado para sortear los temas.

El SNMP usa un paradigma para intercambiar las piezas individuales de los datos. Cada pieza de los datos almacenados dentro de un dispositivo y que es accesible vía

protocolo SNMP es llamado "objeto". Cada objeto consiste de dos partes: el tipo de objeto y la instancia. Algunos tipos de objetos puede solo ocurrir una vez dentro de un dispositivo, estos son llamados *objetos escalares* y son asignados a la instancia de cero (0). Otros objetos pueden tener múltiples instancias; estos objetos son llamados objetos columnares y sus instancias está basado sobre un índice con los que están asociados. La primera fila de una tabla típicamente tiene un índice de 1.

Cada tipo de objeto almacenado dentro de un dispositivo es formalmente definido en un archivo legible de computadora llamado Base de Información de Gestión (MIB). El MIB asocia cada tipo de objeto con una sintaxis precisa, una definición, y un objeto identificador, el cual es generalmente cerca de la longitud de 15 bytes. Una instancia de objeto está identificada por el agregamiento del número de instancia a esta Base del Objeto Identificador. Así, cada pieza de los datos dentro del dispositivo tiene un único número asociado con éste.

Una estación de Gestión SNMP intercambia datos por el envío de cada objeto identificador a lo largo con el conjunto de pedidos. Un solo mensaje SNMP puede y hace incluir el pedido para múltiples objetos simultáneamente. Así, cualquier paquete de datos SNMP probablemente contiene muchos de estos objetos identificadores. Asimismo, la respuesta también retorna al objeto identificador con los datos, aún para respuestas al conjunto de operaciones.

El SNMP también permite a un agente transmitir información no-solicitada llamado *TRAP*. Los datos transmitidos con la notificación del TRAP también incluye Objetos Identificadores. Una versión futura de esta norma definirá las reglas adicionales para los TRAPS dentro del ambiente NTCIP.

Este es un razonable acercamiento para intercambiar los datos cuando los datos intercambiados son infrecuentes y puede cambiar el contenido de un pedido a otro, el cual es típico del Internet. Sin embargo, dentro del ambiente del ITS, la mayoría del volumen de comunicación entre una aplicación de gestión y un agente consiste de un pequeño número de mensajes que son repetidamente intercambiados. En muchos casos, estos intercambios ocurren frecuentemente sobre canales dedicados. Así, una reducción significante en el tamaño de estos mensajes frecuentemente repetidos puede reducir significativamente el tamaño de los canales de comunicación requeridos para un enlace.

El agente SNMP deberá procesar todos los pedidos de acuerdo con esta sección, incluyendo el procesamiento del pedido para generar la transmisión de la respuesta apropiada (asumiendo que el agente SNMP tiene permiso para transmitir) dentro del máximo Tiempo de Respuesta. Si la especificación no indica el tiempo de respuesta

máximo, éste deberá ser 100 milisegundos mas un milisegundo por cada byte en la respuesta de campo variable vinculado.

2.3.3 Protocolo de Mensaje Reparado Simple (Simple Fixed Message Protocol - SFMP)

El SFMP puede ser visto como una versión simplificada, más compacta del SNMP. Un análisis cuidadoso de SNMP revela que el tamaño y complejidad de los paquetes de datos pueden ser deducidos por:

- Identificar los contenidos de los datos dentro de un paquete de datos por usar un solo identificador que refiere un grupo de elementos de datos que usa un identificador separador en asociación con cada elemento de dato en el paquete de dato.
- Definir una estructura de paquete de datos que solo incluye la información que es requerida por un tipo de mensaje dado.
- Usar un conjunto de reglas de codificación que son más suficientes que las Reglas de Codificación Básica usado por SNMP.

a. Identificación de Datos

El SFMP decrece el tamaño de la cabecera consumida por la identificación de datos de dos maneras. Primero, está diseñado con la suposición de que intercambiará un solo objeto compuesto, un objeto que consiste de una secuencia definida de otros objetos. Este enfoque disminuye la cabecera por permitir el uso de un solo objeto identificador que un identificador separador para cada componente del objeto. Segundo, el diseño del SFMP incorpora el concepto que todos los objetos compuesto será localizado bajo el nodo NEMA. Además, incluye un mecanismo de codificación de corte del objeto identificador para objetos bajo este nodo. Además, la complejidad de este protocolo es reducida debido al hecho que un agente no está pedido para manipular un conjunto de comandos con cualquier combinación de datos en cualquier orden, está solo requerido para soportar un objeto a tiempo y si el objeto es un objeto bloque, el orden de los datos esta siempre arreglado. Esto permite menos potencia y menos dispositivos complejos para soportar NTCIP.

b. Estructura del Paquete

En SNMP, todos los paquetes de datos usan una estructura de datos muy similares. Mientras esto provee algunas ventajas en el reuso de la codificación, también resulta en extra información siendo enviado en muchos de los paquetes de datos del

SNMP. Debido a la necesidad de minimizar la cabecera para los mensajes intercambiados más frecuentes y minimizar el procesamiento de requerimientos para decodificar estos bytes extras; el esfuerzo del NTCIP desarrolló la Estructura de los Paquetes de Datos SFMP para un intercambio más eficiente de los mensajes arreglados mientras aun proveen las funciones de seguridad necesarias.

c. Codificación

El SNMP codifica toda su información de acuerdo a las Reglas de Codificación Básica (BER) ASN.1. BER usa tres *tupla* para codificar los datos para la transmisión. El primer elemento de la tupla, el tipo, especifica qué tipo de datos sigue. El segundo elemento de la tupla, la longitud, especifica cuantos octetos de los datos ocupa. El tercer y último elemento de la tupla, el valor, esta la data siendo transmitido. Esta codificación está algunas veces referido como codificación TLV, el cual se entiende por "tipo", "longitud" y "valor". Esto provee un método muy flexible de codificación de información para transmisión; sin embargo, si ambos lados tienen ya acordado en una estructura de data especificado, incluye una innecesaria cabecera por incluir el "tipo" de campo y la "longitud" de campo para una longitud de data arreglada.

Como resultado, el esfuerzo del NTCIP ha definido un conjunto separado de reglas de codificación de ASN.1, conocido como Reglas de Codificación de Octetos (OER), definido en NTCIP 1102. la OER elimina el tipo de campo completamente, y elimina la longitud del campo bajo esas condiciones donde la longitud es conocida. Dado que las definiciones de Objetos (elemento de data) definidos por el NTCIP de la INTEGRACIÓN en el rango de 0 a 255. la OER es apto para reducir significativamente el tamaño de muchos paquetes de datos NTCIP.

d. Definición

Todas las implementaciones SFMP deberá ser declarada para ser una estación agente de gestión o ambos.

Las estaciones de Gestión pueden transmitir SFMP-GetRequest-PDU's, SFMP-Setrequest-NoReply-PDU's necesarios de modo que manejen los agentes. Las estaciones de gestión deberán estar aptas para recibir y procesar SFMP-GetResponse-PDU's, SFMP-SetResponse-PDU's, SFMP-ErrorResponse-PDU's por las reglas definidas dentro de esta cláusula.

Los agentes deberán estar aptos para recibir y procesar SFMP-GetRequest-PDU's, SFMP-SetRequest-PDU's y SFMP-SetRequest-NoReply-PDU's por las reglas definidas dentro de esta cláusula, incluyendo la habilidad de transmitir SFMP-

GetResponse-PDU's, SFMP-SetResponse-PDU's y SFMP-ErrorResponse-PDU's pedidos.

- **Reglas**

Similar al SNMP, las funciones de los dispositivos de todos los modelos de SFMP como alteraciones o inspecciones de variables. Esta estrategia evita la complejidad de definir un tipo de mensaje diferente como una parte de la definición de protocolo por cada comando deseado.

La comunicación entre entidades de protocolo es lograda por el intercambio de protocolos de mensajes, cada cual puede ser enteramente e independientemente representada dentro de un solo datagrama. Una implementación de este protocolo deberá aceptar mensajes válidos cuyas longitudes no excedan los 484 octetos. Sin embargo, es recomendado que las implementaciones soporten mensajes largos en cualquier momento.

Una estación de gestión debe tomar dentro de una cuenta del natural procesamiento de la lista de la variable vinculada de TMP. En TMP, todos los objetos contenidos en un solo paquete de data set-request aparece para ser seteado a sus nuevos valores simultáneamente. Además, una estación de gestión no deberá combinar un cambio de estado pedido con un pedio de setear una instancia de valor asociado con el cambio de estado. Si cada operación es intentada, la operación no puede ser correctamente procesada.

- **Elementos de Procedimiento**

Esta sección describe las acciones de una entidad de protocolo implementando el SFMP. Note, sin embargo, que no tiene la intención de obligar la arquitectura interna de cualquier implementación conforme.

Una entidad de protocolo SFMP transmite un mensaje SFMP para pasar el mensaje serializado al servicio de transporte capaz de enviar el mensaje a la entidad de protocolo par.

Un entidad de protocolo SFMP recibe un mensaje SFMP como sigue:

- Este ejecuta un análisis sintáctico rudimentario de la entrada del datagrama para construir un objeto ASN.1 correspondiente al objeto referencial. Si este análisis falla, se descarta el datagrama y no ejecuta las demás acciones.
- Este luego verifica el número de la versión del mensaje SFMP. Si hay un mal emparejamiento, este descarta el datagrama y no ejecuta las demás acciones.

- Este luego verifica el nombre de la comunidad. Si la autenticación falla, el protocolo graba un evento de autenticación fallado por incrementar el objeto SFMP-inBadCommunityNames y el objeto AgentHealth-authenticationFailures, descarta el datagrama y no ejecuta las demás acciones.
- Este luego procesa el mensaje de acuerdo a las reglas definidas.

- **Iniciando un Pedido**

Una estación de gestión SFMP puede, en cualquier momento, iniciar un set request para generar un SFMP-Data-Packet conteniendo un SFMP-GetRequest-PDU, un SFMP-SetRequest-PDU o un SFMP-SetRequest-NoReply-PDU. Las condiciones que puede resultar en la iniciación de la estación de gestión tal como un pedido son materia de la funcionalidad del fin de aplicación y están más allá del ámbito de esta norma.

Un agente SFMP no deberá tratar un SFMP-Data-Packet conteniendo un SFMP-GetRequest-PDU, un SFMP-SetRequest-PDU o un SFMP-SetRequest-NoReply-PDU. Esta restricción no deberá excluir un solo dispositivo de actuación como una estación de gestión y un agente.

- **Procesando un Pedido**

Una estación de gestión deberá dejar caer silenciosamente (descartar y no ejecutar las demás acciones en un pedido) cualquier SFMP-GetRequest-PDU, SFMP-SetRequest-PDU o SFMP-Setrequest-NoReply-PDU.

El agente SFMP deberá procesar todos los pedidos de acuerdo con las siguientes subcláusulas, incluyendo el procesamiento del pedido suficiente para generar la transmisión de la respuesta apropiada (asumiendo que el agente SFMP tiene permiso para transmitir) dentro del Tiempo de Respuesta Máxima. Si la especificación no indica el Tiempo de Respuesta máxima, este deberá ser de 100 milisegundos mas un milisegundo por cada byte en el campo de data de respuesta SFMP-PDU.

- **Procesamiento de un SFMP Get Request**

La recepción de un SFMP-GetRequest-PDU, un agente SFMP, un agente SFMP deberá responder de acuerdo a las siguientes reglas:

- ✓ Si el SFMP-GetRequest-PDU contiene un campo de información, el agente deberá dejar caer silenciosamente el paquete de la data.
- ✓ Si el valor del campo del mensaje antiguo no corresponde exactamente a un objeto disponible para conseguir operaciones en la vista relevante MIB, el agente

deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar noSuchName y el campo del error de índice deberá indicar cero (0).

- ✓ Si el valor del campo del mensaje antiguo refiere un objeto que es de un tipo agregado no accesible, el agente deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar noSuchName y el campo del error de índice deberá indicar cero (0).
- ✓ Si el tamaño del SFMP-GetResponse-Pdu excedería una limitación local, el agente deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar tooBig y el campo del error de índice deberá indicar cero (0).
- ✓ Si el valor del objeto referencial por el campo del mensaje antiguo no puede ser recuperado por razones no abarcadas por cualquier de las reglas extranjeras, el agente deberá trasnmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar geErr y el campo del error de índice deberá también indicar cero (0) o deberá indicar el elemento dentro de la estructura que esta previniendo la operación
- ✓ Si ni uno de las reglas extranjeras aplica, el agente deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-GetResponse-PDU tal que el campo del número pedido deberá ser usado en la SFMP-GetRequest-PDU y el campo de la data deberá contener la información del pedido.

- o **Procesamiento de un Pedido SFMP Set**

La recepción de un SFMP-SetRequest-PDU, un agente SFMP deberá responder de acuerdo a las siguientes reglas:

- ✓ Si el SFMP-SetRequest-PDU no contiene un campo de data, el agente deberá dejar caer silenciosamente el paquete de la data.
- ✓ Si el objeto referido por el valor del campo del mensaje antiguo esta solamente disponible para conseguir operaciones dentro de la vista relevante MIB, el agente deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar "sólo lectura" y el campo del error de índice deberá indicar cero (0).

- ✓ Si el valor del campo del mensaje antiguo no corresponde exactamente a un objeto disponible para establecer las operaciones en la vista relevante MIB, el agente deberá transmitir a la fuente del pedido un SFMP-Data-Packet conteniendo un SFMP-SetResponse-PDU. El campo del error de estado deberá indicar noSuchName y el campo del error de índice deberá ser cero (0).
- ✓ Si el contenido del campo de la data no puede analizado sintácticamente para encajarla SINTAXIS definida por el objeto referido, el agente deberá transmitir al originador del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo del error de estado deberá indicar badValue y el campo de error de índicedeberá indicar el número de campo al cual primer análisis falló.
- ✓ Si el valor del objeto referido por el campo de mensaje antiguo no puede ser alterado por razones que no abarcan cualquiera de las reglas extranjeras, el agente deberá transmitir a la fuente del pedido un SFMP-Data-Packet conteniendo un SFMP-ErrorResponse-PDU. El campo de error de estado deberá indicar genErr y el campo de error de índice deberá también indicar cero (0) o deberá indicar el elemento dentro de la estructura que está previniendo la operación
- ✓ Si ni uno de las reglas extranjeras aplica, el agente deberá asignar el valor pedido a la materia del objeto. Si el objeto es un objeto bloque, cada asignación de las subvariables especificada por el pedido deberá ser efectuada si simultáneamente se coloca con respecto a todas las asignaciones especificadas en el mismo mensaje. El agente deberá luego transmitir a la fuente del pedido un SFMP-Data-Packet conteniendo un SFMP-SetResponse-PDU tal que el campo del número pedido deberá ser usado en el SFMP-SetRequest-PDU.

- o **Procesamiento de un SFMP SetRequest-Noreply**

La recepción de un SFMP-SetRequest-NoReply-PDU, un agente SFMP deberá responder de acuerdo a las siguientes reglas:

- ✓ Si el SFMP-SetRequest-NoReply-PDU no contiene un campo de dato, el agente deberá descartar silenciosamente el paquete de la data.
- ✓ Si el objeto referido por el valor del campo de mensaje antiguo esta solamente disponible para conseguir operaciones dentro de la vista relevante MIB, el agente deberá descartar silenciosamente el datagrama y no ejecutar las demás acciones.

- ✓ Si el valor del campo de mensaje antiguo no corresponde exactamente a un objeto disponible para conseguir operaciones en la vista relevante MIB, el agente deberá descartar silenciosamente el datagrama y no ejecutar las demás acciones.
- ✓ Si los contenidos del campo de la data no pueden ser analizados sintácticamente para encajar el SINTAXIS definido por el objeto referido, el agente deberá descartar silenciosamente el datagrama y no ejecutar las demás acciones.
- ✓ Si el valor del objeto referido por el campo de mensajes antiguos no puede ser alterado por razones no abarcadas por cualquiera de las reglas extranjeras, el agente deberá descartar silenciosamente el datagrama y no ejecutar las demás acciones.
- ✓ Si ni uno de las reglas extranjeras aplica, el agente deberá asignar el valor pedido al objeto de la materia. Si el objeto es un objeto bloque, cada asignación de la subvariable especificada en el mismo mensaje.

e. Confirmación del Pedido

Un agente SFMP deberá dejar caer silenciosamente cualquier SFMP-Data-Packet conteniendo un SFMP-GetResponse-PDU, SFMP-SetResponse-PDU o SFMP-ErrorResponse-PDU.

Una estación de gestión SFMP deberá esperar a recibir un mensaje de respuesta para cada pedido transmitido, excepto un SetRequest-NoReply. Tal como, este deberá mantener una lista de pedidos sobresalientes. Cada nuevo pedido deberá ser asignado a un número pedido que no es frecuentemente usado por cualquier pedido sobresaliente. Tan pronto como este número pedido es asignado, el pedido debe ser añadido a la lista de pedido sobresaliente.

Sobre la recepción de un SFMP-SetResponse-PDU, la estación de gestión deberá analizar la data dentro de la estructura ASN.1 apropiada. Si cualquier otra información que el pedido del número está presente, el PDU deberá ser dejado caer silenciosamente. Se debe luego remover el pedido asociado que viene de la lista de pedido sobresaliente. Si la estación de gestión es incapaz de encontrar el pedido asociado, se debe registrar el error y notificar el fin de la aplicación.

Sobre la recepción de un SFMP-GetResponse-PDU, la estación de gestión deberá remover el pedido asociado de la lista de pedido sobresaliente y debe analizar el campo de la data dentro de la estructura ASN.1 apropiada. Si la estación de gestión no puede encontrar el pedido asociado o si el contenido del campo de la data no puede ser analizada propiamente, el error debe ser registrado y el fin de la aplicación notificado; de

lo contrario, la estación de gestión debe proveer el fin de la aplicación con la data analizada.

Sobre la recepción de un SFMP-ErrorResponse-PDU, la estación de gestión debe remover el pedido asociado que viene de la lista de pedido sobresaliente, registra el error y notifica el fin de la aplicación. Si la estación de gestión es incapaz de encontrar el pedido asociado, se debe registrar el error y notificar el fin de la aplicación.

La estación de gestión debe periódicamente revisar la lista de pedido sobresaliente por pedidos antiguos anormales. Sobre el descubrimiento de cualquier pedido antiguo anormal, la estación de gestión debe remover el pedido que viene de la lista de pedido sobresaliente, notifica el fin de la aplicación y registra la acción.

f. Estructura del Paquete de Datos SFM

Todos los paquetes de datos SFMP deberá conformar a la estructura general definida por SFMP-Data-Packet y deberá ser decodificada de acuerdo a las Reglas de Codificación del Octeto del NTCIP 1102.

```
SFMP-Data-Packet    –  CHOICE  {
Sfmp-get                        [ 0 ]  SFMP-getRequest-PDU,
Sfmp-set                        [ 16 ]  SFMP-SetRequest-PDU,
Sfmp-set-no-reply           [ 32 ]  SFMP-SetRequest-NoReply-PDU,
Sfmp-get-response           [PRIVATE 0]  SFMP-GetResponse-PDU,
Sfmp-set-response           [PRIVATE 16]  SFMP-SetResponse-PDU,
Sfmp-error                  [PRIVATE 32]  SFMP-ErrorResponse-PDU,

}
```

Cada uno de las estructuras PDU referidos están basados en el mismo corazón de la estructura de la data, pero son distinguidos por las reglas formales que son definidas por usar esta estructura base. Mientras este enfoque no provea un único ASN.1 para cada estructura, esto hace fácil el desarrollo de las implementaciones por tener una estructura usada para todas las operaciones. Esta estructura es la estructura SFMP-PDU, definida como sigue:

```
SFMP-PDU  : :=  SEQUENCE  {
Version                 ENUMERATED{version-1(1),...}          DEFAULT  version-1,
      Community-name    OCTET STRING                  DEFAULT "public",
```

```
Request-number      INTEGER  (0....255)          OPTIONAL,
Error-data          Error-Data                   OPTIONAL,
Message-oid         RELATIVE-OID                 OPTIONAL,
        from {iso org dod internet private enterprise nema}
data                OBJECT-TYPE.&Syntax          OPTIONAL,

}
```

Las siguientes subcláusulas definen varias reglas y subestructuras de este paquete de dato. La ciáusula 2.4 define el significado de cada campo.

- **Estructura del SFMP-GetRequest-PDU**

  La operación SFMP usa el SFMP-GetRequest-PDU:

  SFMP-GetRequest_PDU : := SFMP-PDU

  Las siguientes reglas deberán aplicarse al SFMP-GetRequest-PDU:

- ✓ El campo de la petición de número deberá estar presente.
- ✓ El campo de error de data deberá estar ausente.
- ✓ El campo del mensaje oid deberá estar presente.
- ✓ El campo de la data deberá estar ausente.

- **Estructura de SFMP-SetRequest-PDU y SFMP-SetRequest-NoReply-PDU**

El conjunto de SFMP y las operaciones del conjunto de no respuesta usan un conjunto de reglas idénticos aplicados a la estructura SFMP-PDU como está indicado abajo. La distinción entre estos dos paquetes es hecho por el valor de la elección codificada en el SFMP-Data-Packet, definida en la subcláusiua 2.3, el cual siempre envolverá la estructura PDU.

SFMP-SetRequest-NoReply-PDU : := SFMP-PDU
SFMP-SetRequest-PDU : := SFMP-PDU

Las siguientes reglas deberá aplicarse al SFMP-SetRequest-PDU y SFMP-SetRequest-NoReply-PDU:

- ✓ El campo de la petición de número deberá estar presente.

- ✓ El campo de error de data deberá estar ausente.
- ✓ El campo del mensaje oid deberá estar presente.
- ✓ El campo de la data deberá estar ausente.

- o **Estructura de SFMP-GetResponse**

  Un respuesta SFMP usa la estructura SFMP-GetResponse-PDU:

  SFMP-GetResponse-PDU : := SFMP-PDU

  Las siguientes reglas deberán aplicarse al SFMP-GetResponse-PDU:

- ✓ El campo de la comunidad nombre deberá estar ausente y por defecto "publico" en todos los casos.
- ✓ El campo de la petición de número deberá estar presente.
- ✓ El campo de error de data deberá estar ausente.
- ✓ El campo del mensaje oid deberá estar ausente.
- ✓ El campo de la data deberá estar presente.

- o **Estructura de SFMP-SetResponse**

  Una respuesta SFMP usa la estructura SFMP-SetResponse-PDU:

  SFMP-SetResponse-PDU : := SFMP-PDU

  Las siguientes reglas deberán aplicarse al SFMP-SetResponse-PDU:

- ✓ El campo de la comunidad nombre deberá estar ausente y por defecto "publico" en todos los casos.
- ✓ El campo de la petición de número deberá estar presente.
- ✓ El campo de error de data deberá estar ausente.
- ✓ El campo del mensaje oid deberá estar ausente.
- ✓ El campo de la data deberá estar ausente.

- o **Estructura del SFMP-Error Message**

  Una respuesta de error SFMP usa la estructura SFMP-ErrorResponse-PDU:

  SFMP ErrorResponse-PDU : := SFMP-PDU

```
Error-Data  : :=  SEQUENCE  {
        Error-status                Error-status,
        Error-index                 Error-Index
        }
```

Las siguientes reglas deberán aplicarse al SFMP-ErrorResponse-PDU:

- ✓ El campo de la comunidad nombre deberá estar ausente y por defecto "publico" en todos los casos.
- ✓ El campo de la petición de número deberá estar presente.
- ✓ El campo de error de data deberá estar presente.
- ✓ El campo del mensaje oid deberá estar ausente.
- ✓ El campo de la data deberá estar ausente.

2.3.4 Protocolo de Gestion de Transporte Simple (Simple Transportation Management Protocol – STMP)

Nota 1: Esta definición de STMP es 100% compatible subdesarrollado con la definición provista en NEMA TS 3.2-1996.

Nota 2: El STMP requiere SNMP o SFMP para permitir una estación de gestión para configurar los objetos dinámicos.

El STMP es conceptualmente similar al SFMP, excepto que ha sido diseñado para trabajar con objetos dinámicos como los objetos bloques definidos en el tiempo, más bien que solo un conjunto de objetos de bloques predefinidos. Esto tiene el beneficio de proveer a la estación de gestión con la flexibilidad requerida para definir su propio mensaje, pero como un resultado, este se incrementa significativamente la complejidad del software dentro del agente. Este también usa un número de las mismas truncaciones usadas por SFMP de modo que se incremente el tamaño del paquete de la data comparado con SNMP normal. Este enfoque provee una ventaja significativa y potencial en aplicaciones involucradas en los enlaces de banda ancha.

a. Objetos Dinámicos

El esfuerzo realizado para alcanzar el consenso en un pequeño conjunto de mensajes arreglados para algunos de los dispositivos mas complejos tal como los

controladores de tráfico; aun, este fuese claro que estos dispositivos serían llamados por encima a la información de estado de intercambio frecuente sobre la baja velocidad de los circuitos de comunicación. Como resultado de este análisis, el NTCIP desarrolló el concepto de un objeto dinámico, el cual es la mayor característica del STMP. Un objeto dinámico es una secuencia simple de objetos, similar al objeto bloque, pero los objetos componentes dentro de un objeto dinámico son definidos en el tiempo por la estación de administración.

- **Tabla de Configuración de Objeto Dinámico**

La *dynObjConfigTable* es una tabla indicando al propietario y el estado de cada objeto dinámico, tal como se muestra en la tabla 2-3. Debido a las razones históricas, su índice, el *dynObjNumber*, está localizado bajo un diferente nodo en el árbol del modelo ISO, pero éste no tiene un impacto operacional. El *dynObjConfigTable* tiene filas conceptuales que contiene los siguientes objetos:

Tabla 2-3: Columnas de la Tabla de la Configuración del Objeto Dinámico

dynObjNumber	dynObjConfigOwner	dynObjConfigStatus

El índice para una fila particular en el *dynObjConfigTable* esta definido por el *dynObjNumber*. Este identifica con cual de los 13 objetos dinámicos de esta fila de la tabla está asociado.

El intento del objeto *dynObjConfigOwner* es para indicar la identidad del propietario que definió el objeto dinámico.

El *dynObjConfigStatus* indica el estado del objeto dinámico. El estado permitido de cada objeto dinámico es definido por el tipo **ConfigEntryStatus**, definido en la cláusula 5.2.4.1. el estado puede ser válido (*valid*), inválido (*invalid*), o bajoCreación (*underCreation*).

- **Tabla de Definición de Objeto Dinámico**

En adición de definir el estado (y opcionalmente el propietario) de cada objeto dinámico, la estación de gestión debe también definir los contenidos deseados del objeto dinámico. Un enfoque para solucionar este problema habría sido definir una serie de campos adicionales en el dynObjConfigTable, tal como dynObjField1, dynObjField2, dynObjField3, etc., donde cada uno fue un IDENTIFICADOR DE OBJETO apuntando al objeto deseado. Sin embargo, esto habría resultado en un número largo de tipos de

objetos muy similares. En vez de eso, el esfuerzo del NTCIP definió una tabla embebida que contiene la lista de objetos. La tabla embebida, llamada la tabla *dynObjDef* usa el mismo *dynObjNumber* del índice primario, luego usa un índice secundario, *dynObjIndex*, para indicar la posición de la variable referida en el objeto dinámico.

Finalmente, el *dynObjVariable* se refiere al objeto específico a ser incluido en el campo indicado en el objeto dinámico indicado. Porque la tabla está embebida, las reglas de edición impuesta por el parámetro *dynObjConfigStatus* afecta el acceso delas celdas de esta tabla. Así, el resultado de la tabla compuesta puede ser visualizado como sigue:

Tabla 2-4: Tabla Compuesta para Configuración y Definición del Objeto Dinámico

dynObjNumber	dynObjConfigOwner	dynObjCOnfigStatus	dynObjIndex	dynObjVariable
1	<Owner of Dynamic Object # 1>	<Status of Dynamic Object # 1>	1	<OID of 1st object in dynObj 1>
			2	<OID of 2nd object in dynObj 1>
			3	<OID of 3rd object in dynObj 1>
			....	....
			255	<OID of 255th object in dynObj 1>
2	<Owner of Dynamic Object # 2>	<Status of Dynamic Object # 2>	1	<OID of 1st object in dynObj 2>
			2	<OID of 2nd object in dynObj 2>
			3	<OID of 3rd object in dynObj 2>
			....	....
			255	<OID of 255th object in dynObj 1>
3	<Owner of Dynamic Object # 3>	<Status of Dynamic Object # 3>	1	<OID of 1st object in dynObj 3>
			2	<OID of 2nd object in dynObj 3>
			3	<OID of 3rd object in dynObj 13
			.....	.....
			255	<OID of 255th object in dynObj 1>
.....	.....	.....	.....	.....
13	<Owner of Dynamic Object # 13>	<Status of Dynamic Object # 13>	1	<OID of 1st object in dynObj 13>
			2	<OID of 2nd object in dynObj 13>
			3	<OID of 3rd object in dynObj 13>
			....	....
			255	<OID of 255th object in dynObj 13>

Nota 1: La versión 1 de la Base de Información de Gestión de Transporte (TMIB) tenía un propietario y un estado para cada objeto dinámico variable. El desarrollo de la experiencia indicó que este diseño era menos que lo ideal y así las norma fue cambiada con Amendment 1 en 1998. Los objetos originales, los objetos *dynObjOwner* y *dynObjStatus* son descritos. Esto aseguró que cada objeto dinámico tendría sólo un único propietario y estado en cualquier tiempo.

Nota 2: La versión del TMIB también definió un nodo *dynObjData* que contenía un objeto SNMP por cada objeto dinámico. La intención era permitir una estación de gestión SNMP para ganar el acceso de algunos de los beneficios de la codificación compacta de la data, pero el desarrollo de la experiencia proveyó que este diseño era menos que el ideal y entonces estos objetos fueron despreciados.

- **Objetos Dinámicos y Sistemas de Operación**

El STMP soporta 13 objetos dinámicos por cada agente. En teoria, la estación de gestión puede configurar cada dispositivo con un diferente conjunto de objetos dinámicos, pero en la práctica, la mayoría de estaciones de gestión son probablemente para configurar dispositivos similares con definiciones de objetos dinámicos similares.

- **Otras Truncaciones**

Porque hay un pequeño número de objetos dinámicos definido por el protocolo, el identificador del mensaje sólo requiere cuatro bits más que los múltiples bytes. El STMP también toma las ventajas de otra codificación y diseño de truncaciones para minimizar el tamaño del paquete de la data. Por ejemplo, una contraseña no es requerido porque los objetos dinámicos son definidos a tiempo; un nivel bajo de seguridad ya esta provista por el hecho que la estructura del flujo de la data no es publicado en una norma.

- **Definición**

Todas las implementaciones STMP deberán ser declarados para ser estación de gestión, agente o ambos. Las estaciones de gestión pueden transmitir STMP-GetRequest-PDU's, STMP-GetNextRequest-PDU's y STMP-SetRequest-NoReply-PDU's tan necesarios para administrar agentes. Las estaciones de gestión deberán ser capaces de recibir y procesar STMP-GetResponse-PDU's, STMP-SetResponse-PDU's y STMP-ErrorResponse-PDU's por las reglas definidas dentro de esta cláusula.

Los agentes deberán ser capaces de recibir y procesar STMP-GetRequest-PDU's, STMP-GetNextRequest-PDU's, STMP-SetRequest-PDU's y STMP-SetRequest-NoReply-PDU's por las reglas definidas dentro de esta cláusula, incluyendo la habilidad de transmitir los STMP-GetResponse-PDU's, STMP-SetResponse-PDU's y STMP-ErrorResponse-PDU requeridos.

- **Reglas**

Similar al SNMP y SFMP, los modelos STMP de todas las funciones de los dispositivos como alteraciones o inspecciones de variables. Esta estrategia evita las

complejidades de definir un diferente tipo de mensajes como una parte de la definición del protocolo para cada comando deseado.

La comunicación entre las entidades del protocolo es lograda por el intercambio de los mensajes de protocolo, cada uno del cual puede ser enteramente e independientemente representada dentro de un solo datagrama. Una implementación de este protocolo deberá aceptar cualquier mensaje válido cuya longitud no exceda los 484 octetos. Sin embargo, las implementaciones pueden soportar mensajes más largos.

Una estación de gestión debe tomar en cuenta el natural procesamiento de la lista de variable vinculada del TMP. En TMP, todos los objetos contenidos en un solo conjunto de petición del paquete de la data aparecen para ser puesto a sus nuevos valores simultáneamente. Por tanto, una estación de gestión no deberá combinar una petición de cambio de estado con una petición para poner una instancia de valor asociado con ese cambio de estado. Si dicha operación es intentada, la operación no puede ser correctamente procesada. Esta regla aplica a ambos, el proceso para configurar un objeto dinámico tan bien como la ejecución de un objeto dinámico.

b. Elementos de Procedimiento

Esta sección describe las acciones de una entidad de protocolo implementando el STMP. Se nota, sin embargo, que este no tiene la intención de obligar la arquitectura interna de cualquier implementación conforme.

Una entidad de protocolo SNMP transmite un mensaje STMP por pasar el mensaje serializado a un servicio de transporte capaz de enviar el mensaje al par de la entidad del protocolo.

Una entidad de protocolo STMP recibe un mensaje STMP como sigue:

* Este ejecuta un análisis rudimentario de la entrada del paquete de datos para construir una estructura conteniendo el Tipo de Mensaje, el Identificador de Objeto y la data asociada contenida en el Campo de la Información. Si el análisis falla, si uno de los campos contenía data inválida, la entidad del protocolo descarta el paquete de data y no ejecuta las demás acciones.
* La entidad del protocolo luego procesa el mensaje de acuerdo a las reglas definidas anteriormente.

- **Iniciando una Petición**

Una estación de gestión SNMP puede, en cualquier momento, iniciar un get o una puesta de operación por generar un STMP-Data-Packet conteniendo un STMP-GetRequest-PDU, un STMP-GetNextRequest-PDU, un STMP-SetRequest-PDU, o un

STMP-SetRequest-NoReply-PDU. Las condiciones que pueden resultar en la estación de gestión iniciando un pedido son la materia de la funcionalidad del fin de la aplicación y están más allá del ámbito de esta norma.

Un agente STMP no deberá emitir un STMP-Data-Packet conteniendo un STMP-GetRequest-PDU, un STMP-GetNextRequest-PDU, un STMP-SetRequest-PDU o un STMP-SetRequest-NoReply-PDU. Esta restricción no deberá excluir un solo dispositivo de actuación, ambos, una estación de gestión y un agente.

- **Procesando una Petición**

Una estación de gestión deberá dejar caer silenciosamente cualquier STMP-GetRequest-PDU, STMP-GetNextRequest-PDU, SFMP-SetRequest-PDU o SFMP-SetRequest-NoReply-PDU.

El agente STMP deberá procesar todos los pedidos de acuerdo con las siguientes subcláusulas, incluyendo el procesamiento del pedido suficientemente para generar la transmisión de la respuesta apropiada (asumiendo que el agente STMP tiene permiso para transmitir) dentro del Tiempo de respuesta máximo. Si la especificación no indica el Tiempo de respuesta máxima, ésta deberá ser 100 milisegundos más un milisegundo por cada byte en la respuesta de la campo de Información STMP PDU.

- **Procesando un STMP Get Request**

Sobre la recepción de un STMP-GetRequest-PDU, un agente STMP deberá responder de acuerdo a las siguientes reglas:

- ✓ Si el STMP-GetRequest-PDU contiene una información de campo, el agente deberá dejar caer silenciosamente el paquete de la data.
- ✓ La materia del Objeto Dinámico deberá ser definida para ser el Objeto Dinámico que tiene un dynObjNumber, el cual es igual al valor del campo Identificador de Objeto.
- ✓ Si el dynObjConfigStatus de la Materia del Objeto Dinámico no es válido, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto identificador deberá indicar la Materia del Objeto Dinámico, el campo del error de estado deberá indicar noSuchName, y el campo de error de índice deberá indicar cero (0).
- ✓ Si la Materia del Objeto Dinámico contiene un Objeto Referido, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-

ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto dinámico, el campo de error de estado noSuchName y el campo de error de índice deberá indicar el número dynObjIndex del problema del Objeto Referido

- ✓ Si el tamaño del get-response excedería una limitación local, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto Dinámico, los campos de error de estado deberán indicar tooBig y el campo de error de índice deberá indicar cero (0).
- ✓ Si el valor de la Materia del Objeto Dinámico no puede ser recuperado por razones no cubiertas por cualquiera de las reglas precedentes, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar genErr y el campo de error de índice deberá indicar el elemento dentro de la estructura que esta previniendo la operación, al menos que sea conocido, en cualquier caso deberá indicar a cero (0).
- ✓ Si ninguna de las reglas precedentes aplica, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-GetResponse-PDU tal que el campo del identificador de Objeto deberá indicar el número del objeto dinámico y el campo de la data deberá contener a la Data del Objeto Dinámico.

- o **Procesando un STMP Get Next Request**

Sobre la recepción de un STMP-GetNextRequest-PDU, un agente deberá responder de acuerdo a las siguientes reglas:

- ✓ Si el STMP-GetRequest-PDU contiene una información de campo, el agente deberá dejar caer silenciosamente el paquete de la data.
- ✓ La materia del Objeto Dinámico deberá ser definida para ser el Objeto Dinámico que tiene un dynObjNumber, el cual es igual al valor del campo Identificador de Objeto
- ✓ Si el dynObjConfigStatus de la Materia del Objeto Dinámico no es válido, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto identificador deberá indicar la Materia del Objeto Dinámico, el campo del error de estado

deberá indicar noSuchName, y el campo de error de índice deberá indicar cero (0).

- ✓ Si la Materia del Objeto Dinámico contiene un Objeto Referido, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto dinámico, el campo de error de estado noSuchName y el campo de error de índice deberá indicar el número dynObjIndex del problema del Objeto Referido
- ✓ Si el tamaño del get-response excedería una limitación local, el agente deberá transmitir al creador de la petición un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto Dinámico, los campos de error de estado deberán indicar tooBig y el campo de error de índice deberá indicar cero (0).
- ✓ Si el valor de la Materia del Objeto Dinámico no puede ser recuperado por razones no cubiertas por cualquiera de las reglas precedentes, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Objeto Identificador deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar genErr y el campo de error de índice deberá indicar el elemento dentro de la estructura que esta previniendo la operación, al menos que sea conocido, en cualquier caso deberá indicar a cero (0).
- ✓ Si ninguna de las reglas precedentes aplica, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-GetResponse-PDU. El campo del Identificador de Objeto deberá contener el número del objeto dinámico de la Materia del Objeto Dinámico y el campo de la data deberá contener la Data del Objeto Dinámico para el Objeto Dinámico.

- o **Procesando un STMP Set Request**

Sobre la recepción de un STMP-SetRequest-PDU, un agente STMP deberá responder de acuerdo a las siguientes reglas:

- ✓ La Materia del Objeto Dinámico deberá ser definido para ser el Objeto Dinámico que tiene un dynObjNumber el cual es igual al valor del campo del Identificador de Objeto
- ✓ Si el dynObjConfigStatus de la Materia del Objeto Dinámico no es válido, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo

un STMP-ErrorResponse-PDU. El campo del Identificador de Objeto deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar noSuchName y el campo de error de índice deberá indicar cero (0).

- ✓ Si la Materia del Objeto Dinámico contiene un Objeto Referido que esta sólo disponible para obtener operaciones, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Identificador de Objeto deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar "readOnly" (solo lectura) y el campo de error de índice deberá indicar el número dynObjIndex del Objeto Referido.
- ✓ Si los contenidos del campo de Información no pueden ser analizados para encajar la SYNTAX definida por el objeto referido, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Identificador de Objeto deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar badValue y el campo de error de índice deberá indicar el número de campo al cual el análisis falló.
- ✓ Si cualquiera de los Objetos referidos de la Materia del Objeto Dinámico no puede ser alterado por razones no cubiertas por cualquiera de las reglas precedentes, el agente deberá transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-ErrorResponse-PDU. El campo del Identificador del Objeto deberá indicar la Materia del Objeto Dinámico, el campo de error de estado deberá indicar genErr y el campo de error de índice deberá también indicar cero (0) o debrá indicar que el elemento dentro dela estructura que está previniendo la operación.
- ✓ Si ninguna de las reglas precedentes aplica, el agente deberá asignar los valores pedidos a la Materia del Objeto Referidos. Cada asignación del Objeto Referido especificado en el mismo mensaje. El agente deberá luego transmitir al creador del pedido un STMP-Data-Packet conteniendo un STMP-SetResponse-PDU tal que el campo del número pedido deberá ser el mismo como el que fue usado en el set request.

- o **Procesando un STMP SetRequest-NoReply**

Sobre la recepción de un STMP-SetRequest-NoReply-PDU, un agente STMP deberá acordar las siguientes reglas:

- ✓ La materia del objeto dinámico, deberá estar definida para ser el Objeto Dinámico que tiene un dynObjNumber el cual es igual al valor del campo Identificador de Objeto.

- ✓ Si el dynObjConfigStatus de la Materia del Objeto Dinámico no es igual al válido, el agente deberá descartar el paquete de la data y no ejecutar acción alguna.
- ✓ Si alguno de los Objetos Referidos en la Materia del Objeto Dinámico está solo disponible para conseguir operaciones, el agente deberá descartar el paquete de data y no ejecutar acción alguna.
- ✓ Si los contenidos del campo de la data no puede ser analizado para encajar la SYNTAX definida por el objeto referido, el agente deberá descartar el paquete de data y no ejecutar acción alguna.
- ✓ Si el valor de cualquiera de los Objetos Referidos no puede ser alterado por razones no cubiertas por cualquiera de las reglas precedentes, el agente deberá descartar el paquete de data y no ejecutar acción alguna.
- ✓ Si ninguna de las reglas precedentes se aplica, el agente deberá asignar los valores pedidos a los Objetos Referidos. Cada asignación del Objeto referido especificado por la petición deberá ser efectuada como si el conjunto simultáneamente con respecto a las otras asignaciones especificadas en el mismo mensaje. El agente no deberá transmitir cualquier respuesta.

- **Confirmación del Pedido**

Un agente STMP deberá caer silenciosamente cualquier STMP-Data-Packet conteniendo un STMP-GetResponse-PDU, STMP-SetResponse-PDU o STM-ErrorResponse-PDU.

Sobre la recepción de un STMP-GetResponse-PDU, la estación de gestión deberá analizar el campo de la data dentro de la estructura apropiada ASN.1. si los contenidos del campo de la data no puede ser analizado propietariamente, el error deberá ser logueado (registrado) y el fin de la aplicación notificado; de lo contrario, la estación de gestión debe proveer el fin de la aplicación con la data analizada.

Sobre la recepción de un STMP-SetResponse-PDU, la estación de gestión deberá analizar la data dentro de la estructura apropiada ASN.1. Si cualquier campo de información está presente, el PDU deberá dejarse caer silenciosamente. Esto debe luego remover el pedido asociado de la lista de pedidos sobresalientes. Si la estación de gestión no es capaz de encontrar el pedido asociado, este debe loguear (registrar) el error y notificar el fin de la aplicación.

Sobre la recepción de un mensaje de error, la estación de gestión debe registrar el error y notificar el fin de la aplicación.

c. Estructura del Paquete de Data STMP

El paquete de data STMP está definido para tener un campo de cabecera, y un campo de información (o PDU). El campo de cabecera puede ser además subdividida dentro de un Bit de Formato PDU, el cual es siempre uno, un campo de bit de tipo de mensaje, el cual es tres bits en longitud, y un campo de bit identificador de objeto dinámico el cual tiene 4 bits de longitud. Esto está mostrado en la figura 2.5:

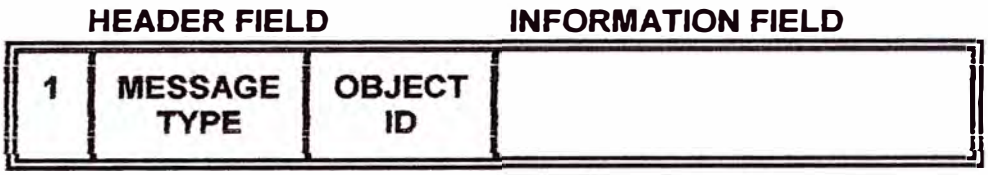

Figura 2.5: CAMPOS STMP PDU

d. Campo de Cabecera (HEADER FIELD)

El campo de cabecera deberá ser un byte de longitud. Es el mismo byte usado por TMP de modo que multiplexe los tres protocolos componentes dentro de una sola estructura. Tal como, la tabla 3-4 provee un mapeo entre los posibles valores para este campo y los propios significados. La siguiente tabla provee una explicación más del campo de cabecera específicamente para STMP.

Tabla 2-5: Contenido del Campo de Cabecera en STMP

BIT	CONTENIDO	Descripción
7	Formato PDU	
	0	Reservado por TMP para SNMP y cualquier otro uso futuro.
	1	Indica que el paquete es STMP o SFMP.
6 - 4	Tipo de Mensaje	NOTA: Las siguientes descripciones para este (Tipo de Mensaje) campo aplica sólo a los paquetes STMP (p.e., cuando el Formato PDU es 0x1 y el Objeto ID está entre 0x0001 y 0x1101)
	000	Un STMP-GetRequest-PDU es contenido dentro del paquete.
	001	Un STMP-SetRequest-PDU es contenido dentro del paquete.
	010	Un STMP-SetRequest-NoReply-PDU es contenido dentro del paquet e.
	011	Un STMP-GetNextRequest-PDU es contenido dentro del paquete.
	100	Un STMP-GetResponse-PDU es contenido dentro del paquete (ACK positivo).
	101	Un STMP-SetResponse-PDU es contenido dentro del paquete (ACK positivo).
	110	Un STMP-ErrorResponse-PDU es contenido dentro del paquete.
	111	Reservado por TMP para uso futuro.

3 - 0	ID Objeto	
	0000	Reservado por TMP para SFMP
	0001 – 1101	ID de "objeto dinámico" de STMP.
	1110	Reservado por TMP para uso futuro.
	1111	Reservado por TMP para uso futuro.

e. Campo de Información PDU

El campo de información deberá ser vacia para STMP-GetRequest-PDU's, STMP-GetNextRequest-PDU's y STMP-SetResponse-PDU's.

El campo de información para STMP-GetResponse-PDU's, STMP-SetRequest-PDU's y STMP-SetRequest-NoReply-PDU's deberá ser la estructura de la Data del Objeto Dinámico definido por 5.2.4.3.

El campo de información PDU de un STMP-ErrorResponse-PDU deberá sólo contener el estado de error y la información del índice de error de acuerdo a la siguiente estructura:

```
STMP-ErrorResponse-PDU ::=
        SEQUENCE {
                Error-status
                  ErrorStatus,
                Error-index
                  ErrorIndex
        }
```

f. Configuración de Objeto Dinámico

Como se expuso en 3.1.1, las tablas de objetos dinámicos usa el campo dynObjVariable para definir el contenido de cada objeto dinámico; cada objeto referido por un dynObjVariable es anexado a un Objeto Referido.

- **Estado de la Entrada de Configuración (Configuration Entry Status)**

El tipo ConfigEntryStatus deberá ser usado para manejar las tablas de Definición de Objeto Dinámico (tabla dynObjDef) y de la Configuración de Objeto Dinámico (tabla DynObjConfig). Para cada objeto dinámico hay un objeto columnar que es definido con un SYNTAX de ConfigEntryStatus.

Todos los otros objetos columnares para la materia de objeto dinámico deberá tener operaciones limitadas por los valores corrientes del objeto ConfigEntryStatus en la fila. El significado de los valores es como sigue:

Si la corriente de estado del objeto ConfigEntryStatus es *inválido*, la información en la correspondiente fila de la tabla dynObjConfig y las correspondientes filas de la tabla dynObjDef con el mismo índice dynObjNumber deberá ser considerado indefinido. Poniendo el estado del objeto a inválido, tiene el efecto de invalidar y limpiar las correspondientes filas de la Tabla de definición de Objeto Dinámico. Esta es una implementación específica si el agente limpia los valores contenidos en las filas invalidadas o redestina la memoria asociada con las filas inválidas. Cuando el estado inválido, el agente deberá rechazar cualquier petición para ir a un estado válido.

Si la corriente de estado del objeto ConfigEntryStatus está *underCreation* (bajo creación), la memoria para las correspondientes filas de la tabla dynObjTable con el mismo índice dynObjNumber deberá haber estado destinada para modificar los valores de los objetos contenidos en las filas asociadas de la tabla. Una vez que esta operación está completada, la estación de gestión puede poner el estado a válido; alternativamente, la estación de gestión puede cancelar la operación por poner el estado a *inválido*.

Si la corriente de estado del objeto ConfigEntryStatus es válido, la correspondiente fila de la tabla dynObjConfig y las correspondientes filas de la tabla dynObjDef con el mismo índice dynObjNumber contiene información que es creída para ser *válido*.

La tabla 2-6 indica las acciones que deberá tomar lugar sobre la recepción de un conjunto de pedidos para cambiar el estado de dynObjConfigStatus. El valor de cada celda en la tabla muestra el resultado de recibir el conjunto de pedidos indicados (cabeza de columna) cuando el dispositivo está en el estado de corriente indicado (cabeza de filas).

Tabla 2-6: Estado de Transición para ConfigEntryStatus

		ESTADO PEDIDO		
		Inválido	*underCreation*	*Válido*
ESTADO DE CORRIENTE	*Inválido*	inválido (1)	underCreation (6)	Inválido (3)
	underCreation	inválido (2)	underCreation (3)	válido (4) o undercreation (5)
	Válido	inválido (2)	válido (3)	válido (1)

Notas:

(1) Ninguna acción toma lugar y la respuesta indica noError.

(2) El estado cambia a inválido, todas las entradas asociadas con el objeto ConfigEntryStatus son borrados o limpiados y la respuesta indica noError.
(3) Ninguna acción toma lugar pero la respuesta indica badValue.
(4) Si la Validación del Objeto Dinámico fallas luego el estado permanece *underCreation* y la respuesta indica genErr.
(5) El estado cambia a *underCreation* y la respuesta indica noError.

Sobre la recepción de un conjunto de pedidos para el estado válido cuando en el estado *underCreation*, el agente deberá intentar para validar la data del objeto dinámico contenido en las filas asociadas de la tabla dynObjDef con el mismo dynObjNumber del pedido asociado. Si la validación es exitosa, el estado deberá cambiar a válido, de lo contrario, el estado permanece en el estado underCreation y el dispositivo deberá retornar a genErr.

- **Validación Objeto Dinámico**

La configuración de un objeto dinámico debe ser validado previo para usar el objeto dinámico; el proceso de validación es activado como se definió en 3.2.4.1. Cuando la validación de la configuración de un objeto dinámico, una agente deberá ejecutar las siguientes revisiones consistentes:

* Para la fila donde dynObjIndex iguala a 1, el dynObjVariable deberá apuntar a un Objeto Referido.

Para cada valor de dynObjIndex otro que 1, el dynObjVariable asociado deberá estar puesto a su valor por defecto, o ambos, el dynObjVariable asociado y el dynObjVariable previo deberán apuntar a un Objeto Referido.

La falla para pasar estas revisiones consistentes deberá prevenir el estado de cambiar a válido. Una vez definido y validado, la data referida por el objeto dinámico deberá ser accesible vía STMP.

- **Estructura de la Data del Objeto Dinámico**

La estructura de la Data del Objeto Dinámico, tan usado dentro del campo de información PDU de algunos mensajes STMP, deberá consistir de una serie de campos de componentes, cada codificación a un Objeto Referido, con el primera codificación de campo el valor del último Objeto Referido del Objeto Dinámico. Cada componente de campo deberá consistir de la codificación OER de la materia del componente.

2.4 Ejemplos

Los siguientes ejemplos demuestra (1) el proceso de configurar un objeto dinámico, (2) la recuperación del objeto dinámico configurado as través de un STMP consigue, y (3) la colocación de un objeto dinámico a través de un conjunto de STMP.

2.4.1 Configurando un Objeto Dinámico

La figura 2.6, demuestra el proceso de configurar un objeto dinámico que consiste de los siguientes objetos, en orden:

(1) globalTime.0,

(2) globalDaylightSaving.0,

(3)controller-standardTimeZone.0 y

(4) eventClassDescription.1.

La selección de estas cuatros objetos por el ejemplo provee un robusto ejemplo de cómo los mensajes STMP son codificados. Es asumido que el lector entienda la codificación de los mensajes SNMP referido como hay una variedad de libros sobre esta materia.

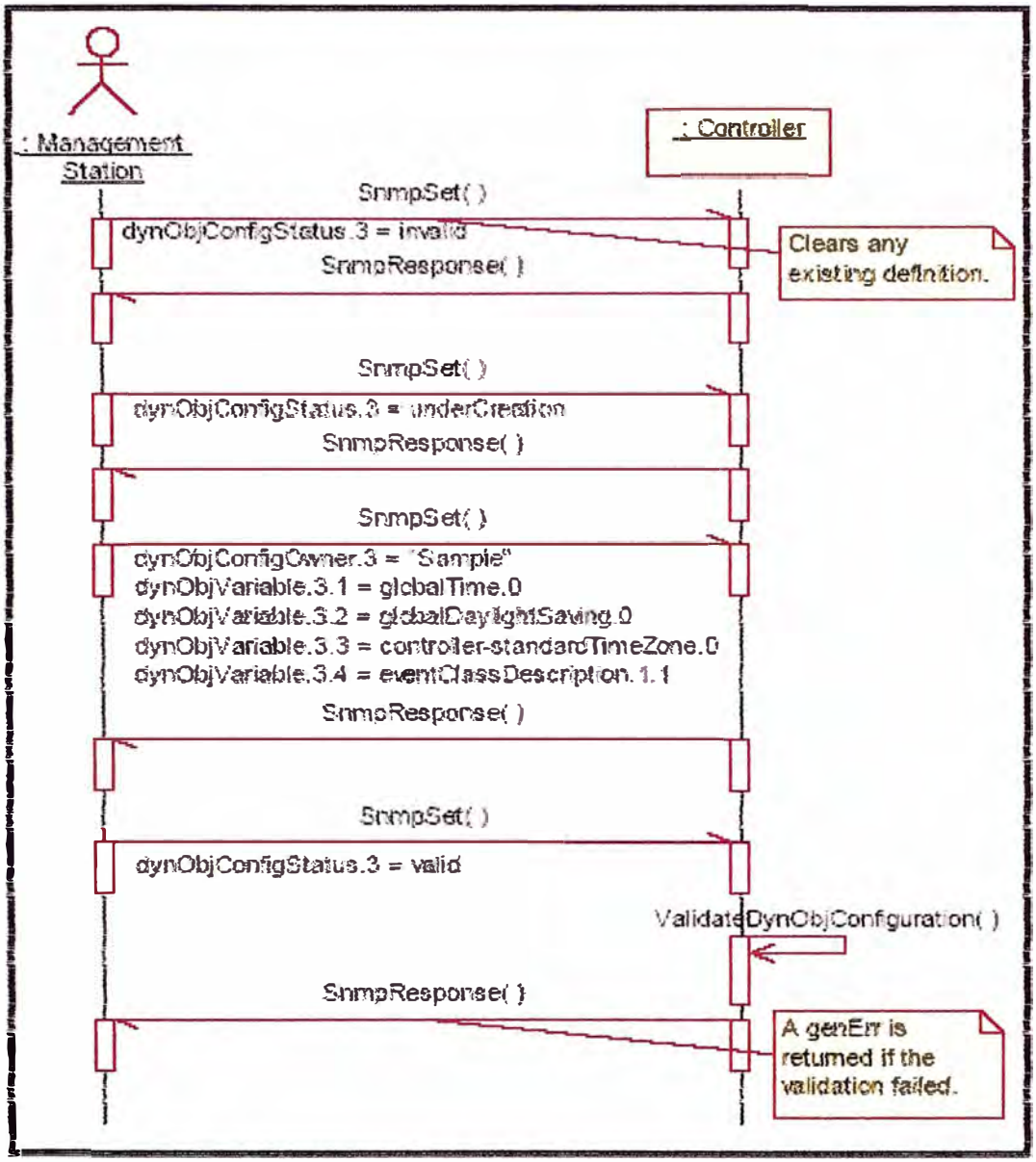

Figura 2.6: Configurando un objeto dinámico.

2.4.2 Consiguiendo un Objeto Dinámico

Una estación de gestión es apto para recuperar los objetos dinámicos definidos por emitir el uno byte STMP-GetRequest-PDU, como sigue:

83 stmp-get para objeto dinámico # 3.

Este comando causará el agente para generar un STMP-GetResponse-PDU como sigue:

C3 stmp-get-response para objeto dinámico # 3

	Information field
3A 24 63 20	variable 1= globalTime.0 = November 14, 2005 at 2:00 am UTC
03	variable 2 = globalDaylightSaving.0 = 3 = enableUSDST
FF FF B9 B0	variable 3 = controller-standardTimeZone.0 = -18000 = EST
06 53 61 6D 70 6C 65	variable 4 = eventClassDescription.1 (6 bytes) = "Sample"

Y la respuesta sería un solo byte como sigue:

D3	stmp-get-response para objeto dinámico # 3

2.5 SEGURIDAD

El TMP provee un nivel básico de seguridad. Sin embargo, el propósito primario del diseño de seguridad TMP es prevenir a los usuarios autorizados al sistema de acceder la data por cualquier de ellos que no estén autorizados.

La seguridad contra los usuarios desautorizados debe ser provisto por servicios de capas más bajas. Por ejemplo, dentro de un sistema multi-drop dedicado, un alto grado de seguridad es provisto por el hecho que la misma capa física es físicamente segura de los típicos hackers. Asimismo, en la red dial-up, las normas NTCIP recomiendan el uso de los Protocolos de Autenticación Challenge – Handshake (CHAP) de manera q se autentique la entidad remota. Si los niveles adicionales de seguridad son deseados, soluciones off-the-self, tal como la Capa de Socketes Segura, son totalmente compatibles con los protocolos NTCIP.

El mecanismo de seguridad provisto por TMP es dependiente sobre el cual de los tres protocolos componentes están en uso.

2.5.1 Seguridad SNMP y SFMP

El SNMP y el SFMP usan un esquema de seguridad común basado en un simple proceso de autenticación. Todos los paquetes de la data SNMP y todos los paquetes de la data pedidos del SFMP incluyen un campo de nombre de comunidad. El campo de Nombre de comunidad es una cadena de octeto no-encriptado que se asocia el pedido con un grupo usuario. Un agente puede ser configurado para proveer diferentes grupos de usuarios con niveles de variación del acceso de la data a través del uso de las vistas del MIB.

Una vista MIB es un término bien definido de la comunidad SNMP y detalló información acerca las vistas de MIB está disponible en una variedad de textos. En

general, permite a los objetos que están definidos como lectura-escritura para ser vistas como si ellos fuesen solo-lectura.

El mecanismo para configurar la visibilidad de la data por cada nombre de comunidad es provisto por el nodo de seguridad del TMP MIB definido en el anexo A. Este nodo define un objeto para mantener el nombre de la comunidad del administrador. El nombre de comunidad del administrador deberá proveer el acceso a todos los objetos definidos en el dispositivo MIB.

El nodo de seguridad también define una tabla de seguridad que consiste de las columnas para un índice, un nombre de comunidad y una máscara de acceso. Cada bit del acceso de máscara es un valor booleano que indica si un grupo de objetos son lectura-escritura o solo-lectura para un nombre de comunidad dado. La asignación de objetos a bits del fabricante específico, excepto por el hecho que los siguientes objetos no deberán ser asignados por cualquier bit y deberá ser visto como no-accesible por todos los nombres de comunidad dentro de la tabla (esta restricción no aplica el nombre de comunidad administrador):

a. Todos los objetos bajo el nodo de seguridad
   {Seguridad global de dispositivos de transporte nema}
b. Todos los objetos bajo el tipo de nodo
   {Tipos de capas de los protocolos de transporte nema}
c. Cualquier objeto tan identificado por varios dispositivos estándares.

2.5.2 Seguridad STMP

El STMP provee un nivel básico de seguridad basado en el hecho que el paquete de la data no está auto-definido. En cambio, el contenido de cada paquete de la data requiere cada entidad del protocolo tener un conocimiento previo de la configuración de cada objeto dinámico. Esta información de la configuración es sólo accesible vía SNMP o SFMP.

Los siguientes objetos no deben ser asignados por cualquier dynObjVariable:

a. Todos los objetos bajo el nodo de seguridad
   {Seguridad global de dispositivos de transporte nema}
b. Todos los objetos bajo el nodo dynObjMgmt
   {dynObjMgmt de los protocolos de transporte nema}
c. Todos los objetos bajo el tipo de nodo}

{Tipo de capas de protocolos de transporte nema}

d. Cualquier objeto tan identificado por varios dispositivos estándares

2.6 Infraestructura de Comunicaciones para Centro a Campo (Center-To-Field):

Cuando se planea una red de comunicaciones C2F que involucra dispositivos de campo, por ejemplo, un sistema de semaforización, es importante considerar la relación entre los siguientes items variables:

1. Tasa de transmisión (Tasa de Bits).
2. Método de Transmisión, por ejemplo, full o half-duplex, secuencial u overlap.
3. Demora de transmisión (incluyendo cualquier modem/radio)
4. Demora de respuesta en el dispositivo de campo (tiempo de recepción de requerimiento a envío de respuesta).
5. tiempo entre dispositivos o entre ciclos de sondeo (si lo necesita).
6. Longitud del mensaje(s) a ser enviado (definiciones de objetos dinámicos)
7. Frecuencia de cada tipo de mensaje (por segundo, por minuto, por día).
8. Número de dispositivos compartidos en la misma línea o canal.
9. Frecuencia de comunicación.

Aunque el STMP es diseñado para el uso con canales de comunicación que usa una tasa de transmisión lenta, como 1200 bps, no es un ancho de banda eficiente como la mayoría de protocolos usados en el pasado. Con la infraestructura de comunicaciones existentes, no puede ser posible mantener el mismo periodo de polling con el mismo número de dispositivos por canal. Esto es debido al hecho que los protocolos propietarios son optimizados para cada equipo del fabricante y consiste de muy pocos mensajes cortos arreglados sin ninguna flexibilidad en términos de cambiar estos mensajes, mientras los protocolos de la norma son flexiblemente diseñados para acomodar todas las necesidades y una amplia variedad de información y mensajes en un ambiente multi-fabricante.

CAPITULO III

DEFINICION DE LOS PROTOCOLOS

3.1 Protocolo Centro a Centro (Center – to – Center)

El NTCIP entregó originalmente dos opciones alternativas de protocolos del nivel de aplicación para comunicaciones C2C; DATEX (DATex Exchange) y CORBA. Estos dos protocolos diferentes fueron encontrados necesarios para reunir la variedad de requerimientos en el intercambio de la data entre sistemas. Más recientemente, había sido incrementado el interés en usar el XML y tecnologías relacionadas para los enlaces C2C debido a su simplicidad y al acceso del ancho de herramientas para proveer estos servicios.

El DATEX fue diseñado para dotar de simplicidad, costo efectivo de soluciones para necesidades básicas. Es especialmente bien idóneo para:

- Sistemas que requieren tiempo real, transferencia de data rápida, por ejemplo; la data del estado de la señal de tráfico.
- Sistemas con ancho de banda de comunicaciones limitadas pero alto carga de transferencia de la data.
- Sistemas con eventos infrecuentes que manejaron intercambios sobre los enlaces dial-up.
- Sistemas de objetos no orientados.

En cambio, el CORBA provee muchas características para soportar redes conectando los sistemas orientados a los objetos, y asumiendo la potencia de procesamiento suficiente y el ancho de banda de las comunicaciones son provistas, pueden ser usadas por todas las aplicaciones entre tales sistemas. El software orientado a los objetos puede tomar todas las ventajas del CORBA e implementarlo fácilmente, esto es mucho más dificultoso de lograr con el software de procedimiento tradicional.

Los desarrollos corrientes son divididos justamente aun entre la DATEX y el CORBA, con muy pocas implementaciones del XML.

Las redes C2C permiten a cada sistema pedir cualquier información disponible de cualquier sistema. Cada sistema puede ser configurado para aceptar o rechazar cualquier pedido. La "data" puede ser de información o puede constituir una orden para tomar alguna acción. Por ejemplo, en DATEX, dependiendo del tipo de mensaje, puede representar un comando para implementar el patrón de tiempo en una señal de tráfico particular o grupo de señales, o este puede representar un reporte del estado indicando que este patrón de tiempo fue solo implementado en una señal de tráfico particular o grupo de señales.

Usando CORBA, un sistema puede automáticamente y dinámicamente "descubrir" la disponibilidad de la data y las opciones de control compartido de otros sistemas. Estos otros sistemas usan la estructura CORBA para publicar sus capacidades y servicios ofrecidos, aceptan registros pedidos de clientes autorizados. Por ejemplo, el sistema de gestión de tráfico CORBA que posee un Circuito Cerrado de Televisión CCTV puede ofrecer al proveedor: (1) la imagen adquirida como (a) snapshot, o (b) video streaming, y (2) permite el control remoto del movimiento de esa CCTV. El sistema posee el CCTV es el "servidor" y el sistema pregunta por las imágenes, y / o el control de la CCTV es el "cliente".

Las comunicaciones C2C requieren una conexión de red par a par entre las computadoras involucradas. Esto es típicamente una red de área local, una red de área amplia o una conexión dial-up. Las redes de área local típicamente usan los cables de par trenzado o fibra óptica. Las red de área amplia usan enlaces de telecomunicaciones comerciales tal como el frame-relay, líneas alquiladas T1 fraccionales, paquetes de radio, o "redes privadas virtuales" (VPN) alquiladas. Las conexiones Dial-up usan ISDN, v.90 o modems similares sobre líneas de "teléfonos claramente antiguas". Cualquier tipo de enlace de comunicación puede ser usado, tan largo como este habilita el uso de los Protocolos de Ruteamiento y Transporte de Internet (TCP/IP y UDP/IP) y tiene suficiente ancho de banda para la carga de las comunicaciones planeadas para lograr la ejecución operacional deseada (esto está basado sobre la frecuencia, tamaño de mensajes para ser intercambiados, y la latencia encontrada usando sistemas C2C.

3.1.1 DATEX (Intercambio de la Data – DATa Exchange)

El DATEX (DAta EXchange) debe ser usado cuando hay una conexión entre dos o más subsistemas de gestión ITS. Un ejemplo de esto es un centro de operaciones de

tráfico conectado a un centro de operaciones de tránsito. Cada subsistema puede ser visto como la consistencia de las interfaces siguientes como se muestra en la figura 1:

- Interface de Aplicación.
- Interface de Operador.
- Interface de Comunicación.
- Interface de Base de datos.

La definición de Perfiles de Aplicación y sus funciones y responsabilidades son definidos en NTCIP 8003:1999. El perfil funcionará en enlaces de comunicación de baja velocidad, aunque el ancho de banda no fue un diseño de primera consideración. La funcionalidad de la capa más baja tal como routing, segmentación, revisión de error de paquetes y transmisión de byte nivel de los paquetes de datos son direccionados por los perfiles de Transporte y Subred.

Este perfil de Aplicación no requiere un perfil de Transporte particular o Perfil de Subred. Ha sido diseñado para trabajar con Perfiles de Transporte sin conexión, pero también trabaja con Perfiles de Transporte de conexión orientada.

Las estructuras de mensaje definido por la Capa de Aplicación son definidos usando la Unica Notación de Sintaxis Abstracta (ASN: Abstract Syntax Notation One). El ISO 14827-2 requiere apoyo de las Reglas de Codificación Básica (BER: Basic Encoding Rules) y permite el soporte de reglas de codificación adicionales a través de un esquema de negociación. Esta norma requiere el soporte adicional de las reglas de codificación del Octeto de modo que se conserve los recursos de comunicación mientras se promociona una única solución durante toda nuestra industria.

a. Lista de Requerimientos del Perfil

Una especificación de Conformidad de Implementación del Perfil (PICS) para una implementación es generado por un implementador o suministrador por indicar el nivel apropiado de soporto provisto por una implementación.

Para reclamar una conformidad con este perfil, una implementación deberá satisfacer los requerimientos de conformidad obligatoria de este perfil.

- El implementador de protocolo, como un checklist o revisión de la lista para reducir el riesgo de falla para conformar a la norma a través del descuido.
- El suministrador y usuario, como una comunicación detallada de las capacidades de la implementación.

- El usuario, como una base para inicialmente revisar la posibilidad de interactuar con otra implementación.
- Un usuario, como la base de los tests de selección apropiada contra el cual se valora el reclamo para la conformidad de la implementación.

b. Notación:

Las siguientes notaciones y símbolos son usados para indicar el estado y el estado condicional en el PRL y PICS dentro de todas las normas NTCIP. No todas estas notaciones y símbolos pueden ser usados dentro de esta norma.

Símbolos de Estado:

Los siguientes símbolos son usados para indicar la norma base y estado de perfil.

Tabla 3-1: Símbolos de Estado

Símbolo	Descripción
m	Mandatory (obligatorio)
m.<n>	Soporte de cada item del grupo etiquetado por el mismo numeral <n> requerido, pero solamente es activo en el tiempo.
o	Opcional
o.<n>	Opcional, pero soporta al menos uno de los grupos de opciones etiquetados por el mismo numeral <n> es requerido.
c	Condicional
n/a	No aplicable (ej.: lógicamente imposible en el ámbito del perfil)
x	Excluido o prohibido

La notación **o.<n>** es usado para mostrar un conjunto de opciones seleccionables (ej.: uno o mas del conjunto debe ser implementado) con el mismo identificador **<n>**. Dos combinaciones de caracter se refiere son usados par los requerimientos de conformidad dinámica. En este caso, el primer carácter se refiere al estado estático (implementación), y el segundo se refiere a la dinámica (uso); asi **"mo"** significa "obligatorio para ser implementado, opcional al ser usado". Los requerimientos de la norma base son mostrados usando las notaciones equivalentes en el caso superior.

La clasificación de los requerimientos y opciones en Internet RFC's no corresponden a la convención descrita anteriormente y deberá ser mapeada dentro del perfil como sigue:

Tabla 3-2: Clasificación del Perfil del RFC

RFC	Perfil
MUST	Obligatorio [3]
SHOULD	Obligatorio [3]
MAY	Opcional
MUST NOT	Prohibido
SHOULD NOT	Prohibido

Notación de Estado Condicional:

Las siguientes notaciones son usadas:

Tabla 3-3: Notación de Estado Condicional

<predicate>:	Esta notación presenta un único item que es condicional en el <predicate>:
<predicate>: :	Esta notación presenta un grupo de items, todos de los cuales son condicionales en el <predicate>:

La notación **<predicate>**: significa que el estado siguiente se aplica solamente cuando los estados PRL o PICS que la característica o características identificadas por el predicate son soportados. En el caso mas simple, el <predicate> es la etiqueta de identificación de un item de PICS. La notación <predicate>:: significa que cuando el grupo predicate es verdadero, luego la cláusula asociada debe ser completada. El símbolo <predicate> también puede ser una expresión booleana compuesta de muchos índices, "AND", "OR" y "NOT" deberán ser usados para indicar las operaciones booleanas.

3.1.2 CORBA (Arquitectura del Corredor de Pedido del Objeto Común - Common Object Request Broker Architecture)

Antecedentes:

A inicios del desarrollo de ITS, la necesidad parla integración del center – to – center fue considerado secundario a la integración del centro con su propia infraestructura de campo. Sin embargo, fue solo cuestión de tiempo antes del crecimiento rápido del desarrollo del ITS elevada por la necesidad.

Al principio, el lugar de iniciación lógica para la norma de protocolos de comunicaciones centro a centro fue la extensión de las especificaciones del Protocolo de Clase C, el cual esta basado por encima de la pila de comunicación ISO. Esto pronto se convirtió en la extensión del protocolo de clase C para manejar muchos sistemas heterogéneos que pueden típicamente componer un corredor regional, sería impráctico.

Esto requeriría todas las capas de la pila de comunicación a ser especificado y un gran número de servicios tendrían que ser desarrollados en todos los sistemas participantes para asegurar la interoperabilidad. Como una alternativa, una propuesta fue hecha por una norma de objeto orientado diseñado especialmente para sistemas distribuidos. El resultado fue una propuesta para especificación del protocolo centro a centro basado sobre la Arquitectura del Corredor de Pedido del Objeto Común (CORBA: Common Object Request Broker Architecture). El CORBA va a proveer una estructura de trama sobre el cual puede ser aplicado las especificaciones para los enfoques particulares y requerimiento de servicios que caracteriza una red de transporte multicentro.

El Perfil de Aplicación del CORBA provee una norma de interoperabilidad para la Capa de Aplicación y Presentación para las comunicaciones entre los subsistemas de gestión dentro del ITS. Su propósito primario es definir la interacción entre las aplicaciones del ITS y las aplicaciones del CORBA soportando la interoperabilidad del ITS.

Un perfil define una combinación de las normas base y/u otros perfiles que colectivamente ejecutan la función indicada. La definición de Perfiles de Aplicación y sus funciones y responsabilidades son definidas dentro de la cláusula 2 de AASTHO/NEMA TS 3.PRO-199x. Este perfil se refiere a las normas ISO aprobadas y propuestas por el modelo OSI. La capa de Sesión es definida como siendo NULL porque la capa de Aplicación seleccionada manipula esta funcionalidad.

La capa de Transporte, usando TCP, es aumentado por códigos de aplicaciones dentro del CORBA. Figura 3.1: ilustra las capas que son direccionadas y el principio de protocolos o normas que son aplicables a estas capas.

Capas OSI	Esta Norma
Aplicación	CORBA
Presentación	CORBA = GIOP
Sesión	NULL *IIOP* (no definido en esta norma)
Transporte	
Red	
Enlace de datos	
Físico	

FIGURA 3.1: Principio de Normas Base Direccionadas en este Perfil

Requerimientos de Arquitectura

No hay una arquitectura específica, pero las suposiciones es que hay una relación Cliente/Servidor entre los subsistemas conectados definidos. Este perfil es diseñado para usar las capas de Sesión, Transporte, Red, Enlace de Datos y Físico del modelo OSI.

Requerimientos de la Capa de Presentación

1. Protocolos Host-to-Host

La implementación del protocolo Inter-ORB General en la cima de del protocolo del nivel de transporte IIO-TCP es obligatorio para CORBA.

2. Requerimientos de la Capa de Transporte

La capa de Transporte deberá conformar el protocolo de nivel de transporte del TCP definido en TBD, la capa de transporte deberá ser aumentada con el Protocolo de Internet Inter.-ORB (IIOP) definido en CORBA.

CAPITULO IV

REQUERIMIENTOS Y ALTERNATIVAS

4.1 Enfoque de la Ingeniería:

Hay ciertos pasos que deben ser tomados en cualquier proyecto de Obtención de los Sistemas para lograr reunir las metas trazadas. Usando un enfoque de la Ingeniería a la obtención e implementación provistas para las revisiones y balanceos necesitados para asegurar que todos los requerimientos de los proyectos son identificados y documentados, y que los requerimientos correctos son correctamente implementados. La Figura 4.1 presenta un modelo de ingeniería de sistemas típico que las organizaciones podrían usar cuando consideran la obtención y la implementación de los dispositivos y/o software NTCIP.

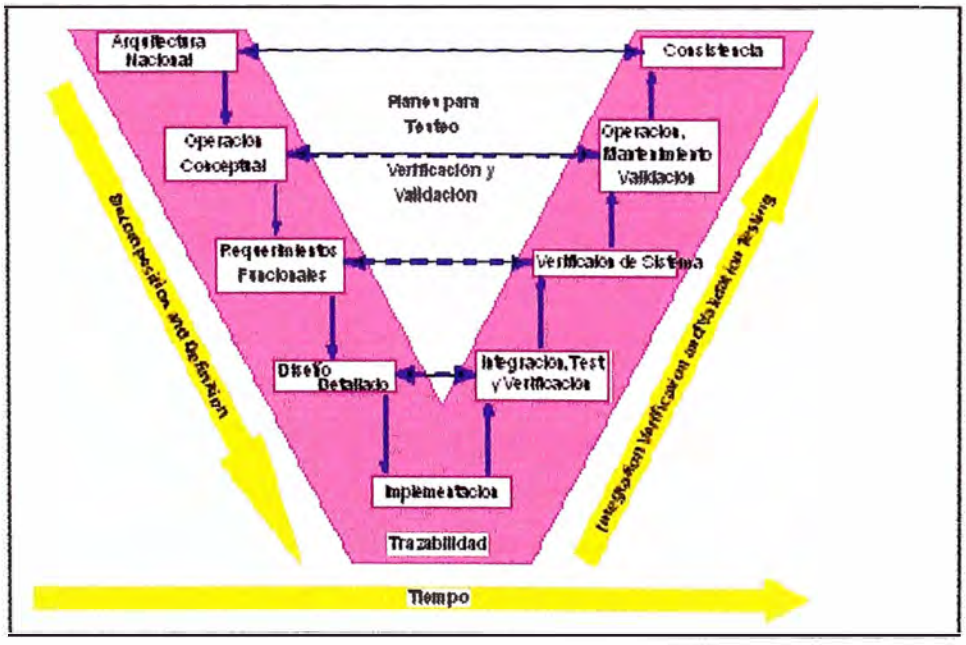

Figura 4.1: Ejemplo de Modelo de Ingeniería

El enfoque de la Ingeniería puede ser representado gráficamente a través del uso de un modelo. La forma general del modelo es en forma de la letra "V", como se muestra en la figura anterior. Esto es importante de notar que este modelo es simplemente la representación gráfica de un proceso que debe ser seguido durante todo el ciclo de vida de un proyecto.

Por favor note que mientras Figura 4.1 muestra el modelo como un simple gráfico de dos dimensiones, hay también una tercera dimensión. El grosor puede también ser usado para representar la cantidad de esfuerzo en cualquier plataforma dada. Como resultado, el botón de la "V" sería más grueso que el tope como la mayoría del costo y actividad son típicamente asociadas con la implementación del proyecto de sistemas.

El lado izquierdo de la "V" representa la decisión de preparar procesos que deben venir antes de la construcción e implementación del sistema actual. Se advierte cómo cada tarea añade más detalles. Parte de este detalle debe también considerar y proveer para las funciones del lado derecho del modelo. Por ejemplo, durante la descomposición y definición del proceso, los diseñadores también deben considerar cómo el sistema será testeado y operados últimamente.

Correr a través del modelo es también el elemento de "Trazabilidad", el cual ayuda a ilustrar que los requerimientos del sistema desarrollados durante la descomposición y definición de procesos son mapeados para especificar el testeo y verificación de procesos. Considerar un requerimiento de proyecto que indica un sistema de señal de tráfico debe acomodar las 24 fases vehiculares.

Un proceso debe también ser identificado para testear y verificar que el sistema puede acomodar el número de fases requeridos. Sin un testeo del proceso de ingeniería de sistemas, la validación y verificación podría ser lanzado como parte de la aprobación final del sistema más que ser una consideración integral durante el desarrollo del proyecto.

Los conectores cruz entre las alas de la "V" también enlazan los tests de integración, verificación y validación para la descomposición y definición. Este enlace es provisto a través de la "trazabilidad". El intento aquí es mostrar que el sistema implementa satisfactoriamente todos los requerimientos del sistema identificados para el proyecto y que estos son los requerimientos correctos, implementados correctamente.

Los niveles muestran a lo largo de cada pierna de la "V" que representa puntos de control. Esto significa que la documentación de la arquitectura y requerimientos del sistema deben ser completados antes que un diseñado detallado pueda ser completado.

Hay también una dimensión vertical que enlaza la línea del "tiempo". Esto ilustra que como el tiempo se mueve adelante cada tarea sucesiva construye sobre una tarea

previa y espera la siguiente tarea. El equipo de desarrollo debe usar el Concepto de Operaciones para construir la lista de requerimientos y mientras se construye esta lista, debe también ser considerando cualquier implicación al diseño e implementación del sistema.

En uso actual, el modelo de la "V" típicamente termina viendo más como una "W". Las variaciones típicas son representadas en los figuras 4.2, 4.3 y 4.4.

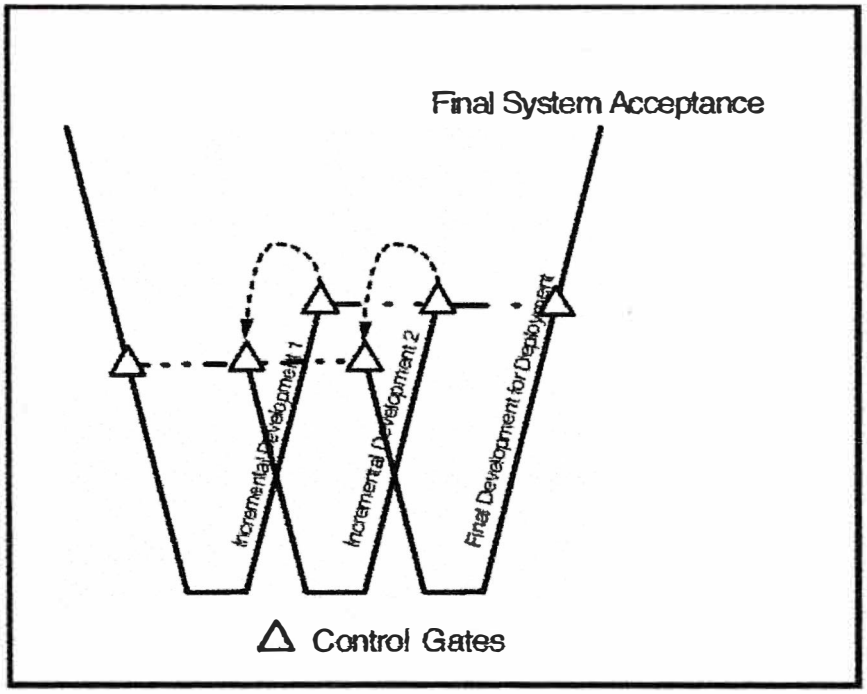

Figura 4.2: Entrega Única del Desarrollo Incremental

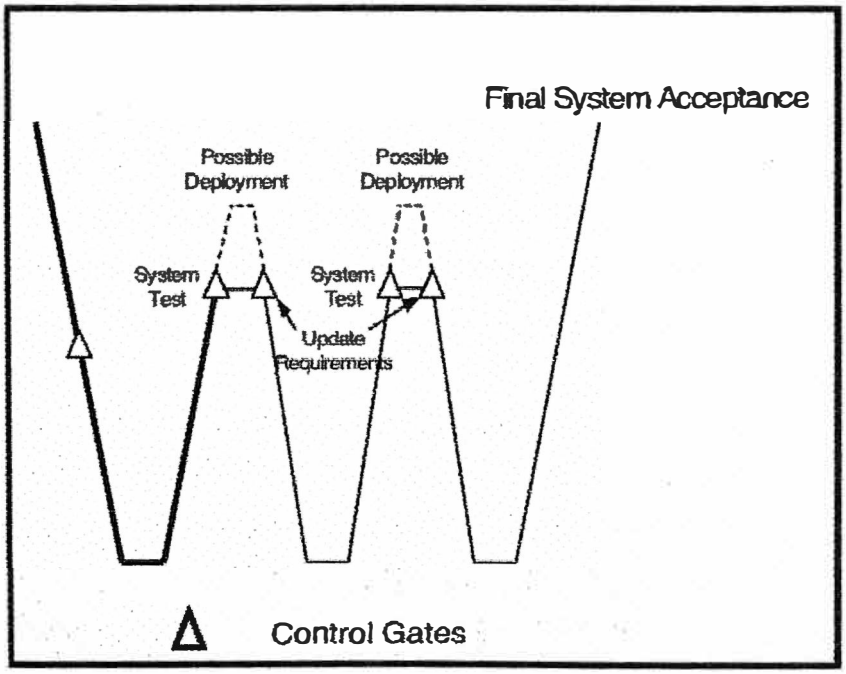

Figura 4.3: Entrega Única o Múltiples del Desarrollo Evolucionario

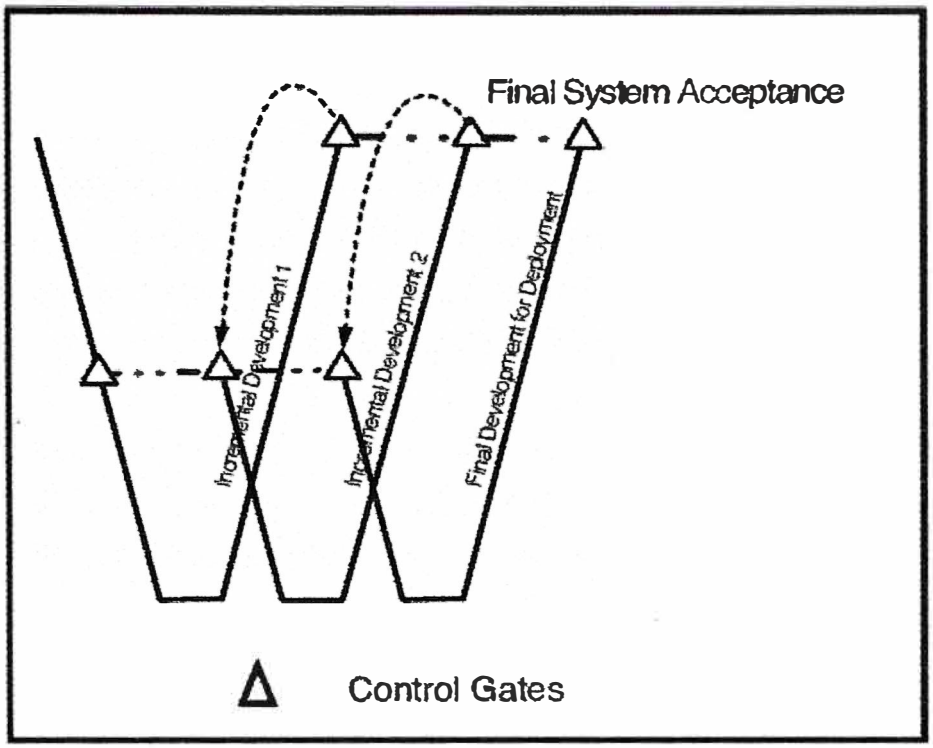

Figura 4.4: Desarrollo múltiples con Desarrollo Incremental

4.2 Gestión de Configuración

La gestión de configuración es una parte del proceso de ingeniería y un elemento crítico en la vida de cualquier sistema. Las personas quienes son primariamente involucradas en el campo de la ingeniería de transporte, esto es un concepto relativamente nuevo. Dado que el Sistema de Transporte Inteligente de hoy, se recomienda que un plan para la gestión de configuración sea implementado al inicio del desarrollo del sistema. Como con muchos proyectos, hay elementos del sistema heredado que debe ser incluido como parte de este plan de gestión de configuración.

La gestión de configuración puede tener un impacto significante en reducir los costos de ciclo de vida del proyecto. El tiempo y costos de errores del sistema encontrados pueden ser reducidos a través de la gestión de configuración. La gestión de configuración puede también ayudar a controlar el proyecto y el resultado del costo y el impacto del horario.

Aquí hay dos definiciones de gestión de configuración:

La gestión de configuración es la práctica de la manipulación de los cambios sistemáticos que un sistema puede mantener su integridad sobre tiempo. Otro nombre para esto es "cambio de control". Incluye técnicas para la evaluación de cambios propuestos, cambios de pista, y mantener copias del sistema como si existiese en varios puntos del tiempo, y

La gestión de configuración permite el desarrollo ordenado de un sistema, subsistema o configuración. Un buen programa de gestión de configuración asegura que el diseño son trazables al requerimiento. Ese cambio es controlado y documentado, esas interfaces son definidas y definidas, y que hay consistencia entre el producto y su documentación de soporte. La gestión de configuración provee documentación que describes qué está supuesto para ser producido, qué está siendo producido, qué ha sido producido y qué modificaciones han sido hechas para qué fuese producido.

Se observa que el control de mención de la definición y los cambios de pista al sistema. La gestión de configuración direcciona ese proceso.

La gestión de configuración es con frecuencia separada en cuatro tareas relacionadas:

4.1.1 Identificación:

Esta tarea está referida al inventario del sistema. Esto incluye un esquema para identificar únicamente cada elemento del sistema. Incluido para cada elemento único sería su relación estructural con cada otro elemento del sistema, descripciones de interfaces, requerimientos funcionales, características físicas, identificación de la versión e identificación de la configuración. Esto no es limitado al software, pero debe también incluir detalles del hardware. Estos elementos son típicamente llamados Items de Configuración. Como muchos sistemas, esto debe comenzar con los sistemas heredados que serán reusados en el sistema que está siendo desarrollado.

Uno de los primeros pasos sería documentar que esta pedido para cada elemento, en detalle. Muchos paquetes de software disponibles comercialmente están disponibles para facilitar la organización y el encaminamiento de los elementos. Una vez que el inventario ha sido completado, los siguientes pasos en este proceso son más fáciles.

4.1.2 Control:

El control es el proceso sistemático de mantenimiento y preservación de la base de línea de un sistema estable – en otras palabras, controla los cambios al sistema. Este proceso es típicamente formalizado a través de la sumisión de la documentación de pedidos para el cambio al cuerpo de revisión.

Los cambios pedidos son con frecuencia llamados Propuestas de Cambio de Ingeniería (ECP). Son divididos en dos clases. *Clase 1* cambia la aprobación formal

pedida con la base de línea de los requerimientos, seguridad, interfaces, capacidades de operación / servicio, interfaces humanas y más. Ellos cambian el sistema y con frecuencia impactan costos y horarios. La *Clase 2* cambia los conflictos menores para corregir tipos y otros cambios de "housekeeping" para corregir la documentación para reflejar la configuración normal. Dentro de cada clase, el pedido es además separado en términos del tipo de pedido, prioridad del pedido y justificación del pedido.

4.1.3 Cuenta de Estado:

Esta es la relación de mantenimiento y la función de reporte de la configuración del proceso de administración. El estado de cuenta involucra las siguientes tareas:

- Colectar, catalogar y mantener todas las documentaciones de la configuración.
- Encaminar y reportar el estado de todos los cambios propuestos.
- Encaminar y reportar el estado de implementación de todos los cambios aprobados.
- Configuración de todos los hardwares del sistema, incluye esos en inventario operacional.

Mantener un buen estado de operación de cuenta es crítico para el análisis e implementación de todos los cambios propuestos futuros.

4.1.4 Audiciones y Revisiones:

Periódicamente la revisión y la audición a un sistema y sus componentes conforme a su documentación de configuración debe ser una parte integral del proceso. La meta es verificar que el sistema satisface sus requerimientos. Esto es esencialmente la función de calidad de control de la administración de la configuración. Hay tres audiciones comunes en administración de configuración.

- **Audición de la Configuración Funcional:** Esta audición está hecho después de todos los hardware del sistemas ha sido testeado. Esto engancha los requerimientos iniciales para el sistema implementado.

- **Audición de la Configuración Física:** Esta audición está hecho siguiendo la Audición de Configuración Funcional para confirmar que los planes y especificaciones enganchados qué ha sido construido.

- **Revisión de la Verificación del Sistema:** Esta revisión evalúa el proceso de ingeniería de sistemas de si mismo para ver si éste esta ejecutándose como se planeó.

4.3 REQUERIMIENTOS:

Los proyectos exitosos se confían en el entendimiento de los requerimientos funcional, de diseño, y testeo antes de cualquier procedimiento, desarrollo o implementación.

4.3.1 Requerimientos Funcionales

El primer aspecto de un proyecto es determinar los requerimientos exactos para el sistema. Esto requerirá el desarrollo de un Concepto de Operaciones, describiendo las operaciones a realizar; después, un conjunto detallado de Requerimientos Funcionales pueden ser desarrollados, contra el cual el producto final será juzgado. Los requerimientos funcionales comienzan con la documentación de cualquier requerimiento operacional existente, añadiendo cualquier nuevo requerimiento. Es importante entender que el concepto de "Trazabilidad" corre a través del enfoque de la ingeniería. La Trazabilidad provee un vínculo entre cada elemento en el modelo de ingeniería – significa que el Testeo de Verificación y Validación puede ser trazado de regreso a través de Implementaciones, Diseño de detalle, Requerimientos Funcionales y Concepto de Operaciones.

a. Como las Normas para los Protocolos de Comunicación en ITS encajan Juntos

Idealmente, habría solamente solo una norma NTCIP que reúna las necesidades de todos – que es colectivamente conveniente, efectiva y contribuye positivamente al desarrollo de las implementaciones ITS interoperable e intercambiable. Sin embargo, la realidad requiere un gran número de opciones para reunir las necesidades únicas del desarrollo del sistema específico. Por ejemplo, algunas agencias tienen gran cantidad de cable de par trenzado que quieren continuar usando. Otras agencias están instalando nuevos sistemas y quieren tomar ventaja del cable de fibra óptica y/o otras tecnologías. Asimismo, algunas agencias tienen un apreciable intercambio de data simple que necesita con otros dispositivos de campo, donde otros centros necesitan intercambiar grandes cantidades de información con otros centros. El NTCIP acomoda estas diversas necesidades para proveer una familia de normas, con cada norma proveyendo características únicas.

La Figura 4.5 representa la estructura de normas NTCIP. El capítulo anterior se discutió como la estructura esta basada por encima de cinco niveles, incluyendo Niveles de Información, Aplicación, Transporte, Subred y Planta. Los tres del medio de los cinco niveles se relacionan con las siete capas del modelo OSI. El nivel de Planta esta incluido como una referencia para mostrar la relación a la infraestructura de campo. La figura muestra todas las normas que residen sobre cada nivel y representa varias opciones que deben ser hechas durante el proceso de desarrollo de la especificación. Las líneas de conexión representan los vínculos de compatibilidad entre varias normas.

- **Nivel de Información:** Las normas de Información definen el significado de la data y mensajes, y generalmente el acuerdo con la información ITS (más que información acerca de la red de comunicaciones).

- **Nivel de Aplicación:** Las normas de Aplicación definen las reglas y procesos para intercambiar la data de información. Las reglas pueden incluir definiciones de gramática propia y sintaxis de una sola declaración, también como la secuencia de declaraciones permitidas. Esto es similar a combinar palabras y frases para formar una oración o un pensamiento completo, y definir las reglas para saludar cada otro y la información de intercambio.

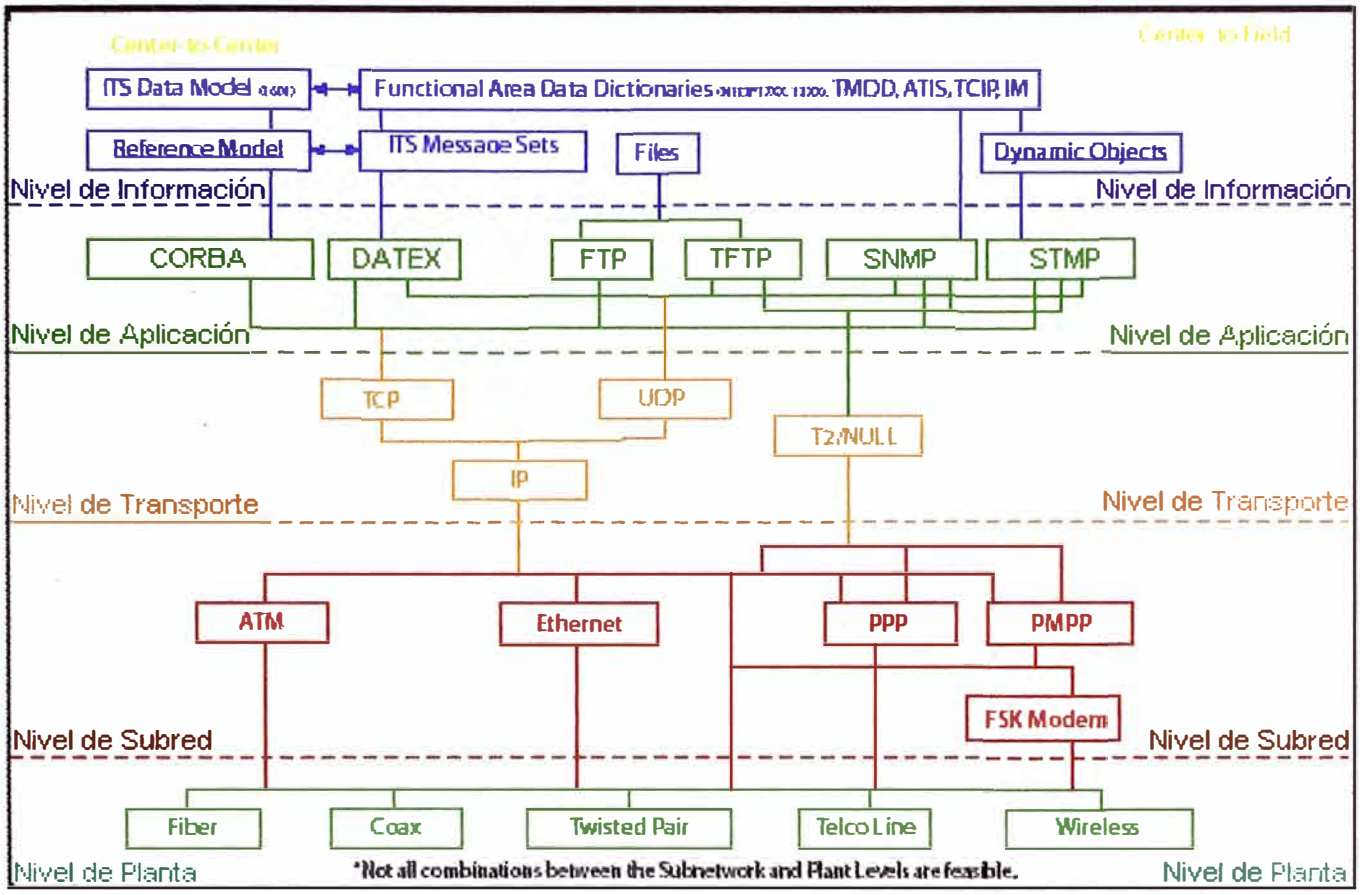

Figura 4.5: Estructura de las Normas NTCIP

- **Nivel de Transporte:** Las normas de Transporte definen las reglas y procesos para el intercambio de la Aplicación de la Data entre el punto "A" y el punto "X" en una red. Esto incluye cualquier enrutamiento necesario, desensamble/re-ensamble de los mensajes y funciones de administración de red. Esto es similar a las reglas y procesos usados por la compañía de teléfonos para conectar dos teléfonos localizadas remotamente.

- **Nivel de Red:** Las normas de Subred definen las reglas y procesos para el intercambio de la data entre dos dispositivos "adyacentes" sobre algún medio de comunicación. Esto es equivalente a las reglas usadas por la compañía de teléfonos para intercambiar la data sobre un enlace celular versus las reglas usadas para intercambiar la data sobre un cable de par trenzado.

- **Nivel de Planta:** El nivel de Planta es mostrado en la estructura del NTCIP como un punto de referencia El Nivel de Planta es una opción de infraestructura y no una

norma que selecciona su opción. Sin embargo, la selección del nivel de planta tendrá un impacto en la selección del protocolo de la subred para el cual debe interactuar.

Cualquier intercambio de la data requiere el uso de norma(s) tomadas de cada uno de los cinco niveles. En teoría, una norma de un nivel debe ser diseñado tal que puede ser combinado con cualquier norma de otro nivel. Sin embargo, en la práctica, las normas con frecuencia requerirán ciertos servicios de otros niveles.

4.3.2 Requerimientos de Diseño

Se deben considerar los diferentes niveles de la estructura NTCIP cuando preparen las especificaciones del procedimiento. Las opciones apropiadas de cada uno de los cinco niveles que componen la estructura del NTCIP necesitarán para ser hecho tan pronto como sea posible durante otro concepto operacional, los análisis de requerimiento, o el proceso del desarrollo de las especificaciones del diseño. O subsecuentemente durante el proceso del procedimiento.

Estos requerimientos consisten en preparar la elección apropiada de las normas para cada nivel dentro de la estructura NTCIP. Para hacer efectivamente estas selecciones, un buen conocimiento de recursos, como la infraestructura y equipos de comunicaciones existentes, podrían estar disponibles de un sistema existente. La Figura 4.6 presenta un resumen de una lista de revisión básica para su uso en la preparación de especificaciones detalladas para sistemas NTCIP. Las especificaciones de procedimiento detallado requerirán primero el conocimiento de la implementación del sistema, tal como el medio de la infraestructura; necesidades de procesamiento y data y la funcionalidad del sistema.

- Considerar las necesidades específicas de comunicaciones por desarrollar los requerimientos funcionales.
- Analizar los recursos disponibles.
- Definir una pila NTCIP entera para los sistemas.
- Reunir las normas apropiadas para cada nivel dentro de la pila NTCIP para encajar los requerimientos funcionales con las funciones y opciones de la norma NTCIP.
- Determinar la Conformidad de los Grupos requeridos.
- Determinar los Elementos de la Data requeridos (objetos).
- Definir los Rangos de Valores reales para la implementación.
- Determinar todos los requerimientos funcionales que no pueden ser concordados.
- Determinar las especificaciones para reunir las necesidades no direccionadas por las normas NTCIP.
- No permite excepciones para propuestas subsecuentes si la existencia de sistemas centrales es para ser usado sin modificación.

Figura 4.6: Resumen de la Lista de Revisión del Procedimiento

Las consideraciones importantes para determinar las necesidades de comunicaciones específicas incluye la comunicación de la data y del tiempo, carga del canal y dispositivos de latencia.

El proyecto y las especificaciones del proceso debe también incluir información relacionada al hardware y/o dispositivos, integración del sistema, testeo y configuración del dispositivo. Estas disposiciones deben también direccionar la posesión, redistribución y/o reuso de los derechos del MIB's, tan bien como los requerimientos para la documentación y obtención del MIB.

4.3.3 Diseño

Después de la identificación y documentación de los requerimientos Funcionales, el Diseño Detallado puede comenzar. Este elemento enfoca sobre los temas de diseño específico encontrados cuando preparan los documentos de procedimiento, o planes y especificaciones.

4.3.4 Alternativas de Implementación

En muchos casos, la industria privada ha desarrollado herramientas para auxiliar a los desarrolladores del sistema en la implementación de estos protocolos. Estar enterado qué productos están disponibles, inherente en un sistema de operador o buscador, y sus costos asociados permitirá a la agencia poner una expectación razonable, y el desarrollador provee un estimado realista de costos de desarrollo. Por ejemplo, algunos desarrolladores pueden usar una implementación TCP/IP más que la creación de si mismo. Las normas por el cual hay productos conocidos incluyen:

- Protocolo de Transferencia de Archivo (FTP).
- Protocolo de Transferencia de Archivo Trivial (TFTP).
- SNMP.
- CORBA.
- XML.
- TCP/IP y UDP/IP.
- Protocolo Punto a punto (PPP).Ethemet.

Mientras el software puede ahorrar una cantidad considerable del tiempo de desarrollo y simplificar el mantenimiento del mismo, esto no puede siempre proveer la implementación más eficiente. Sin embargo, la ejecución del sistema en tiempo real puede frecuentemente ser mejorado por la violación de diferentes reglas de una capa de

diseño real y por el código de optimización de la construcción según especificaciones del embebimiento para un propósito específico. La agencia debe estar enterada de los beneficios y perjuicios de cada enfoque antes de aprobar un enfoque en pleno desarrollo y el costo estimado.

4.3.5 Centro a Campo

El Figura 4.7 construye sobre la discusión anterior por la expansión en las consideraciones que deben ser direccionados durante el planeamiento inicial y escenarios de desarrollo para los documentos de la obtención. La lista de revisión incluye los puntos que el fabricante del dispositivo y/o desarrollador / integrador del sistema debe proveer como parte de su sumisión propuesta. En el caso de una agencia ejercedora la ruta de la especificación detallada, estos puntos deben ser direccionados en los documentos de la obtención. La lista de revisión también apunta a los recursos adicionales que están disponibles en la refinación de las especificaciones detalladas.

Ejemplo 4.1: Ejemplo de una Pila C2F usando SNMP

Este ejemplo muestra un posible camino a través de la estructura NTCIP para la comúnmente referida y publicada Perfil de Clase B. Esto debe ser notado que la terminología preferida para este camino es la "pila", más que el perfil.

- Considerar las necesidades de las comunicaciones específicas por desarrollar los requerimientos funcionales, incluyendo:
  - Data de Comunicaciones y tiempo.
  - Carga de Canal.
  - Latencia del dispositivo.
- Analizar los recursos disponibles:
  - Nuevo sistema con recursos no existentes.
  - Sistema existente con recursos disponibles.
- Determinar los Grupos de Conformancia requeridos:
  - Obligatorio.
  - Opcional.
  - Ver las normas específicas que relacionan la funcionalidad necesitada.
- Determinar los Elementos de la Data requeridos (objetos):
  - Obligatorio.
  - Opcional.
  - Ver las normas específicas que relacionan la funcionalidad necesitada.
- Definir los Rangos de Valores reales para la implementación del sistema:
  - Ver funcionalidades de requerimiento.
  - Ver las normas específicas que relacionan la funcionalidad necesitada.
- Determinar todos los requerimientos funcionales que no pueden ser encajados.
- Desarrollar las especificaciones para reunir las necesidades no direccionadas por las normas NTCIP.
- Definir cómo los items de manufacturador específico, si permitió, serán direccionados.

Figura 4.7: Resumen de la Lista de Revisión del Procedimiento

La Figura 4.8 representa gráficamente un ejemplo de una pila NTCIP C2F y es una variación de que fue originalmente publicada como el Perfil de Clase B. La pila es mostrada como este se relaciona a la estructura NTCIP. La combinación de selecciones apropiadas de cada uno de los Niveles de Información, Aplicación, Transporte, Subred y de Planta crea la pila. La figura muestra las opciones en cada nivel de la estructura NTCIP que son requeridos para crear una variación de la Clase B, como este fue publicado originalmente. Por ejemplo, la selección del protocolo SNMP está hecho en el Nivel de Aplicación de la pila NTCIP.

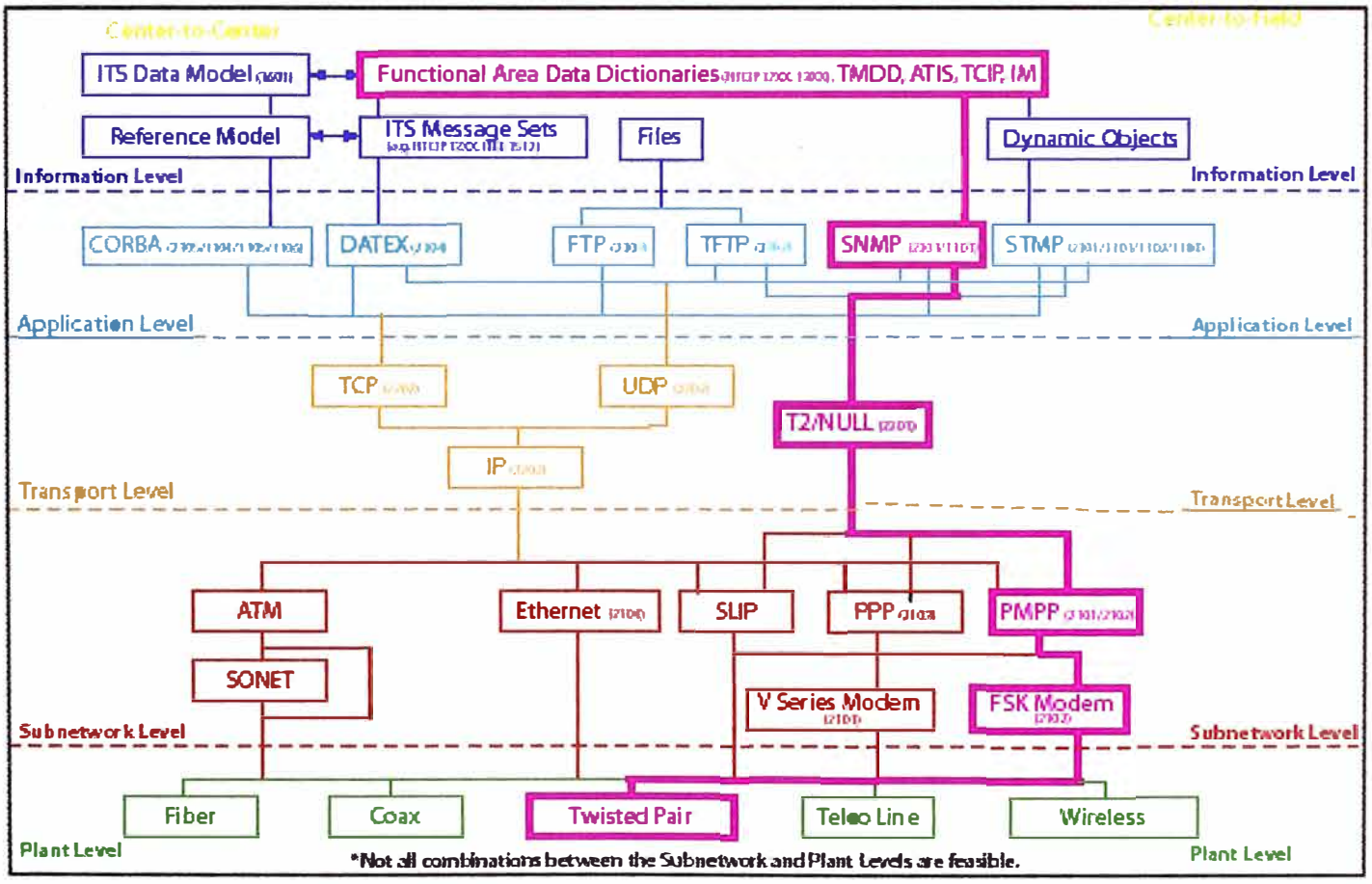

Figura 4.8: Ejemplo de la Pila Center - to - Field

La pila de la clase B que fue originalmente publicada incluye sólo los niveles de Aplicación, Transporte y Subred de la estructura NTCIP. Las opciones que son ofrecidas en el Nivel de Aplicación incluyen SNMP y STMP. La única opción que está definida por el Nivel de Transporte es T2/NULL. La opción del Nivel de Subred incluye Punto – Multipunto, usando otras normas comerciales EIA / TIA – 232 o para los modems FSK de

1200 bps. El Nivel de Planta es asumido a ser agencia que posee el cable de par trenzado.

a. Opciones de la Pila NTCIP

Los Niveles de Información, de Aplicación, de Transporte, de Subred y de Planta de la estructura NTCIP presenta una variedad de opciones que pueden ser seleccionados para formar una pila NTCIP. El figura 4.9 presenta una vista expandida de las opciones disponibles C2F.

- Nivel de Información:
  - Selección de Normas Aplicables.
    - NTCIP 1201 – Definiciones de Objeto Global (siempre usado con un dispositivo de norma específica).
    - Dispositivo de Normas específica(s).
  - Especificar Conformancia de Grupos basados en el estatuto delos PICS en el dispositivo de normas específicas.
    - Obligatorio.
    - Opcional.
    - Basado sobre la funcionalidad del dispositivo.
  - Especificar los Elementos de la Data.
    - Obligatorio.
    - Opcional.
    - Determinar los Rangos de Valores.
- Nivel de Aplicación:
  - SNMP (Simple Network Management Protocol).
    - Norma de Internet.
    - El soporte es obligatorio en la Conformidad Nivel 1 y 2.
  - STMP (Simple Transportation Management Protocol).
    - Protocolo más eficiente.
    - Definir Objetos Dinámicos (múltiple pedido de elementos de la data en un solo mensaje).
    - El soporte es obligatorio en la Conformidad Nivel 2.
- Nivel de Transporte:
  - TCP.
    - IP.
  - UDP.
    - IP.
  - T2/Null
- Nivel de Subred:
  - ATM.
    - SONET.
  - Ethernet.
  - PPP
    - FSK Modem
  - PNP
    - EIA / TIA-232-E
    - FSK Modem
- Nivel de Planta:
  - Fibra Óptica.
  - Cable coaxial.
  - Par trenzado.
  - Línea Telco

Figura 4.9: Opciones Centro a Campo

El Nivel de Información de la estructura NTCIP enfoca en los requerimientos de información del dispositivo o sistema para lograr la funcionalidad deseada. Una discusión minuciosa de las opciones del Nivel de Información disponible serán presentados después en esta sección.

En el caso del C2F, la selección de un protocolo de Nivel de Aplicación es una importante consideración. Hay muchas opciones para los protocolos C2F:

- Protocolo de Administración de Red Simple (SNMP) que es comúnmente usada en Internet y aplicaciones de la industria de la computación.
- El más eficiente Protocolo de Administración de Transporte Simple (STMP) que permite al usuario acceder a los elementos de la data múltiple usando una sola petición.
- El Protocolo de Transferencia de Archivo Trivial (TFTP) y el Protocolo de Transferencia de Archivo (FTP) son comúnmente protocolos usados en la industria del Internet.

Las opciones del Nivel de Transporte son esencialmente comprimidas dentro de una opción entre el uso de protocolos ruteables y no ruteables. El Protocolo de Transporte del Transporte (T2, formalmente conocido como Protocolo NULL) en el Nivel de Transporte es usado con protocolos no ruteables. En el caso de protocolos ruteables, una opción adicional es requerido entre la conexión orientada y sin conexión. El Protocolo de Control de Transmisión (TCP) es un protocolo de conexión orientada que es usado en conjunto con el Protocolo Internet (IP). El Protocolo del Datagrama del usuario (UDP) es un protocolo sin conexión que es también usado en conjunto con el Protocolo Internet (IP). El UDP es comúnmente usado en conjunto con el SNMP, STMP y los Niveles de Aplicación TFTP, mientras el TCP es típicamente usado en conjunto con el Nivel de Aplicación FTP.

El Nivel de Red presenta una serie de redes, protocolos Punto a Punto y Punto a Multipunto. El ATM, SONET y Ethernet son todos los ejemplos de las opciones de protocolo de red de banda ancha. El PPP y PNP son también opciones disponibles en el Nivel de Subred.

El Nivel de Planta de la estructura NTCIP no denota las normas de comunicación NTCIP, pero incluye fibra óptica, cable coaxial, cable par trenzado y líneas telco.

En los casos de selección de protocolo, sería aconsejable consultar a los fabricantes del equipo y sistemas para asistencia en la selección del más apropiado protocolo(s) soportado que reúna todos los requerimientos del sistema. El STMP debe ser

considerado esencial para los sistemas de señal de tráfico operando sobre el medio tradicional, pero otros dispositivos no pueden necesitarlo.

Las necesidades funcionales de dispositivos particulares, equipos y sistemas son importantes cuando la consideración de la selección de las declaraciones de conformidad apropiada. Mientras las normas de comunicación NTCIP no prescriben específicamente los requerimientos funcionales, tal puede ser deducida por la construcción del elemento de la data. Los requerimientos de las comunicaciones NTCIP deben ser consistentes con las especificaciones funcionales para el dispositivo. Como en el caso de un sistema de señal de tráfico C2F, la selección de los conjuntos de los elementos de la data de la norma apropiada que cede la funcionalidad requerida para una implementación específica podría incluir los elementos de la data de dos normas NTCIP, Definiciones de Objeto Global y Objetos de Control de Señal Actuado. Últimamente, los valores de rango específico asociados con estos elementos de la data también necesitarían ser consistente con los requerimientos funcionales del dispositivo.

Revisando las normas que podrían ser aplicables a una implementación específica, la atención debe ser dibujada en la sección de Declaración de la Conformidad del documento. Los elementos de la data son ordenados en grupos basados por encima de la data asociada con varios niveles de funcionalidad. Algunos grupos son obligatorios, mientras muchas son opcionales. Los elementos de la data específica dentro de cada grupo de conformidad, a pesar del grupo de conformidad que está siendo opcional u obligatorio, puede también ser obligatorio u opcional. La implementación específica y los requerimientos de la funcionalidad dictarán la selección de grupos de conformidad apropiados y los elementos de la data. Una vez que los elementos de la data son identificados, una determinación de valores de rango apropiado puede ser asignado a cada uno para representar el nivel deseado de la funcionalidad.

b. Recursos Disponibles para Información Adicional

Últimamente, especificar el NTCIP no hace la vida más fácil para los planificadores de sistemas. Las especificaciones detalladas deben ser cuidadosamente pensadas y mayor conocimiento minucioso de la operación y la funcionalidad es necesitada temprano (en el escenario de la preparación de la especificación) de modo de adecuar los equipos y sistemas específicos que reúna las necesidades requeridas. Por estas razones, una agencia podría querer considerar un método de obtención del perfil de la funcionalidad deseada como parte del paquete de obtención y solicitar una propuesta del fabricante, proveedor, desarrollador o integrador direccionando los detalles de la implementación específica.

- **Ejemplos de Desarrollo de la Especificación NTCIP**

Esta sección es dedicado a ejemplos de cómo el planificador de sistemas daría un paso a través de un proceso para desarrollar las especificaciones de la obtención detallada para sistemas NTCIP. Los ejemplos están provistos para determinar:

- Una pila NTCIP apropiada basada por encima de la estructura NTCIP.
- Grupos de Conformidad opcional y obligatorio apropiados y los elementos de la data necesitados para lograr una funcionalidad deseada.
- Los valores del rango que podrían ser necesitados para una implementación específica.

- ***La Pila NTCIP para Controlador de Señal de Tráfico Center – to – Field***

Ejemplo 4.2 – Una pila NTCIP apropiada es necesitada para una aplicación del controlador de tráfico típico. En este ejemplo, el controlador va a ser localizado en el gabinete de campo y es un dispositivo sobre un canal de comunicación multi-drop. El sistema de gestión de transporte central constantemente se comunica directamente al controlador de tráfico sobre una agencia que posee cable par trenzado.. el sistema de gestión central es para comunicarse sobre un base una vez por segundo con el controlador de tráfico.

El planificador de sistema puede comenzar por determinar las selecciones apropiadas por cada nivel usando la estructura NTCIP, como se muestra en *figura 4.10*. es dado que una agencia que posee planta de comunicaciones de cable de par trenzado proveerá la infraestructura física para comunicaciones C2F. La selección en el **Nivel de Planta** debe reflejar la selección del cable par trenzado.

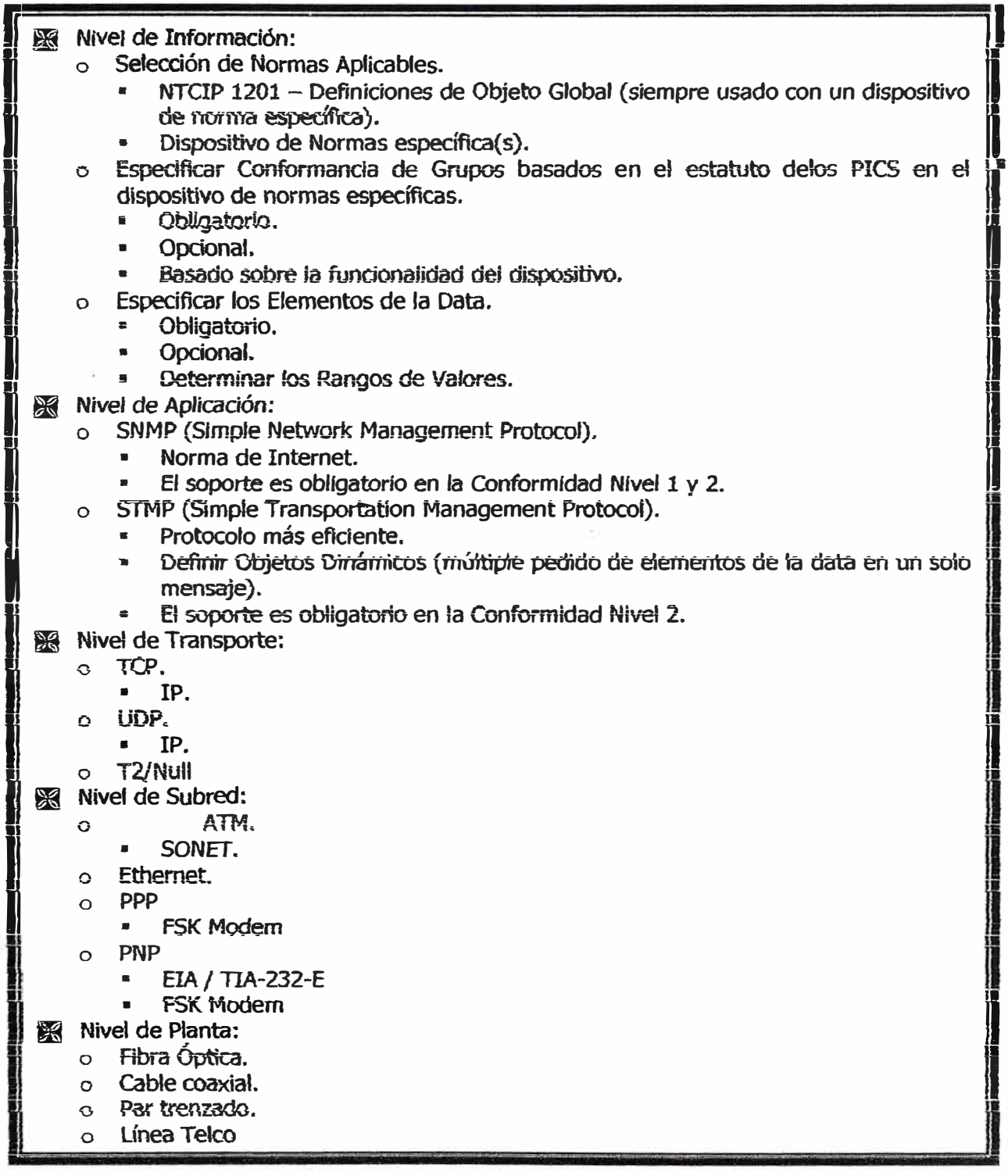

Figura 4.10: Ejemplo de la estructura NTCIP para un Controlador de Tráfico Centro a Campo

Las selecciones hechas en los **niveles** de **Transporte** y de **Red** pueden ahora ser hechas basadas por encima del tipo de comunicaciones deseados entre el sistema de gestión de transporte central y el controlador de tráfico de campo. En este ejemplo, un enlace de comunicaciones Punto a Multipunto dedicado sin enrutamiento a través de los

dispositivos de los más altos niveles es la alternativa deseada. Tal como, las selecciones de NTCIP 2102 – PNP y MODEM FSK pueden ser hechos en el Nivel de Transporte.

Para las selecciones apropiadas en el Nivel de Aplicación, el planificador de sistemas esta referido a las publicaciones NTCIP describiendo la Estructura de Gestión de Transporte Simple (STMF). La Estructura de Gestión de Transporte Simple describe dos niveles de conformidad:

- **Nivel de Conformidad 1**
  * Protocolo de Administración de Red Simple (SNMP)

- **Nivel de Conformidad 2**
  * Protocolo de Administración de Red Simple (SNMP)
  * Protocolo de Administración de Transporte Simple (STMP)

El SNMP es comúnmente usado en la norma de Internet que está muy bien soportada. El STMP es un protocolo más eficiente para el uso por la industria del transporte que permite el uso de objetos dinámicos. La selección preferida en el Nivel de Aplicación para sistemas de señal de tráfico es NTCIP 2301 – el STMP porque de la tasa de la data baja y las tasa de frecuencia altas (aquí, uno por segundo) que son comunes a la mayoría de los sistemas de señal de tráfico.

La selección de las normas del Nivel de Información, grupos de conformidad y elementos de la data está basada por encima de la funcionalidad deseada del sistema que esta siendo implementado. En el caso de este ejemplo donde un sistema de señal de tráfico está siendo implementado, el planificador del sistema necesitará mirar específicamente en los requerimientos de la norma primaria NTCIP 1202 – *Norma de las Definiciones de Objetos para las Unidades de Controlador de Tráfico Actuado* para el criterio de conformidad y elementos de la data. Adicionalmente, la norma de soporte NTCIP 1201 – *Definiciones de Objetos Global* define una serie de elementos de la data que cruzan y cortan para la configuración, administración de la base de datos, administración del tiempo, horarios de los eventos base en el tiempo, reportes, STMP y PNP. Como resultado, las normas para el Control de Señal Actuado y las Definiciones de Objeto Global serán necesitadas para lograr el nivel deseado de funcionalidad.

- **Grupo de Conformidad y Selección del Elemento de la Data para Controladores de Tráfico**

  Ejemplo 4.3 – Una selección apropiada de grupos de conformidad y elementos de la data son necesitados para una aplicación del controlador de tráfico típico. En este ejemplo, el controlador estará basado sobre las normas NEMA TS-2 – Tipo 2 de Controlador de Tráfico Actuado. El controlador NEMA tipo 2 es compatible a los Gabinetes de los Controladores de Tráfico NEMA TS-1 con los conectores A, B y C.

La NEMA TS 2 – 1998 Norma para las Asambleas de Controladores de Tráfico describe una especificación funcional para asambleas de controladores de tráfico, incluyendo la unidad del controlador, la unidad de gestión de malfuncionamiento, terminales y facilidades, dispositivos auxiliares, unidad de interface gabinete y bus. La NEMA TS 2 – 1998 describe a los controladores de tráfico en términos de ser otro Actuado o Predeterminado. También, hay dos opciones de interfaces citados como Tipo 1 y Tipo 2. la Interface del Tipo 1 es una nueva norma de ejecución basada usando la comunicación serial y la interface Tipo 2 utiliza el MS A, B y C para proveer la compatibilidad a los estilos de los gabinetes de estilo TS 1.

- **Rango de Valores de los Elementos de la Data para un Controlador de Señal de Tráfico Actuado.**

  Ejemplo 4.4 – Una selección apropiado del rango de valores son necesitados para una aplicación de controlador de señal de tráfico típico. En este ejemplo, el controlador será un controlador de 8 fases basados por encima de las normas del Controlador de Tráfico Actuado NEMA TS-2 TIPO 2.

Como en el ejemplo 4.3, la referencia esta hecha a la norma NEMA TS 2 – 1998, este provee una lista del rango de valores de los elementos de la data NTCIP para ser soportados por el controlador de tráfico conforme.

La figura 4.11 muestra un elemento de la data típico de la norma NTCIP 1202 – Definiciones de Objetos para Unidades de Controladores de Tráfico Actuado. El elemento de la data mostrado es el máximo número de fases de los Parámetros de Fases. El máximo elemento de la data de las Fases tiene un estado de obligatoriedad. El rango de valores de este elemento de la data esta denotado como los valores íntegros de 0 a 255. Esto significa que el dispositivo puede soportar cualquier valor dentro de ese rango. Adicionalmente, el elemento de la data indica que un elemento de la data de sólo lectura,

donde escribir un nuevo valor esta prohibido. También, incluido en el elemento de la data está una descripción de que este elemento de la data significa.

NTCIP 1202 – Parámetros de Fase de Conformidad de Grupo – Fase Máxima

```
MaxPhases OBJECT-TYPe
SYNTAX INTEGER (0...255)
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The Maximun Number of Phases this Actuated
Controller Unit supports. This object indicates
tha maximun rows which shall appear in the
phaseTable object."
::={phase1}
```

Figura 4.11: Muestra de los Elementos de la Data del Controlador de Tráfico Actuado

El ejemplo del figura 4.11 también provee una oportunidad para mencionar para mencionar la discusión concurrente de desarrollar los casos de evaluación para las normas NTCIP, y como la conformidad de la implementación en esta púnica dimensión sería determinada. Por ejemplo, en este caso el "caso del test" necesitaría direccionar y determinar exhaustivamente si el elemento de la data *maxPhase*: (1) puede ser puesto a todos los valores de 0 hasta 255 sin error, (2) retorna un valor puesto específico correctamente en cada tiempo, y (3) retorna un error si el set es un valor menos que "0" o más grande que "255". Si un proyecto desarrollado especificó un valor de "32" como el limite deseado, luego esas mismos casos de test informativos pueden ser reusados para la aceptancia del testeo, excepto que ellos estarían limitados a la examinación de valores de 0 a 32, y revisar para los errores en valores menos que "0" y más grande que "32".

La figura 4.12 muestra todos los rangos de valores mínimos que están definidos como parte de la norma NEMA TS 2 – 1998. El rango de valores mostrados están basados por encima de los requerimientos de las funcionalidades mínimas de la norma NEMA. En el caso de los valores de Fase Mínimas, podemos ver que el valor del rango mínimo para ser soportado es 8. la norma NEMA requiere un mínimo de 8 fases para reunir los requerimientos de la norma NEMA TS 2 – 1998. Al menos los requerimientos para más fases son identificadas, el número mínimo de fases igualaría el máximo número de fases y el valor para ser comunicado usando NTCIP para el Máximo Número de Fases sería de 8. Similarmente, otros rango de valores pueden ser relacionados al nivel de la funcionalidad que es también requerido por la especificación del fabricante.

Elemento de la Data	Requerimientos del Proyecto Mínimo
TS 3.4 – 1996 Definiciones de Objetos Globales	
ModuleType	Valor 3
dBCreateTransaction	Todos los valores
dBErrorType	Todos los valores
globalDaylightSaving	Valores 2 y 3
maxTimebaseScheduleEntries	16
maxDayPlans	15
maxDayEvent	10
maxEventLogConfigs	50
mventConfigMode	valores de 2 a 5
mventConfigAction	valores de 2 y 3
maxEventLogSize	255
maxeventClasses	7
maxGroupAddress	2
TS 3.5 – 1996 Unidades de Controladores de Señal de Tráfico Actuado	
maxPhases	8
phaseStartUp	valores de 2 a 6
phaseOptions	todos los valores
maxPhaseGrousp	1
maxVehicleDetector	64
vehicledetectorOption	todos los valores
maxPedestrianDetector	8
unitAutoPedestrainClear	Todos los valores
unitControlStatus	Todos los valores
unitFlashStatus	Todos los valores
unitControl	Todos los valores
maxAlarmGroups	1
maxSpecialFunctionsOutputs	8
coordCorrectionMode	Valores de 2 a 4
coordMaximunMode	Valores de 2 a 4
coordForceMode	Valores de 2 y 3
maxPatterns	48
patternTableType	menos 2,3 o 4
maxSplits	16
splitMode	valores de 2 a 7
localFreeStatus	valores de 2 a 11
maxTimebaseAscActions	48
MaxPreempts	6
PremptControl	Todos los valores
preemptState	Valores de 2 a 9
MaxRings	2
maxSequences	16
MaxChannels	16
ChannelControlType	valores de 2 a 4
ChanelFlash	valores: 0, 2, 4, 6, 8, 10, 12 y 14
ChannelDim	Valores de 0 a 15
MaxChannelstatusGroups	2
MaxOverlaps	4
OverlapType	Valores de 2 a 3

maxOverlapStatusgroups	1
1MaxPort1Addresses	18
Port1Status	Valores de 2 y 3.

Figura 4.12: Rango de Valores del Elemento de la Data para Controlador de Tráfico Actuado

4.3.4 Centro a Centro

La industria ITS está normalmente desarrollando tres diferentes soluciones del Nivel de Aplicación para las comunicaciones inter-sistemas. Dos de estas soluciones han sido definidas por el NTCIP: **DAT**a **EX**change en ASN.1 (**DATEX-ASN**; comúnmente referida simplemente **DATEX**) y la Arquitectura del Corredor de Pedido del Objeto Común (**CORBA**). Otro protocolo potencial C2C, el e**X**tensible **M**arkup **L**anguage (**XML**), no es una solución completa, más si sólo es un formato de estructura de la data y esto no define las reglas para intercambiar las estructuras de la data.

Sin embargo, el trabajo en curso dentro de la comunidad de Internet probablemente producirá una manera normada para intercambiar esta data en un futuro cercano. Mientras tanto, los proyectos han estado desarrollando una variedad de enfoques simples para intercambiar esta data como una medida de recurso provisional.

Todos los tres enfoques proveen la misma funcionalidad básica, pero ellos difieren en el método de la implementación y cada uno tiene algunas características únicas (referencia a "Protocolos Centro a Centro"). Un sistema particular puede soportar uno, dos, o los tres protocolos. Las compuertas o traductores pueden ser desarrollados para pasar los mensajes entre ellos cuando sea necesario. El Protocolo Internet (IP) y el TCP y UDP son usados en el nivel de Transporte para todas las tres soluciones.

A pesar del protocolo del nivel de aplicación, las comunicaciones C2C requieren la participación de los sistemas para intercambiar los mensajes del nivel de información. El contenido de estos mensajes es derivado del siguiente proceso de ingeniería de sistemas para identificar los requerimientos del sistema para el intercambio de la data. Muchos de los esfuerzos para definir estos intercambios de la data pueden ser ejecutados independientemente de una selección de un protocolo. Esto resulta en una definición genérica de los mensajes usados por todos los protocolos. Esta definición asegura que implementaciones diferentes comparten un proceso lógico común del intercambio de la data. Aún si las diferentes implementaciones usan diferentes protocolos, esto debe ser posible para producir protocolos traductores para permitir las dos implementaciones para interoperar.

Hay aun una variedad de detalles de protocolos específicos que deben ser normados si la interoperabilidad es para ser logrado cuando la implementación de estos

intercambios de la data sobre cualquier protocolo específico. En adición a la definición genérica, debe haber una definición del protocolo específico por cada protocolo reconocido.

Los conjuntos de mensaje C2C que han sido desarrollados para citar son esencialmente definiciones genéricas de los mensajes. Estos incluyen:

- Mensajes Externos del Centro de la Gestión Tráfico.
- Perfiles de Interface de Comunicaciones de Tránsito.
- Mensajes de Gestión de Incidentes.
- Mensajes de Información al Viajero.

No hay normas existentes que definan los detalles de cómo implementar un mensaje dado sobre un protocolo dado. Todos los desarrollos existentes de estas normas han hecho interpretaciones de cómo implementar mejor sobre un protocolo dado, y a través de estos desarrollos la industria del transporte ha ganado experiencia valiosas dentro de cómo podemos mejorar nuestras normas genéricas existentes, tan bien como enfocar mejor el tópico de las normas del protocolo específico. La comunidad de las normas está ahora apalancándose esta experiencia para producir la actualización de conjuntos de mensajes genéricos y desarrolla las primeras versiones del conjunto de mensaje de protocolo específico.

La elección del protocolo y conjuntos de mensajes / modelo de objetos depende de la aplicación y del ambiente. Los siguientes factores son relevantes:

Nota: *Las comunicaciones C2C toman lugar entre los sistemas de computadoras, y esas computadoras o sistemas pueden estar dentro del mismo "centro" o en centros separados.*

Los protocolos C2C NTCIP y relacionados con las definiciones genéricas y mensajes de protocolos específicos son necesarios, pero no suficiente para dos centros para intercambiar la data útilmente. El software de aplicación es necesitado para acumular, procesar, mostrar, interpretar, actuar generar la entrada o salida de la data. Por ejemplo, el Protocolo de Transferencia de Correo Simple es una norma para la transferencia del e-mail entre las computadoras, pero una computadora necesita más que el protocolo, esto también necesita un programa de e-mail que habilite a un usuario a componer y enviar un mail, recuperar y leer un mail, y archivar los mensajes enviados y recibidos.

Las comunicaciones C2C entre los sistemas de computadoras trabajarán solamente si las computadores tienen el software de aplicación apropiado. Este software no tiene que ser normado, solo como el programa de e-mail del Outlook de Microsoft trabaja bastante diferente de l programa Comunicador del Netscape, pero el e-mail puede ser enviado entre los dos porque ellos usan el Protocolo de Transferencia de Correo Simple.

Algunas de las funciones que un centro puede necesitar en el paquete del software de gestión de comunicaciones C2C incluyen lo siguiente:

- El interface de usuario, por ejemplo, la forma de subscripción, el display de la data, reportes de estado.
- Interpretación y disposición apropiada de mensajes entrantes.
- Las bases de datos para el almacenamiento de las subscripciones y otros datos administrativos.
- Las interfaces con las bases de datos de transporte y programas existentes.
- El monitoreo y gestión de la ejecución de la red.
- Registro de eventos y reportes.

Ni una de estas funciones son especificadas o provistas por los protocolos o conjuntos de mensajes, desde que ellos no tienen que ser normados. Algunos al menos necesitarán ser provistos para un sistema que maneje y prepare el uso de las comunicaciones C2C. Un sistema puede tener un elaborado y sofisticado paquete de comunicaciones C2C, o uno básico. El formador proveerá más funciones y será más fácil de usar, pero costará más.

CAPITULO V

EJEMPLOS DE IMPLEMENTACIONES NTCIP

Muchas implementaciones NTCIP son presentadas en esta sección como ejemplos de cómo varios niveles de Información, Aplicación, Transporte, Subred y Planta pueden ser combinados.

Los siguientes ejemplos se referirán ocasionalmente a la terminología heredada tal como los Perfiles de Clases.

5.1 Centro a Campo:

Dos ejemplos son provistos para las comunicaciones C2F.

5.1.1 Ejemplo de Implementación Centro a Campo sin Ruteamiento:

Este ejemplo muestra una posible implementación de comunicaciones C2F donde el ruteamiento a través de un dispositivo intermediario no es necesitado.

La figura 5.1 representa un ejemplo común de una implementación donde el ruteamiento a través de un dispositivo intermediario no es necesitado. En este ejemplo, el nivel de Transporte es T2/NULL porque no hay necesidad para un protocolo de ruteamiento.

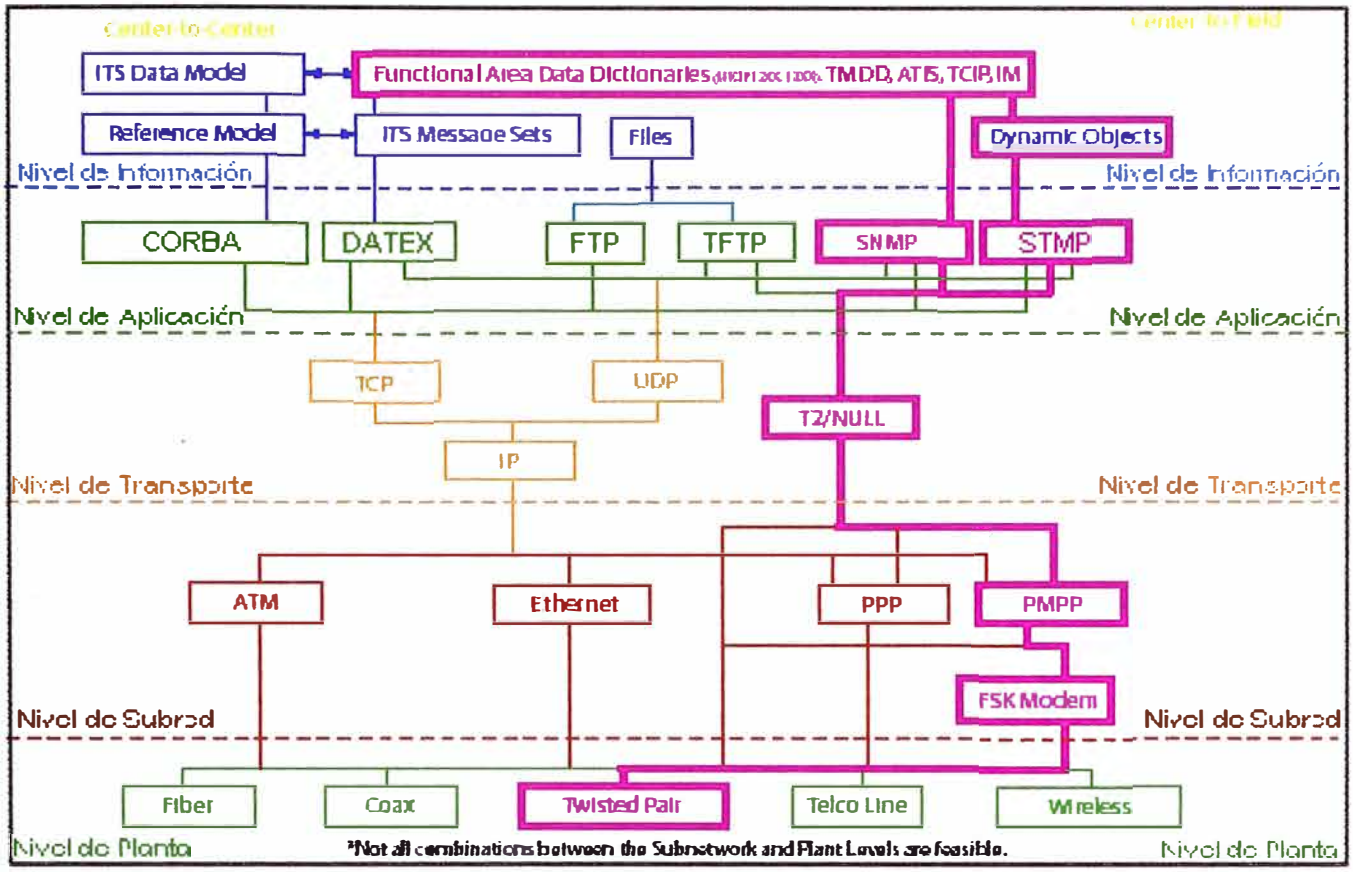

Figura 5.1: Ejemplo de Implementación Centro a Campo sin Ruteamiento

Este ejemplo ilustrado en la figura 5.1 destaca una implementación de la infraestructura NTCIP. La figura muestra la implementación del SNMP y STMP en el nivel de Aplicación y el T2/NULL en el nivel de Transporte. Juntos, estas normas provee servicios para un sistema NTCIP, tal como un sistema de semáforos, esto no involucra ruteamiento a través de dispositivos intermediarios. El ejemplo muestra la selección de ambos; SNMP y STMP en el nivel de Aplicación dentro de la pila NTCIP desde que será una implementación común en muchos sistemas, tal como los sistemas de semaforización, que usan objetos dinámicos.

La implementación subset de la estructura NTCIP mostrado en este ejemplo debe ser notado que la tendencia está trasladándose de varias pilas denotas con caracteres alfanuméricos y esta moviéndose hacia la designación de las normas especificas en cada nivel dentro de la estructura NTCIP.

La norma del nivel de Subred seleccionado en este ejemplo e Punto – Multipunto, modems FSK. El nivel de Planta en este ejemplo de implementación NTCIP es mostrado para ser agencia apropiada del cable de par trenzado, pero cualquier medio apropiado puede ser usado.

5.1.2 Ejemplo de Implementación Centro a Campo con Ruteamiento.

Este ejemplo muestra una posible implementación de comunicaciones C2F donde el ruteamiento a través de un dispositivo intermediario es necesitado. El ruteamiento puede ser tomado también de la forma de sin conexión o los servicios de entrega de transporte de conexión orientada dependiendo de la selección en el nivel de Transporte. Para servicios de entrega de transporte de conexión orientada, la selección del UDP/IP debe ser hecho en el nivel de Transporte. Para servicios de entrega de transporte sin conexión, el TCP/IP debe ser seleccionado como el nivel de Transporte apropiado. En otras palabras, el TCP establece una conexión directa entre dos dispositivos a través de un *handshake arrangement (apretón/estrechamiento de preparativos)* y luego pasa a transmitir la data con la seguridad de que todos los mensajes serán recibidos – de lo contrario los mensajes serán retransmitidos. El UDP, de otra manera, usa más de un enfoque de la difusión sin la seguridad de que el mensaje fuese recibido.

El ejemplo de la implementación ilustrada en la figura 5.2 destaca una implementación de la estructura NTCIP. La figura muestra las normas implementadas en cada nivel del la estructura NTCIP. El ejemplo muestra la implementación de STMP y SNMP en el nivel de Aplicación y el TCP, UDP/IP en el Nivel de Transporte. Juntos, estas normas proveen servicios para un sistema NTCIP.

La norma del nivel de Subred seleccionado en este ejemplo es Punto a Punto. El nivel de Planta en esta implementación es mostrado para ser una línea alquilada TELCO.

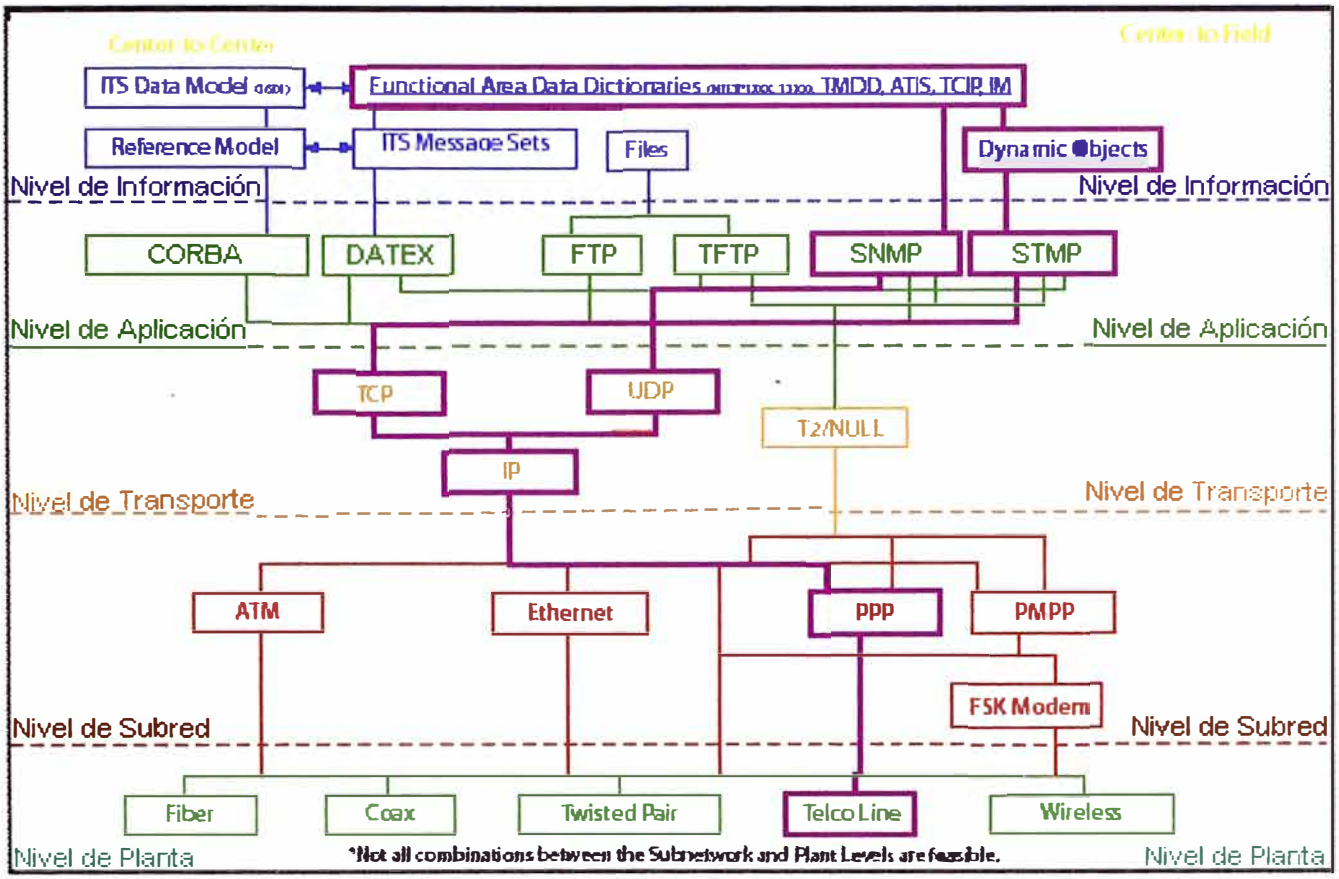

Figura 5.2: Ejemplo de Implementación Centro a Campo con Ruteamiento

5.1.3 Ejemplo de Implementación Centro a Campo con enlaces Ruteables y No-Ruteables:

Este ejemplo muestra una implementación de comunicaciones C2F donde los enlaces ruteables y no-ruteables son usados, tal como en el caso de un sistema de semaforización de lazo cerrado.

La figura 5.3 representa un ejemplo común de una implementación center-to-field donde los enlaces ruteables y no-ruteables son necesitados. Este es el caso clásico de un sistema de semaforización de lazo cerrado, donde la central de tráfico sintoniza el controlador maestro y éste luego coordina con los controladores esclavos usando el cable trenzado. El ruteamiento puede ser tomado también de la forma de servicios de entrega de transporte sin conexión y conexión orientada dependiendo de la selección en el nivel de Transporte. Para los servicios de entrega de transporte sin conexión, la selección del UDP/IP debe ser hecha en el nivel de Transporte. Para servicios de entrega de transporte de conexión orientada, el TCP/IP debe ser seleccionado como el nivel de Transporte. En otras palabras, el TCP establece una conexión directa entre los dos dispositivos a través

de handshake arrangement y luego se pasa a transmitir la data con la seguridad de que todos los mensajes serán recibidos – de lo contrario los mensajes son retransmitidos. El UDP, de otra manera, usa más de un enfoque de difusión sin la seguridad de que el mensaje fuese recibido.

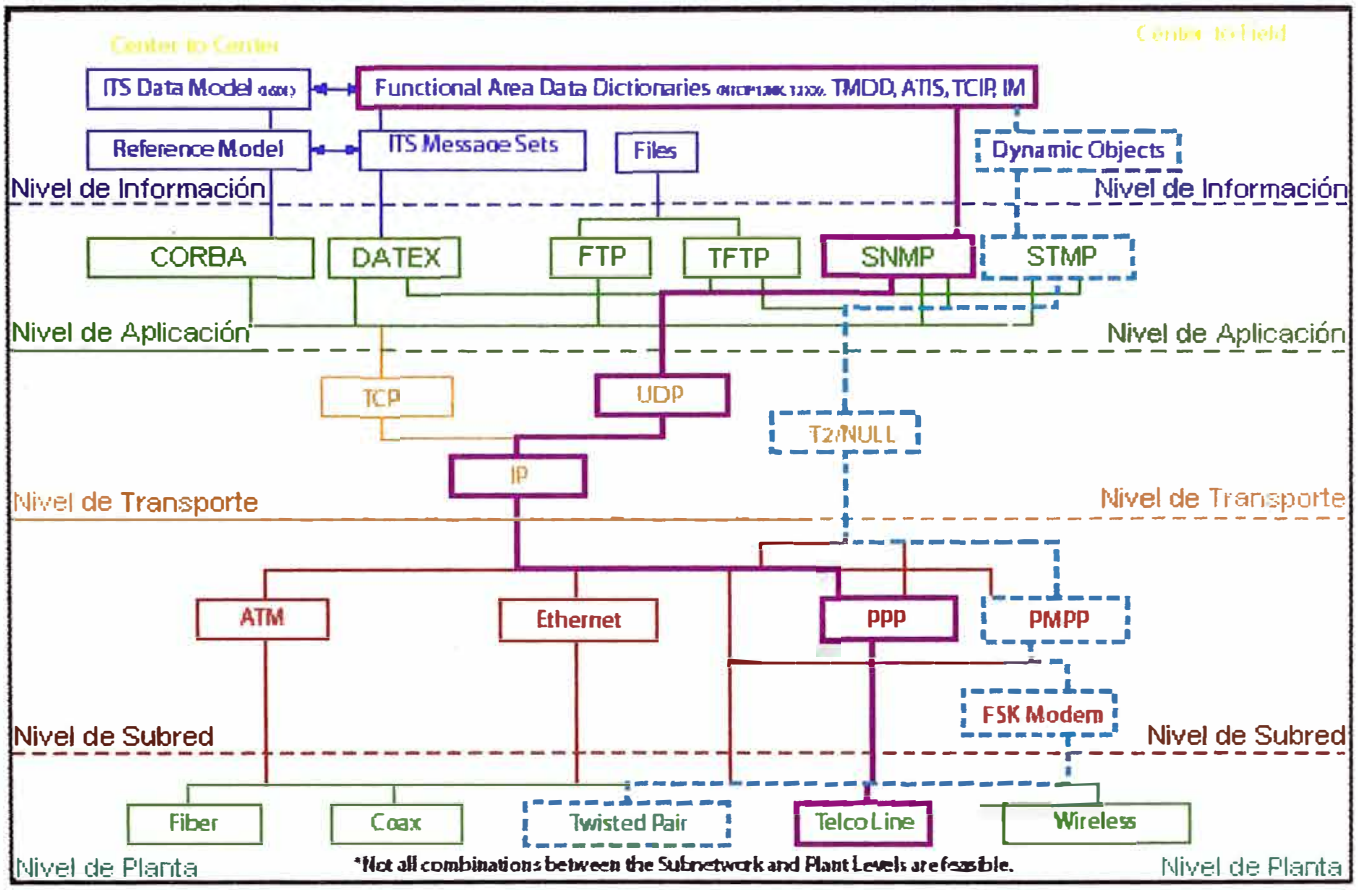

Figura 5.3: Ejemplo de Implementación de Centro a Campo con Enlaces Ruteables y no Ruteables

La mayoría de sistemas de semaforización de lazo cerrado usan UDP/IP para la sintonización de la central de tráfico al controlador Maestro. Una vez que la conexión del dial-up está hecha, el controlador maestro luego se comunicará con los controladores de tráfico esclavos usando el protocolo Punto-Multipunto y el MODEM FSK.

El ejemplo de la implementación ilustrada en la figura 5.3 destaca una implementación para un sistema de semaforización de lazo cerrado típico. Las líneas en negrita denota la porción de la sintonización ruteable de la ruta de comunicación. Las líneas punteadas denotan la conexión de comunicación no ruteable. La figura muestra las normas implementadas en cada nivel de la estructura NTCIP.

El ejemplo muestra la implementación de STMP y SNMP en el nivel de Aplicación. El SNMP es usado para la parte de dial up, mientras que el STMP es usado cuando los

objetos dinámicos son necesitados para que los controladores esclavos subordinen al controlador maestro. El TCP/IP o UDP/IP es seleccionado para usar en el nivel de Transporte para la conexión del dial up entre la central de tráfico y el controlador maestro. Juntos, estas normas proveen servicios para un sistema NTCIP, tal como un sistema de semaforización, que involucra un ruteamiento intermedio. El T2/NULL es usado como el Perfil de Transporte para la parte de comunicaciones no ruteables de la conexión entre el controlador maestro y los controladores esclavos.

Las normas de Subred seleccionadas en este ejemplo también dependen de si las partes ruteables y no ruteables están siendo considerados. El protocolo punto a punto es usado cuando la infraestructura del nivel de planta es TELCO. Mientras que el protocolo punto-multipunto y los modems FSK son usados con el cable trenzado del nivel de Planta para las comunicaciones entre el controlador maestro y sus esclavos.

5.2 Centro a Centro

Dos ejemplos son provistos para las comunicaciones C2C.

5.2.1 Ejemplo de Implementación Centro a Centro usando DATEX

La figura 5.4 muestra un ejemplo de implementación C2C y es una variación de un enfoque usando DATEX. Este ejemplo de implementación tiene la intención de proveer los servicios de transporte de conexión orientada entre los centros de Gestión de Transporte soportando los dispositivos de campo esclavos.

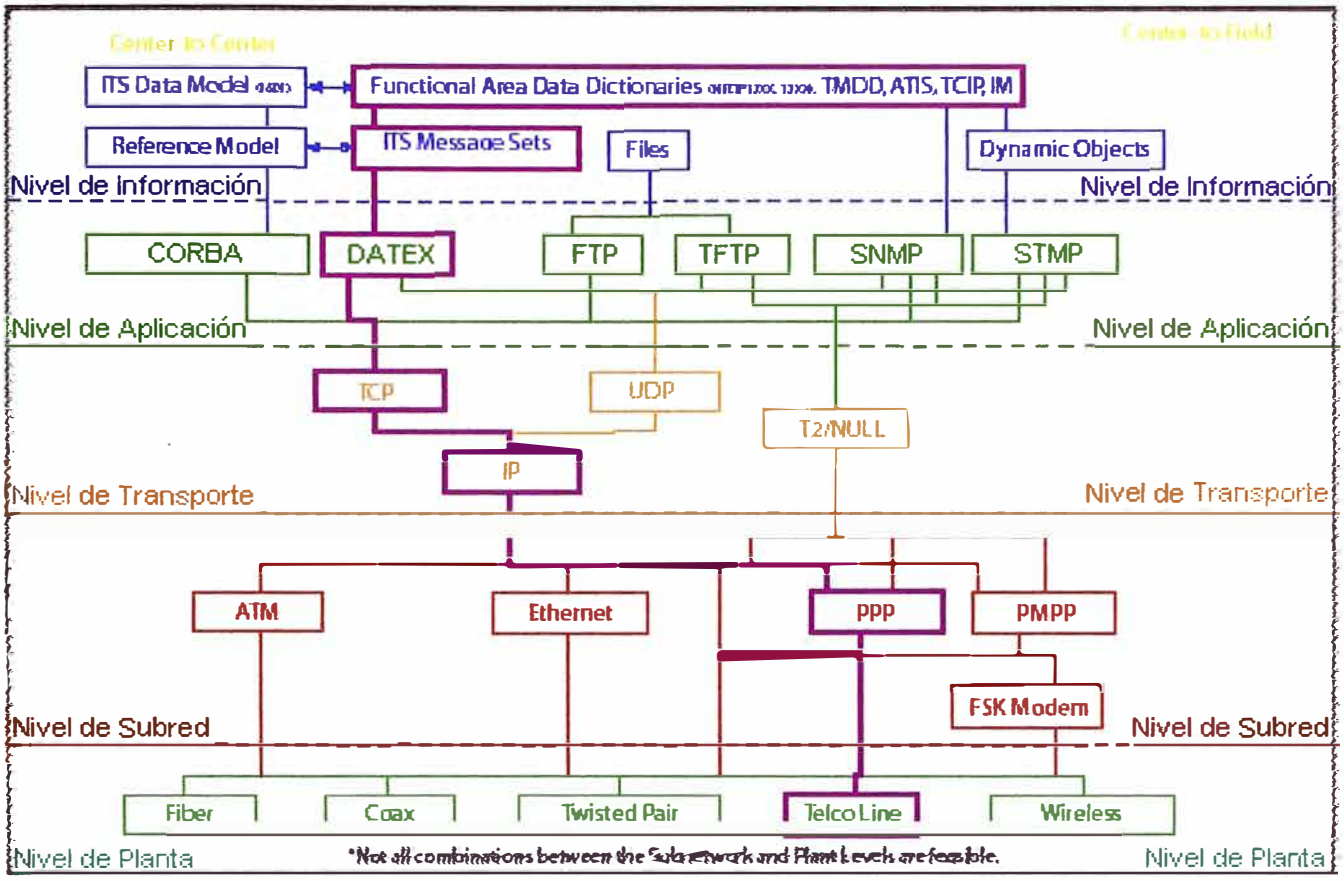

Figura 5.4: Ejemplo de Implementación Centro a Centro con DATEX

El ejemplo ilustrado destaca una implementación de la estructura NTCIP para comunicaciones C2C. La figura muestra las normas implementadas en cada nivel de esta estructura usando DATEX en el nivel de Aplicación dentro de dicha estructura.

Para las comunicaciones C2C, las opciones que son ofrecidas en el Nivel de Aplicación incluye DATEX y CORBA. Las opciones que son definidas para el nivel de Transporte son UDP/IP para servicios de transporte sin conexión y el TCP/IP para servicios de entrega de transporte con conexión orientada. Las opciones del nivel de Subred incluyen una variedad de opciones de grandes anchos de banda, tal como ATM, Ethernet y PPP. En este caso, un ejemplo podría ser para usar el Frame Relay con el protocolo punto a punto (PPP) en el nivel de Subred. El nivel de planta incluye una variedad de opciones tal como líneas telco, como este ejemplo, o fibra.

5.2.2 Ejemplo de Implementación Centro a Centro usando CORBA

Este ejemplo muestra una posible implementación de comunicaciones C2C usando CORBA.

La figura 5.5 representa un ejemplo de implementación C2C y es una variación de un enfoque usando CORBA. Este ejemplo de implementación tiene la intención de proveer servicios de entrega de transporte de conexión orientada entre los centros de gestión de transporte soportando los dispositivos de campo esclavos.

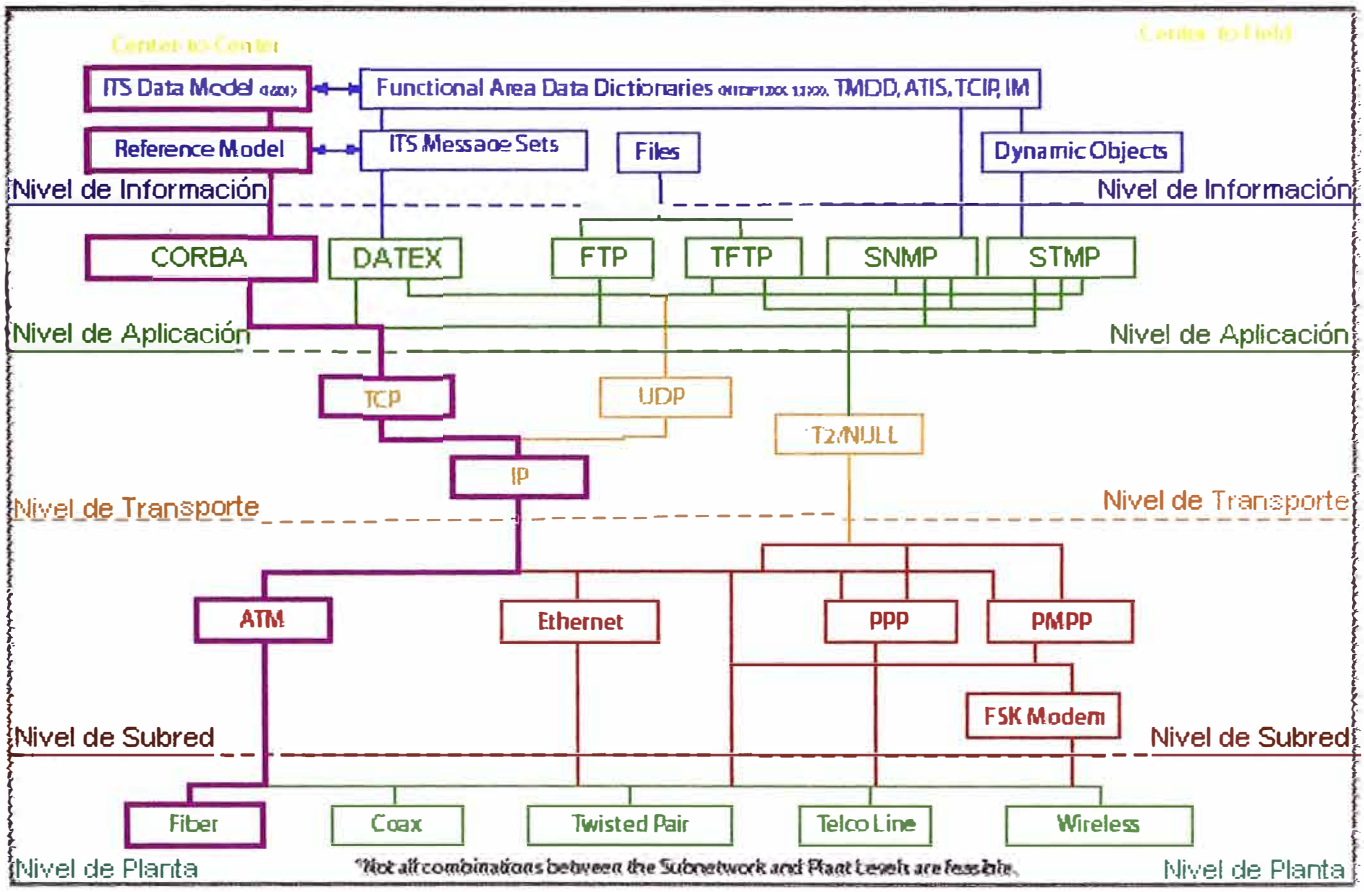

Figura 5.5: Implementación Centro a Centro con CORBA

La implementación ilustrada en la figura 5.5 destaca una implementación de la estructura NTCIP para comunicaciones C2C. La figura muestra las normas implementadas en cada nivel de la estructura NTCIP usando CORBA en el nivel de Aplicación dentro de dicha estructura.

Para las comunicaciones C2C, las opciones que son ofrecidas en el Nivel de Aplicación incluye DATEX y CORBA. Las opciones que son definidas para el nivel de Transporte son UDP/IP para servicios de transporte sin conexión y el TCP/IP para servicios de entrega de transporte de conexión orientada. Las opciones del nivel de Subred incluyen una variedad de opciones de altos anchos de banda, tal como ATM, Ethernet y PPP. En este caso, un ejemplo podría ser el uso de ATM en el nivel de Subred, aunque otras opciones podrían también ser apropiadas. El nivel de Planta puede incluir una variedad de opciones tal como fibra, como este ejemplo, o líneas telco.

CONCLUSIONES

Los Protocolos de Comunicación de Sistemas de Transporte Inteligente concluyen lo siguiente:

1. El propósito de estos protocolos es que como la comunidad del Transporte ha necesitado por mucho tiempo un sistema de transporte que pueda ser estructurado usando dispositivos y componentes que fuese ***intercambiables*** e ***interoperables***. Es por esta razón que esta familia de protocolos este siendo incluido y especificado en muchos nuevos desarrollos de sistemas.

2. Se concluye que construir más carreteras no es la solución a los problemas del transporte. Mediante el uso de equipos informáticos y dispositivos de comunicación, la infraestructura de transporte (sistemas de carretera y los vehículos usados) puede pasar a ser más inteligente, y por lo tanto, reducir los atascos, disminuir las emisiones de los vehículos en tráfico, reducir el tiempo de viaje, aumentar la capacidad de las carreteras existentes y hacer más seguros los desplazamientos por carretera.

3. Los ITS pueden ser definidos como el matrimonio entre los avances en tecnologías de información y sistemas de comunicación con los vehículos y redes de caminos que forman parte del sistema de transporte. Son inteligentes debido a que proveen de información oportuna tanto a usuarios como a operadores. Utilizando estas tecnologías en conjunto con el sistema de transporte es posible salvar vidas, ahorrar tiempo y dinero.

4. El NTCIP ofrece el incremento y las opciones para las agencias de operación de sistemas de gestión de transporte. Esto remueve barreras para las interagencias de coordinación y permite a los equipos de diferentes modelos y procedencias de fabricación ser mezclados en una misma línea de comunicación.

ANEXO A

CONFORMIDAD DEL PERFIL DE IMPLEMENTACION

Listas de Requerimientos

A1 Notación

Las siguientes claves son usadas, en la lista de conformidad subsecuente, se define las funciones, parámetros, clases, etc.

A1.1 Norma Base y Claves de Notación del Estado del Perfil

M, m ; obligatorio (mandatory).

O : opcional.

O.<n> ; opcional, pero soporta al menos uno de los grupos de opciones etiquetados por el mismo numeral.

<n> ; es requerido.

U ; no es ambiguo en la definición de la norma base.

<index> ; este símbolo significa que el estado siguiente se aplica solo cuando los estados PICS que uno o mas de los itmes es soportado.

<index>: ; cuando este grupo es cierto luego la cláusula asociada debe ser completada.

I ; afuera.

D ; depreciado (listado por la compatibilidad con otros sistemas mas antiguos).

- ; no aplicable.

X ; excluido (el uso es prohibido dentro del contexto de este perfil)

El nivel de requerimiento obligatorio "m" indicará que el soporte de la característica para todas las implementaciones reclaman soporte dentro de este Perfil.

El nivel de requerimiento opcional "o" indicará que el soporte de la característica es dejado al implementador.

El nivel de requerimiento condicional "c" indicará que el soporte para el item depende sobre una condición especificada. La condición y los requerimientos del apoyo resultante están separados.

El nivel de requerimiento obligatorio "I" indicará que el apoyo para el item es fuera del ámbito de esta parte.

A2 Lista de Requerimientos de PICS

A2.1 Capa de Aplicación

A2.1.1 Arquitectura y Especificación del CORBA

Tal como muestra la tabla A-1:

Tabla A-1: Arquitectura y Especificación del CORBA

	NORMA BASE			CORBA	
Item	**Característica**	**Estado del *Cliente***	**Estado del *Servidor***	**Estado del *Cliente***	**Estado del *Servidor***
1	El Modelo de Objeto	M	M	m	m
2	Arquitectura CORBA	M	M	m	m
3	Sintaxis y Semática OMG - IDL	M	M	m	m
4	Interface de Invocación Dinámica	M	M	m	m
5	Interface ORB	M	M	m	m
6	Interface esqueleto Dinámico	M	M	m	m
7	La Interface de Almacén	M	M	m	m
8	El Adaptador de Objeto Básico	M	M	m	m
9	Resumen de Interoperabilidad	O	O	o	o
10	Arquitectura de Interoperabilidad ORB	O	O	o	o
11	Puentes y Edificios Inter - ORB	O	O	o	o
12	Arquitectura Internetworking	O	O	o	o
13	Mapeo: COM y CORBA	O	O	o	o
14	Mapeo: Automatización OLE y CORBA	O	O	o	o
15	Requerim. para un Lenguaje de Mapeo	M	M	m	m
16	Mapeo de OMG IDL a C++	O.1	O.1	o.1	o.1
17	Mapeo de OMG IDL a ADA	O.1	O.1	o.1	o.1
18	Mapeo de OMG IDL a SmallTalk	O.1	O.1	o.1	o.1
19	Tipos de Normas OMG IDL	O.1	O.1	o.1	o.1
20	Arquitectura CORBA	M	M	m	m
21	Etiquetas OMG IDL	M	M	m	m

A2.1.2 Facilidades del CORBA

De acuerdo a la tabla A-2:

Tabla A-2: Facilidades del CORBA

NORMA BASE					CORBA	
Item	Característica	Dirección	Estado del Cliente	Estado del Servidor	Estado del Cliente	Estado del Servidor
1	Todas las Facilidades del CORBA	C->S	O	O	o	o

A2.1.3 Servicios del CORBA

La especificación del Servicio del Objeto Común CORBA. Se asume que como buena consideración de la Seguridad, Eventos, y Servicios de Dudas, la funcionalidad es obligatoria, aún si no puede ser provisto a través de los servicios del CORBA

Tabla A-3: Servicios del CORBA

NORMA BASE				CORBA	
Item	Característica	Estado del Cliente	Estado del Servidor	Estado del Cliente	Estado del Servidor
1	Principios de Diseño General	O	O	o	o
2	Especificación de Servicios de Nombramiento	O	O	o	o
3	Especificación de Servicio de Evento	O	O	o	o
4	Especificación de Servicio Objeto Persistente	O	O	o	o
5	Especificación de Servicio de Tiempo de Vida	O	O	o	o
6	Servicio de Control de Concurrencia	O	O	o	o
7	Especificación de Servicio Externo	O	O	o	o
8	Especificación de Servicio de Relación	O	O	o	o
9	Especificación de Servicio de Transacción	O	O	o	o
10	Especificación de Servicio de Duda	O	O	o	o
11	Especificación de Servicio de Licencia	O	O	o	o
12	Servicio de Propiedad	O	O	o	o
13	Especificación de Tiempo de Servicio	O	O	o	o
14	Especificación de Servicio de Seguridad	O	O	m	m
15	Modelo de Referencia de Seguridad	O	O	m	m
16	Autenticación de Servicios	O	O	m	m
17	Credenciales	O	O	m	m
18	Objeto de Referencia	O	O	o	o
19	Operación de Seguridad Normal	O	O	o	o
20	Seguridad Auditiva	O	O	m	m
21	Póliza de Seguridad de Administración	O	O	m	m
22	Uso de Interfaces para Control de Acceso	O	O	o	o
23	Uso de Interfaces para Delegación	O	O	o	o
24	Sin Rechazo	O	O	m	m
25	Protocolo Seguro Inter-ORB (SECIOP)	O	O	o	o
26	Especificación de Servicio de Objeto de Marca	O	O	o	m
27	Especificación de Colección de Objetos	O	O	o	o

A.2.2 Capa de Presentación

Arquitectura y especificaciones de CORBA, de acuerdo a la tabla A-4:

Tabla A-4: Especificaciones de CORBA

NORMA BASE					CORBA	
Item	Característica	Dirección	Estado del Cliente	Estado del Servidor	Estado del Cliente	Estado del Servidor
1	Representación de la Data Común GIOP		M	M	m	m
2	Cabecera de Mensaje GIOP		M	M	m	m
3	Tipos de Mensaje GIOP		M	M	m	m
4	Mensaje de Pedido	C->S	M	M	m	m
5	Mensaje de Respuesta	S->C	M	M	m	m
6	Pedido de Cancelar	C->S	M	M	m	m
7	Pedido de Localizar	C->S	M	M	m	m
8	Respuesta de Localizacion	S->C	M	M	m	m
9	Conexión de Cierre	C->S	M	M	m	m
10	Error de Mensaje	S->C	M	M	m	m
11	ESIOP		O	O	o	o
12	DCE-CIOP RPC		O	O	c::11	c::11
13	Invocar RPC		O	O	c::11	c::11
14	Localizar RPC		O	O	c::11	c::11
15	Representación de la data DCE-CIOP		O	O	c::11	c::11
16	Mensajes DCE-CIOP		O	O	c::11	c::11
17	Localización de Objeto DCE-CIOP		O	O	c::11	c::11

A2.3 Capa de Transporte (adiciones vía IIOP), Arquitectura y Especificaciones CORBA

De acuerdo a la tabla A-5:

Tabla A-5: Capa de Transporte, Arquitectura y Especificaciones CORBA

NORMA BASE				CORBA	
Item	Característica	Estado del Cliente	Estado del Servidor	Estado del Cliente	Estado del Servidor
1	Protocolo de Internet Inetr-ORB	M	M	m	m
2	Conexión de Uso TCP/IP	M	M	m	m
3	Perfiles IIOP IOR	M	M	m	m
4	Componentes de Perfiles IIOP IOR	M	M	m	m

ANEXO B

ESTRUCTURA DE GESTION DE TRANSPORTE SIMPLE (SIMPLE TRANSPORTATION MANAGEMENT FRAMEWORK – STMF)

B1. Introducción

El transporte MIB versión 2 (TMIB-II) provee una trama de trabajo para la organización e identificación de la información en localización de objetos para equipo específico de transporte. El TMIB-II esta ubicado bajo el nodo NEMA del árbol de objeto global. Este MIB es controlado por los Sistemas de Gestión de Transporte y los Dispositivos de Control Asociado NEMA (3 – TS). NEMA 3 – TS puede diseñar subnodo del TMIB-II para ser administrado por otros grupos u organizaciones.

B1.1 Tipos de Byte y UByte:

Cambiar el límite más bajo del Byte de -127 a -128.

B1.2 Tipos de Short y Ushort:

Cambiar el límite más bajo del Short de -32767 a -32768.

B1.3 Tipos de Long y Ulong:

Cambiar el límite más bajo del Long de -2147483647 a -2147483648.

B1.4 Tipo de EntryStatus:

Cambia el título de la cláusula a "ConfigEntryStatus Type".

Reemplaza todo el texto en esta cláusula con los siguiente: El tipo EntryStatus, ha sido reemplazado con el tipo ConfigEntrystatus, este tipo será usado para gestionar el dynObjDef (Tabla) que permite a nuevas filas ser creadas por las aplicaciones de gestión que funcionan remotamente. Para cada fila en el dynObjConfigTable habrá un objeto columnar que está definido con una SINTAXIS de ConfigEntrystatus. Este deberá tener tres valores: válido, bajoCreación (underCreation) e inválido. Otros objetos en la fila tendrán operaciones limitadas por el valor normal del objeto de EntryStatus en la fila. El significado de estos valores es como sigue:

Si el objeto de estado es *inválido*, entonces la información en las filas correspondientes del dynObjDef (Tabla) con el mismo índice dynObjNumber será considerado indefinido. Poniendo el objeto de estado a inválido, tiene el efecto de invalidar las filas correspondientes. Es implementación específica si el agente aclara los valores contenidos en una fila invalidada, desaloja la memoria asociada con filas inválidas o simplemente deja los últimos valores dentro de la fila. Cuando en el estado *inválido*, el agente rechazará cualquier pedido para ir al estado *válido*.

El estado de underCreation (bajocreación) indicará que la memoria para las filas correspondientes del dynObjDef (Tabla) con el mismo índice dynObjNumber es destinado, pero puede contener algunos datos inválidos. Cuando en este estado, la aplicación de gestión es permitido para modificar los valores de los objetos contenidos en las filas asociadas de la tabla. Una vez que esta operación es completada, la estación de gestión puede ponerse al estado válido, alternativamente, la estación de gestión puede cancelar la operación por colocar ele stado a inválido. Si el agente determina que una entrada ha sido en el estado de underCreation por un tiempo largo anormal, puede colocarse este objeto a *inválido*.

El estado válido indicará que las filas correspondientes del dynObjDef (tabla) con el mismo índice dynObjNumber contiene información que es creída para ser válida.

La siguiente tabla indica las acciones que tomarán lugar por encima del recibo de un conjunto de pedidos para cambiar el estado de las filas correspondientes del dynObjDef (tabla) con el mismo índice dynObjNumber. El valor de cada célula en la tabla muestra el resultado de recibir el conjunto indicado de pedidos (cabecera de columnas) cuando el dispositivo esta en el estado indicado (cabecera de filas).

Tabla B1: Tabla de Transición de Estado

		ESTADO COMANDADO		
		invalido	underCreation	valido
ESTADO NORMAL	invalido	invalido (1)	underCreation (1)	invalido (3)
	underCreation	invalido (2)	underCreation (3)	valido (4) o underCreation (5)
	valido	invalido (2)	valido (3)	valido (1)

Notas:

(1) no hay acción que tome lugar y responda las indicaciones noError.

(2) Todas las entradas asociadas con el objeto ConfigEntryStatus que son borrados y responden las indicaciones noError.

(3) No hay acción que tome lugar pero responde las indicaciones badValue.

(4) Si la consistencia revisa lo logrado, entonces el estado cambia a válido y responde las indicaciones noError.

(5) Si la consistencia revisa las fallas, entonces el estado hace recordar underCreation y responde las indicaciones genErr.

Por encima del recibo del conjunto de pedidos para el estado *válido* cuando en el estado de underCreation, el agente ejecutará una revisión de consistencia sobre los datos contenidos en las filas asociadas del dynObjDef (tabla) con el mismo índice dynObjNumber de la tabla. Si la revisión de la consistencia es lograda, el estado cambiará a válido, de otra manera, el estado recuerda que el estado underCreation y el dispositivo retornarán a genErr.

ANEXO C

¿COMO MIGRAR DE UN SISTEMA A OTRO?

C1 Actualización y/o Migración de Sistemas Center – to – Field Existentes.

No se puede actualizar o migrar versiones legales de software de controladores o controladores para hacerlos de conformidad a NTCIP. Las restricciones tal como potencia de computación, memoria disponible, costos de modificación pueden excluir las modificaciones. Si tales controladores o software no pueden ser mejorados o reemplazados, los sistemas de control de tráfico que continúen para hacer uso del equipo antiguo o versiones de software antiguos tendrán probablemente que continuar usando los protocolos únicos de comunicación con esos dispositivos. Sin embargo, los controladores y software de versión corriente dentro del sistema puede ser capaz de modificaciones al usar NTCIP y todas las futuras versiones deben ser especificadas conforme al NTCIP. Sin duda, el fabricante del equipo debe ser contactado y preguntado si las mejoras para la conformidad del NTCIP están disponibles.

La incapacidad de mejorar los equipos más viejos nunca deben detener a una agencia de reemplazos o estrategias de migración para hacer mas beneficioso las implementaciones de la conformidad NTCIP. Por ejemplo, un sistema central cuyos dispositivos de campo corrientes no son mejorados puede ser expandido para funcionar con los protocolos NTCIP sobre las canales de comunicación mientras los equipos más antiguos es mantenido en otros.

La Figura C.1 ilustra un modelo para una migración de tres pasos de los sistemas heredados a NTCIP. Como se muestra, inicialmente los detalles de la interface propietaria pueden o no pueden ser conocidos (indicado por una nube mostrando la posesión propietaria de los detalles del sistema). Luego, hay algún estado intermedio y algún período de tiempo donde el sistema operacional consiste de una mixtura de los sistemas heredados y el hardware más nuevo del NTCIP. Allí puede ser compartido el uso de un canal de comunicación común o no para dispositivos NTCIP y heredados – la figura ilustra estos como separado. El sistema de control central puede ser separado o combinado, puede correr sobre la misma computadora o en computadoras separadas – esto es determinado por el ámbito del proyecto para lograr estos pasos de la migración.

La búsqueda de una estrategia de migración para con el uso de las normas abiertas comienza a minimizar el uso de comunicaciones propietarias y se inicia para maximizar el uso del NTCIP (como se muestra por la nube ahora siendo dotado como esto comienza a atenuarse) Últimamente, en algún punto futuro, la migración es completada y el NTCIP esta totalmente desarrollada, teniendo reemplazado todo ahora retirado los sistemas heredados (no hay nube propietaria del todo).

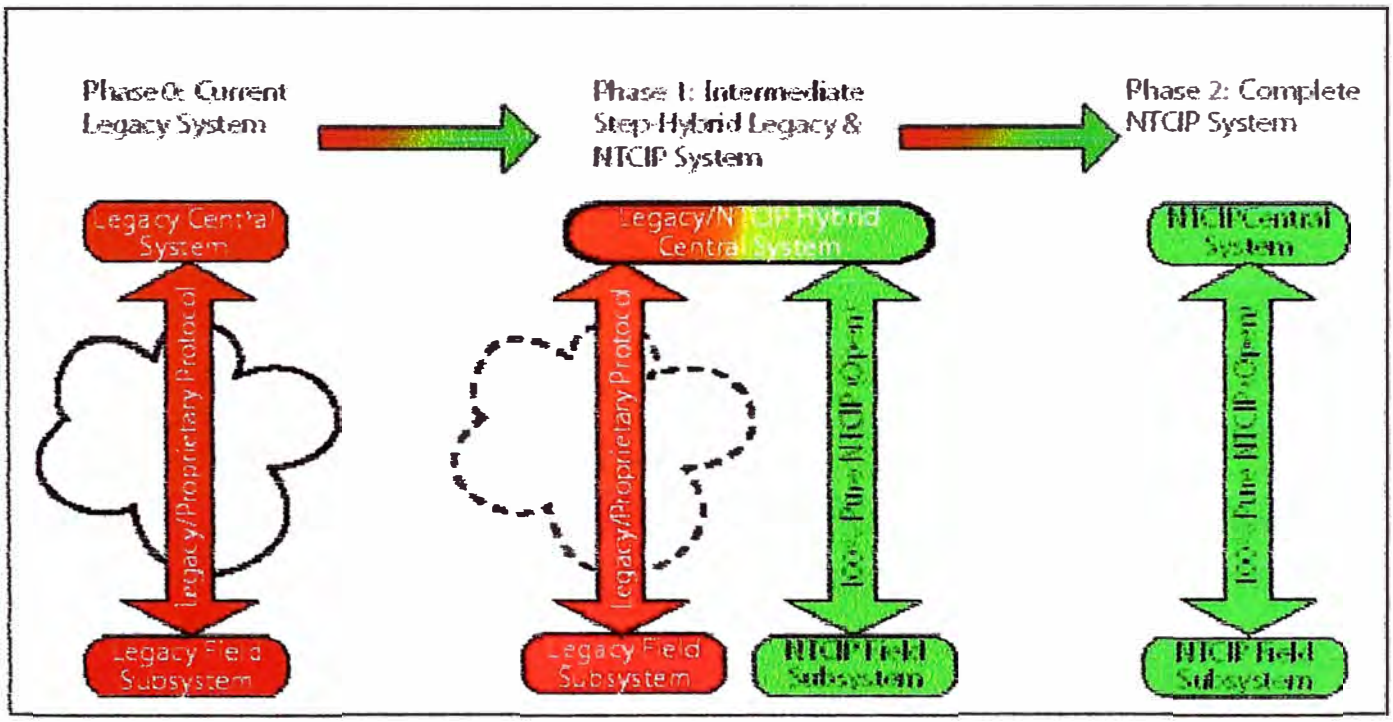

Figura C1: Un ejemplo del Proceso de Migración en Tres Fases

En general, los dispositivos NTCIP y los que no son, no pueden ser mezclados en el mismo canal de comunicación. Además, todos los dispositivos comparten un canal deben ser mejorados simultáneamente. Una computadora central o un controlador maestro que se comunica con ambos tipos de dispositivos necesitarán usar un puerto de comunicaciones diferentes para dispositivos NTCIP y para los que no son, y necesitará soportar ambos protocolos.

En los sistemas de señal de tráfico de lazo cerrado, la computadora central puede comunicarse con los controladores usando un protocolo diferente que ese use por el control maestro de campo para comunicarse con los controladores. Con los controladores y el control maestro de campo, el software de la computadora central necesitará ser modificado para añadir soporte para un protocolo NTCIP, si el NTCIP es usado para comunicaciones con controles maestros de campo.

Un enfoque para la introducción del NTCIP en un sistema C2F es operar dos sistemas separados – un NTCIP y otro que no lo es – durante un periodo de transición (ver el paso medio en Figura 2.7). Los dispositivos de campo pueden gradualmente ser conmutados sobre uno al otro como ellos son reemplazados o su software es mejorado. Esto puede ser la única opción, si el sistema corriente es bastante antiguo y mejorándolo para NTCIP no es práctico. Como una transición sería lógicamente hecha como parte de un sistema general mejorado.

C2 Materias Heredadas y Migración de Sistemas

La migración de sistemas heredados propietarios a esos que son normados puede seguir muchas trayectorias. Mientras este tema es primariamente asociado con la instalación inicial de las normas basado en el sistema, muchos de los conceptos discutidos aquí deben también ser considerados durante el ciclo de vida de un sistema basada en normas.

Dado que la migración tendrá un impacto en el software y hardware del sistema, y que el futuro cambie / mejore en tecnología son un hecho de la vida, la consideración debe ser dado para separarlas decisiones del hardware y el software. En muchos sistemas heredados antiguos, el hardware y software han sido provistos como un paquete integral. Solo como en la carpeta del PC world, los usuarios típicamente van a través de muchos software mejorados antes que el hardware sea finalmente reemplazado. La separación del software con el hardware también da al usuario la flexibilidad y una gran opción de software de aplicaciones potenciales. Muchos fabricantes y desarrolladores de sistemas están comenzando a estructurar sus sistemas en una manera que permita tal separación.

Hay muchas maneras que pueden ser tomados en la migración de los sistemas heredados a normas corrientes. Los dos más probables escenarios son presentados como sigue:

C2.1 Reemplazar el Sistema Entero de una vez:

Para agencias pequeñas con sólo un puñado de señales, este enfoque puede ser posible. Si la agencia tuvo previamente instalados dispositivos de campo que aceptarán nuevo software, los usuarios pueden fácilmente cargan el nuevo software durante un periodo de temporada baja. Sin embargo, para muchas agencias, esta estrategia puede proveer éxitos para pequeños subsistemas, pero no para un sistema entero.

C2.2 Migrar Partes del Sistema:

Los sistemas más grandes tendrán que ser averiados dentro de la chatarra manejable. El tamaño y forma de estas chatarras tendrán que ser cuidadosamente seleccionadas. Algunos de las restricciones en su selección son:

C2.2.1 Canales de Comunicación Disponibles:

El análisis de ancho de banda identificará cuántos canales de comunicación son necesitados. Los dispositivos son luego asignados a los canales disponibles. Todos los dispositivos en el mismo canal deben hablar el mismo lenguaje (por ejemplo, usar el mis protocolo de comunicación). El resultado de este enfoque es que dos sistemas separados deben ser operados, con frecuencia independientemente, hasta que la migración es completa. Un sistema operará usando los protocolos de comunicación y el otro operará usando los protocolos de comunicación heredados.

C2.2.2 Capacidad de Canal de Comunicación:

Esta restricción está cercanamente relacionada a lo anterior. Los protocolos de comunicación no pueden permitir tantos muchos dispositivos en un canal como sistemas heredados. En este caso, las infraestructuras de comunicaciones deben ser alteradas para acomodar la nueva carga de canal.

C2.2.3 Dotación de Personal:

El tiempo empleado estará necesitado para trabajo de campo, tan bien como la data de entrada, para el nuevo sistema. En muchas agencias el tiempo empleado disponible sugiere que estas mejoras tendrán que tomar un asiento de atrás para mantenimiento de emergencia. Las estrategias contraídas también necesitarán ser cuidadosamente considerados para determinar el enfoque del expediente principal para ejecutar estas actividades.

C2.2.4 Consideraciones Operacionales:

Una agencia puede querer considerar seleccionar menos localizaciones críticas para el primero desarrollamiento. Como tal, cualquier problema no cubierto durante el testeo del sistema puede ser corregido con el impacto mínimo. Para los sistemas de señal de tráfico, la consideración debe ser dada para seleccionar los grupos coordinados de señales.

Otros items con frecuencia pasados por alto incluyen un número de cosas que pueden tener una gran impacto en la migración del sistema.

- **Migración de la Data:** La data del sistema del antiguo sistema no puede ser fácilmente traducido al nuevo sistema. Tiempo y recursos tendrán que ser dedicados a la entrada de la configuración de la data necesitada para el nuevo sistema para operar eficientemente. Esto también incluye algunos gráficos que son necesitados.

- **¿Dos sistemas? :** Durante este periodo de migración habrá dos sistemas en operación. Si tu no puedes apagar y reemplazar el sistema entero de una vez, un plan será necesitado para el cuidado y alimentación del sistema heredado. No olvidar que la migración del sistema puede tomar muchos años, dependiendo por encima el tamaño del sistema y constituyendo la disponibilidad.

Al final de la migración del sistema es un sistema basada en normas que será menos costoso y menos difícultoso para la siguiente migración del sistema.

BIBLIOGRAFIA

1. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "CORBA Security Service Specification" – USA. 2001.

2. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "The NTCIP Guide - version 3" – USA, 2002.

3. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Application profile for Datex-ASN" – USA, 2001.

4. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Ethernet Subnetwork Profile" – USA, 2002.

5. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Point to Multipoint Protocol using FSK Modem Subnetwork Profile" – USA, 2002.

6. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Transportation transport Profile" – USA, 2002.

7. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Octet Encoding Rules (OER) Base Protocol" – USA, 2001.

8. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Simple Transportation Management Framework" – USA, 2001.

9. ASSHTO (American Association of State Highway and Transportation Officials), ITE (Institute of Transportation Engineers), NEMA (National Electrical Manufacturers Association), "Transportation Management Protocols" – USA, 2005.