

Universidad Nacional de La Plata

Facultad de Informática



Maestría en Redes de Datos

Trabajo Integrador para acceder a

A la Especialización de

Interconexión en Redes de Datos y Servicios

ETHERNET INDUSTRIAL:

Modelos y conectividad en el ámbito de procesos industriales

Director:

Ing. ing. Luís Marrone

Tesista:

Lic. José Carlos Prado

- 2010 -

ETHERNET INDUSTRIAL:

Modelos y conectividad en el ámbito de procesos industriales

INDICE

ETHERNET INDUSTRIAL:

MODELOS Y CONECTIVIDAD EN EL AMBITO DE PROCESOS INDUSTRIALES

CAPITULO 1

1. Introducción.....	7
1.1 Las comunicaciones en la Industria.....	8
1.2 Función de los niveles de comunicación industrial.....	10
1.2.1 Nivel de proceso.....	10
1.2.2 Nivel de campo/estación.....	10
1.2.3 Nivel de célula.....	11
1.2.4 Nivel de área.....	11
1.2.5 Nivel de fabrica.....	12
1.2.6 Nivel de empresa.....	12
1.3 Redes de control y redes de datos.....	13
Referencias bibliograficas.....	19
Referencias de figuras.....	19
Referencias de tablas.....	19

CAPITULO 2

2. Buses de campo.....	20
2.1 Introducción.....	20
2.2 Buses de campo y niveles OSI.....	20
2.2.1 Nivel físico.....	21
2.2.2 Nivel de enlace.....	21
2.2.3 Nivel de aplicación.....	21
2.3 La tecnología de los buses de campo.....	22
2.4 Buses propietarios y buses abiertos.....	22
2.5 Características.....	23
2.6 Ventajas y desventajas de los buses.....	23
2.7 Buses de campo existentes.....	24
2.7.1 Buses de alta velocidad y baja funcionalidad.....	24
2.7.2 Buses de alta velocidad y funcionalidad media.....	24
2.7.3 Buses de altas prestaciones.....	25
2.7.4 Buses para áreas de seguridad intrínseca.....	25
2.8 Funcionalidad de algunos buses estandarizados.....	25
2.8.1 Criterios de elección.....	25
2.9 Bus AS-i.....	26
2.9.1 Introducción.....	26
2.9.2 Características principales del bus.....	27
2.9.3 Otras características importantes.....	27
2.9.4 Relación con el modelo OSI.....	27
2.9.5 Capa física.....	28

2.9.5.1	Modulación de la señal.....	28
2.9.6	Capa de enlace de datos.....	29
2.9.6.1	Control de acceso al medio.....	30
2.9.7	Capa de aplicación.....	31
2.10	Bus DeviceNet.....	32
2.10.1	Relación con el modelo OSI.....	32
2.10.1.1	Capa física.....	33
2.10.1.2	Capa de enlace.....	33
2.10.1.3	Capa de red y de transporte.....	34
2.10.1.4	Capa de sesión.....	34
2.10.1.5	Capa de presentación.....	34
2.10.1.6	Capa de aplicación.....	35
2.11	Bus Profibus.....	35
2.11.1	Característica de comunicación.....	36
2.11.2	Arquitectura de protocolos.....	36
2.11.3	Relación con el modelo OSI.....	36
2.11.4	Control de acceso al medio.....	37
2.11.5	Capa de aplicación.....	38
2.11.6	Topologías.....	38
2.12	Comparación de los buses de campo.....	39
	Referencias bibliograficas.....	41
	Referencias de figuras.....	41
	Referencias de tablas.....	41

CAPITULO 3

3.	Ethernet Industrial.....	43
3.1	Introducción.....	43
3.2	Requerimientos para su utilización en planta.....	44
3.3	Consideraciones de la capa física de Ethernet Industrial.....	45
3.4	Hardware necesario.....	46
3.4.1	Medios y conectores.....	46
3.4.2	Placas de interfaz o nic.....	47
3.4.5	Switches.....	47
3.4.6	Routers.....	48
3.4.6.1	Funcionamiento de OPC.....	49
3.4.7	Gateways.....	51
3.4.8	GPRS.....	51
3.4.9	Convertidores fibra – cobre.....	51
3.4.10	Comserver.....	52
3.4.1	IWLAN (Redes inalámbricas industriales).....	52
3.5	Topologías empleadas.....	53
3.5.1	Topología Bus.....	53
3.5.2	Topología anillo.....	54
3.5.3	Topología estrella.....	55
3.6	Método de acceso al medio.....	56
3.7	Acceso determinístico – Switch Ethernet.....	58
3.7.1	Características adicionales de los switch industriales.....	60
3.7.2	Funciones de administración.....	61
3.8	Protocolo Spanning- Tree.....	62

3.9	Otras soluciones.....	64
3.10	Ethernet basado en tiempo real.....	65
3.11	Protocolos de la capa de aplicación para Ethernet Industrial.....	65
3.11.1	Ethercat.....	66
3.11.2	Profinet (Profibus).....	68
3.11.3	Ethernet Power Link.....	72
3.11.4	Ethernet IP.....	77
3.11.5	Modbus TCP/IP.....	81
3.11.5.1	Estructura del protocolo.....	82
3.11.5	Sercos III.....	84
3.11.7	CC-Link IE.....	86
3.12	Perspectiva de Ethernet Industrial.....	89
	Referencias Bibliograficas.....	89
	Referencias de figuras.....	90
	Referencias de tablas.....	90

CAPITULO 4

4.	Redes Inalámbricas (Wi-Fi).....	91
4.1	Introducción.....	91
4.2	Tecnologías Inalámbricas.....	92
4.2.1	Red Pan (Personal Área Network).....	92
4.2.1.1	RFID.....	93
4.2.1.2	Tecnología ZigBee.....	95
4.2.1.3	Bluetooth (IEEE 802.15.1).....	98
4.2.2	Redes WLAN (Wireless Local Area Network).....	102
4.2.2.1	IEEE 802.11b.....	103
4.2.2.2	IEEE 802.11g.....	104
4.2.2.3	IEEE 802.11a.....	104
4.2.2.4	IEEE 802.11h.....	104
4.2.2.5	Capa física.....	104
4.2.2.6	Capa de enlace.....	106
4.2.2.7	Configuraciones WLAN.....	108
4.2.2.8	Dispositivos para comunicaciones industriales.....	110
4.2.2.9	Seguridad de la red inalámbrica.....	110
4.2.2.10	Otras características de la norma IEEE 802.11.....	111
4.2.3	Redes Wi-Fi MAN (Wi-Max 802.16).....	111
4.2.4	Redes WWAN (Wi-Fi Wide Area Network).....	112
4.2.4.1	Red GSM.....	113
4.2.4.2	Redes EDGE.....	113
4.2.4.3	Redes HSCSD.....	114
4.2.4.4	Redes UMTS.....	114
4.2.4.5	Redes GPRS.....	115
4.3	Redes IWLAN (Industrial Wireless).....	116
4.3.1	Monitoreo del canal inalámbrico.....	117
4.3.2	Determinismo y tiempo real.....	119
4.3.3	Roaming forzado.....	121
4.3.4	Modos de conexión y operación.....	122
4.3.4.1	Sistema distribuido inalámbrico.....	122
4.3.4.2	Utilización de cables de radiación coaxial (RCOAX).....	124

4.3.4.3 Operación en modo puente (Bridge).....	125
4.3.4.4 Operación en modo redundante.....	126
4.3.4.5 Infraestructura inalámbrica redundante – Spanning-Tree (ST).....	126
4.3.4.6 Función de Hopping (IHOP).....	126
4.3.4.7 Función de HiPath Wireless Controller.....	127
4.3.5 Seguridad de datos y protección contra acceso no autorizado.....	128
4.3.6 Otras normas IWLAN a utilizar.....	129
4.3.6.1 Norma 802.11e.....	129
4.3.6.2 Norma 802.11i.....	129
4.3.6.3 Norma 802.11n.....	130
4.3.6.4 Norma 802.11s.....	130
4.3.7 Aplicaciones IWLAN.....	131
4.3.7.1 Comunicación con estaciones móviles para adquirir datos.....	132
4.3.7.2 Servicio móvil.....	132
4.3.7.3 Adquisición de datos en depósitos y logística.....	132
4.3.8 Ejemplos de aplicación de una red IWLAN integrada.....	133
4.3.8.1 Aplicación en una planta procesadora de huevos.....	133
4.3.8.2 Aplicación en planta de fabricación de automóviles.....	134
4.3.9 Actualidad y futuro de las redes inalámbricas.....	136
4.4 Conclusiones.....	137
Referencias bibliograficas.....	141
Referencias de figuras.....	142
Referencias de tablas.....	143
Glosario.....	144

ETHERNET INDUSTRIAL:

MODELOS Y CONECTIVIDAD EN EL AMBITO DE PROCESOS INDUSTRIALES

1. INTRODUCCION

Las comunicaciones en la industria han seguido un proceso gradual, aplicando las tecnologías disponibles en cada momento. Esto ha dado lugar a las denominadas “islas automatizadas”, término empleado para designar una serie de equipos aislados entre sí y dedicados al control de una maquina o parte de un proceso. Dichos equipos pueden ser PLCs, computadoras utilizadas en diseño y gestión, controladores numéricos, sensores, actuadores, etc.

El desarrollo de las comunicaciones, y su aplicación en la industria, especialmente las redes Ethernet, han permitido la implantación de redes industriales que facilitan la comunicación entre estas isla automatizadas, aumentando el rendimiento y las posibilidades de control.

La integración de los diferentes equipos y dispositivos existentes en una planta, se hace dividiendo las tareas entre grupos de diferentes procesadores, formando un modelo jerárquico de fabricación asistida por computador (CIM), que de acuerdo a la función y el tipo de conexiones se dividen en varios niveles de control, permitiendo que los datos de producción y de servicios estén disponibles, prácticamente en toda la planta y a disposición de ser accedidos cuando se desee, por el personal de control desde sus puestos, e influenciar con sus acciones en todo el proceso.

Ethernet Industrial es similar a la Ethernet convencional, pero está rediseñada para ser utilizada en plantas tanto de procesos continuos como de manufactura. La misma utiliza componentes y medios Ethernet estándar para reemplazar a los protocolos especializados tradicionalmente de las redes industriales y para satisfacer los requerimientos, incorpora características de robustez, redundancia y durabilidad, que permiten a los diferentes dispositivos seguir conectados a pesar de las diversas condiciones agresivas que se trabajan en planta.

Ethernet Industrial permite a las empresas tomar datos de una línea de manufactura y utilizarlos en el software corporativo, como por ejemplo las aplicaciones de control de inventarios y de gestión de activos. Todos los dispositivos de entrada/salida pueden trabajar con la Web, con solo colocar una dirección IP en los sistemas, toda la información de diagnóstico sobre ellos estará disponible en tiempo real para ser utilizada por los encargados de las tareas de diagnóstico, mantenimiento y monitorización remota.

En la actualidad las comunicaciones en tiempo real, son muy importantes en las aplicaciones industriales. Muchas soluciones se basan en procesos rápidos y cíclicos con tiempo de respuesta debajo de los 100 ms., factores que afectan la confiabilidad y la velocidad de traspaso de los datos entre los dispositivos de la red, los que tienen que cumplir con tiempos de respuesta estrictos, especialmente para equipos en movimiento,

que necesitan recursos estandarizados como “reserva de datos” y “mecanismos de traspaso”, recursos ofrecidos por las redes inalámbricas industriales IWLAN.

Las redes inalámbricas son cada vez más populares. Permiten un alto grado de flexibilidad y reducción de costos durante la instalación y operación de la planta, por eso es que se utilizan mucho en: automatización de procesos y manufactura. Sin una conexión inalámbrica a la red de comunicación principal, muchas aplicaciones con equipos en movimiento serian imposibles o solo se podrían implementar con muy poca eficiencia.

En una red inalámbrica, los datos de producción y de servicio están disponibles prácticamente en toda la planta (como se muestra en la Figura Nro: 1, y por ello están a disposición de ser accedidos cuando se lo desee por los ingenieros de planta, donde podrán seguir desde sus puestos los procesos e influenciar sobre ellos. En la figura se muestra una red de comunicación industrial típica de Siemens, desde el nivel de proceso al nivel de gestión.

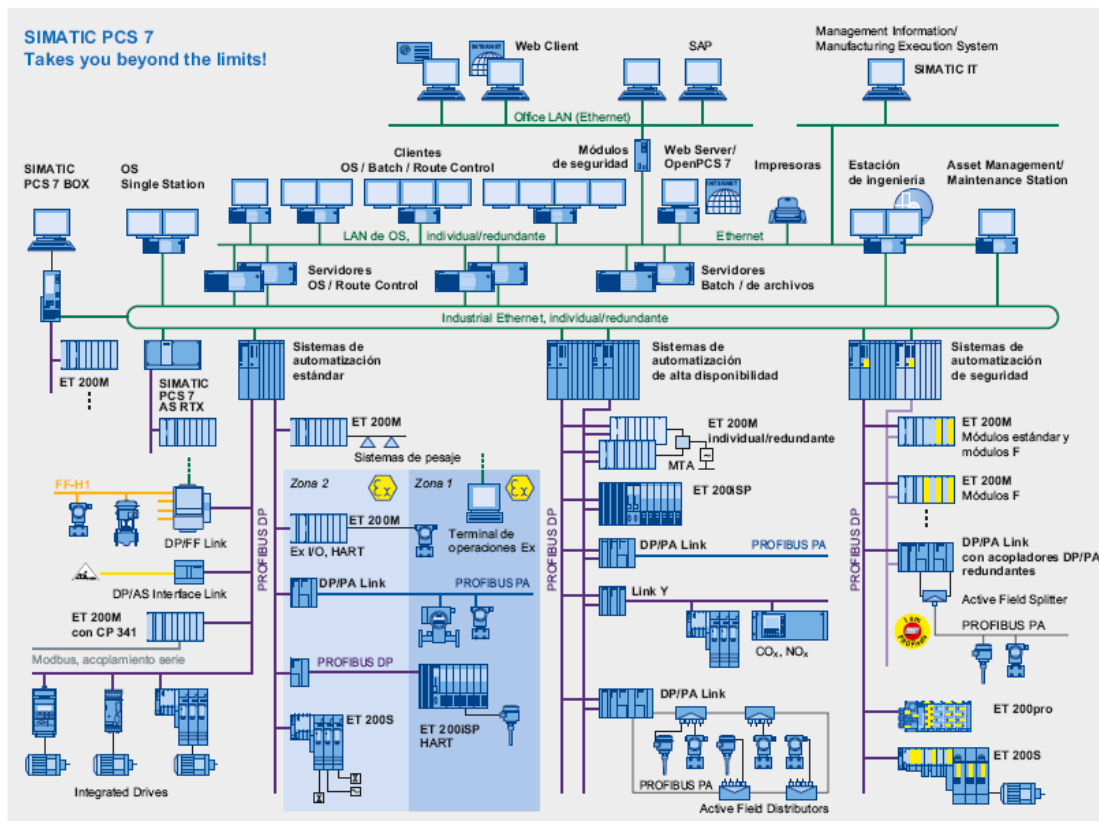


Fig. Nro: 1 Red de comunicación Industrial Siemens ⁽¹⁾

1.1 LAS COMUNICACIONES EN LA INDUSTRIA

Las comunicaciones desempeñan una importante función en la implantación de los sistemas modernos de Automatización Industrial, función vital para empresas cuyas operaciones se encuentran dispersas geográficamente, como ser la supervisión y control de estaciones petroleras, refinerías, fábricas, etc.

Dichas redes de comunicaciones tienen los siguientes objetivos:

- a) Transmisión de datos desde la planta, hasta los Centros de Control de Operaciones y de Procesamiento de la Información.
- b) Recolección de datos, instantáneamente desde las localidades remotas.
- c) Proveer servicios paralelos de Transmisión de Voz e Imágenes.
- d) Proveer recursos para aumentar la confiabilidad y la seguridad en los procesos productivos, mediante la detección temprana de alarmas, supervisión y el control continuo de procesos de alto riesgo, verificación del estado de las instalaciones y seguimiento de las condiciones de operación de estaciones remotas.

Además, en la actualidad los Sistemas de Planificación de la Producción y de los Recursos de Manufactura (MRP / MRPII), Sistemas de ejecución de la Manufactura (MES), planificación de los Recursos Empresariales (ERP), requieren información de la planta y no tiene sentido que esta información sea digitada manualmente. Esta información deberá fluir de forma transparente desde el piso de planta hasta el de gestión sin ningún tipo de inconveniente.

Hay que tener en cuenta también que la tecnología de la información, ha comenzado a salir del ámbito de la empresa hacia otros lugares, como ser: clientes y proveedores, con nuevos conceptos: e-business, e-commerce, B2B Business To Business, B2C Business To Commerce y las Cadenas de Abastecimiento, lo cual hace que la integración sea una necesidad.

Para poder cumplir con esta serie de objetivos la red de comunicaciones esta integrada, en base a un modelo arquitectónico bien definido, permitiendo: calidad, confiabilidad y conectividad en la transmisión de datos. Así nació un nuevo concepto como es el de Fabricación Integrada por Computadora CIM (Computer Integrated Manufacturing). El mismo representa la conjunción de las 3 fases productivas: diseño, ingeniería y fabricación.

De esta forma podemos representar la estructura de cualquier empresa manufacturera completamente automatizada con una pirámide escalonada llamada Pirámide CIM.



Fig. Nro: 2 Pirámide de integración CIM ⁽²⁾

Este modelo fue introducido en la década de los 70-80, por el inglés Joseph Harrinton, con la función de la aplicación de computadoras en el control de procesos productivos, posteriormente fue mejorando el sistema con la colaboración de un grupo de investigación de la Universidad de Purdue de los Estados Unidos de Norte América.

En la actualidad la mayoría de los dispositivos utilizados en la industria, desde los básicos que componen un Sistema de Automatización y Control, tienen alguna capacidad de procesamiento o inteligencia, como los sensores, instrumentos de medición y actuadores, que están basados en un microprocesador o microcontrolador, que los convierten en pequeñas computadoras, con la capacidad de procesar datos del sistema.

1.2 FUNCION DE LOS NIVELES DE COMUNICACIÓN INDUSTRIAL

Los diferentes niveles llevan a cabo las siguientes funciones:

1.2.1 NIVEL DE PROCESO

El nivel inferior (nivel **de proceso**). Este nivel es la base fundamental de todo sistema de automatización y control, es donde se encuentran todos los dispositivos que transforman la materia prima y energía para poder obtener un producto final. Se realiza el control digital directo de las variables del sistema o el control de los elementos de fabricación (en sistemas de fabricación flexible). Se adquieren datos, y se actúa en función de los algoritmos de control y consignas seleccionadas por el nivel superior. Se ejecutan programas de mecanización o manipulación, se activan alarmas y se transmiten los mensajes e informaciones oportunas al nivel superior.

Podemos clasificar los dispositivos de este nivel en dos grupos:

Los equipos que recogen la información del nivel de planta y la envían a los niveles superiores, compuestos por los **Sensores e Instrumentación**, pudiendo procesar tanto información analógica como digital.

Los dispositivos que reciben la información de los niveles superiores y la entregan al nivel de proceso, llamados **actuadores, acondicionadores o manipuladores**. Los actuadores modifican o cambian el proceso, (paso de un fluido, gas, agua, energía eléctrica, etc.), definiendo la función de entrada de la planta y pueden ser tanto analógicos como digitales.

La tendencia es que todos los dispositivos de este nivel tengan una comunicación bidireccional, y no solo transferencia de información unidireccional, de tal forma que los dispositivos no solo envíen información del proceso o de autodiagnóstico, sino que también puedan recibir información de calibración y de ajustes. Todo esto es posible si estos dispositivos puedan conectarse a una red de comunicaciones, que en la actualidad son los buses de campo y redes Ethernet industriales.

1.2.2 NIVEL DE CAMPO/ ESTACION

En el nivel de **campo/estación**, es donde están los dispositivos que tienen algún tipo de inteligencia o procesamiento y que tienen capacidad de comunicarse con otros

equipos, estos son los IEDs (dispositivo electrónico inteligente), como ser los PLC o autómatas que poseen un programa de control con funciones lógicas, secuenciales y matemáticas que permiten que la planta se comporte de acuerdo al requerimiento del operador.

En la actualidad, estos dispositivos inteligentes tienen la capacidad de adquirir, convertir, visualizar y procesar varias variables analógicas o digitales. También se encuentran los paneles del operador o consolas IHM (interfaz hombre maquina), las cuales se encuentran cercana al proceso y al controlador permitiendo al operador visualizar las variables del proceso como así también ingresar valores de corrección.

La comunicación industrial, entre los diferentes dispositivos y el envío de información hacia el nivel superior, se efectúa por redes, que se diferencian de las de computadoras, por los tiempos de respuestas y la cantidad de información que manejan.

1.2.3 NIVEL DE CELULA

Este nivel es del sistema de Supervisión e Interfaces Hombre Maquina (HMI, MMI SCADA), es el nivel de fabricación o de control.

Este nivel esta compuesto por la unión de Hardware y Software que permiten:

- Presentar, la información capturada en la planta de forma grafica y amigable al operador.
- Anunciar al operario las condiciones de anormalidad de la planta (alarmas y eventos).
- Almacenar dicha información en registros históricos para su análisis inmediato o posterior para la toma de dediciones operativas.

Este nivel tiene como punto fundamental el ingreso de la información, la conexión a la red de comunicación industrial, y la posibilidad de conectarse hacia los niveles de gestión de la producción y administrativos. Una de sus bondades es poder centralizar la información en un solo punto de operación evitando el desplazamiento de los operadores de forma periódica hacia los paneles para tomar información o para introducir algún parámetro de control.

Los equipos de este nivel pueden estar ubicados a unos metros del proceso o a varios kilómetros, debido a esto cambian su nombre. Los que están montados sobre los paneles de las maquinas (pocos metros), se los denomina “Paneles de operación local”, cuando están ubicados en la sala de control de la planta se los conoce como MMI o HMI (Interfaz Hombre Maquina o Interfaz Humano Maquina) o sistema de supervisión, y cuando se encuentran a varios kilómetros en aplicaciones distribuidas, como en acueductos, oleoductos, etc., se los denomina SCADA (Supervisory Control And Data Acquisition).

1.2.4 NIVEL DE AREA

En este nivel se lleva a cabo la visualización, supervisión y coordinación de las múltiples áreas de la planta de producción. Controla y organiza toda el **área** de

producción tratando de optimizar balances de materiales y energía (flujos entre almacén, planta, distribución e incluso proveedores). Para ello establece las condiciones de operación de cada proceso del área y las envía a cada control supervisor para que estos las adapten y distribuyan entre los controles directos.

La información aquí visualizada, es información clasificada de producción como: actividad o inactividad de una maquina, numero de unidades producidas, calculo de índices de producción, etc. Se usan tres vías para capturar la información, comunicaciones directamente con los controladores y computadores de los niveles inferiores a través del método **cliente-servidor, maestro esclavo** o visualización de las variables utilizando tecnologías de Internet como ser paginas **WEB**.

1.2.5 NIVEL DE FABRICA

En este nivel se realiza la planificación, gestión, diseño y análisis de la producción del conjunto de la **fábrica**, tareas que manejan mayor cantidad de información que los niveles inferiores. También se encuentran los elementos de la oficina técnica que mediante herramientas CAD/CAM/CAE permiten el diseño de productos y la elaboración automática de programas para los diferentes elementos de fabricación.

Las operaciones que se llevan a cabo en este nivel son las siguientes:

- Planificación de la manufactura: MRP / MRPII (Manufacturing Resource Planning).
- Ejecución de la manufactura: MES.
- Diseño asistido: CAD (Computer Aid Desingn).
- Estadísticas: SPC (Statistical Process Control).
- Mantenimiento.

1.2.6 NIVEL DE EMPRESA

En este nivel se encuentran los sistemas informáticos que integran todas las dependencias de la fabrica/empresa, la cual puede tener una o varias plantas de producción distribuidas geográficamente. La herramienta utilizada es la ERP (Enterprise Resource Planning).

El intercambio de la información hacia el nivel de planta se realiza entre el ERP y el MES/MRP, como la forma mejor estructurada, sin embargo también es posible tener conexión directa con los sistemas HMI y controladores distribuidos en toda la fabrica.

Esta aplicación cubre el nivel interno de la empresa, sin embargo con la expansión de las tecnologías de Internet y las técnicas de seguridad utilizadas en la misma, han hecho que el intercambio de información sobrepase el perímetro corporativo e involucre a otras compañías con las cuales se interactúa, como ser: proveedores, clientes y los clientes potenciales (mercadeo y publicidad), que a través de conceptos como B2B (Business to Business), B2C (Business to Comerse), e-Commerce, e-Business, Suply Cchain o cadena de suministro, las cuales permiten manejar información de excelente calidad y veracidad, tomada en tiempo real desde el extremo más lejano de la planta.

En la siguiente figura se muestra un modelo jerárquico de comunicaciones para plantas complejas de control.

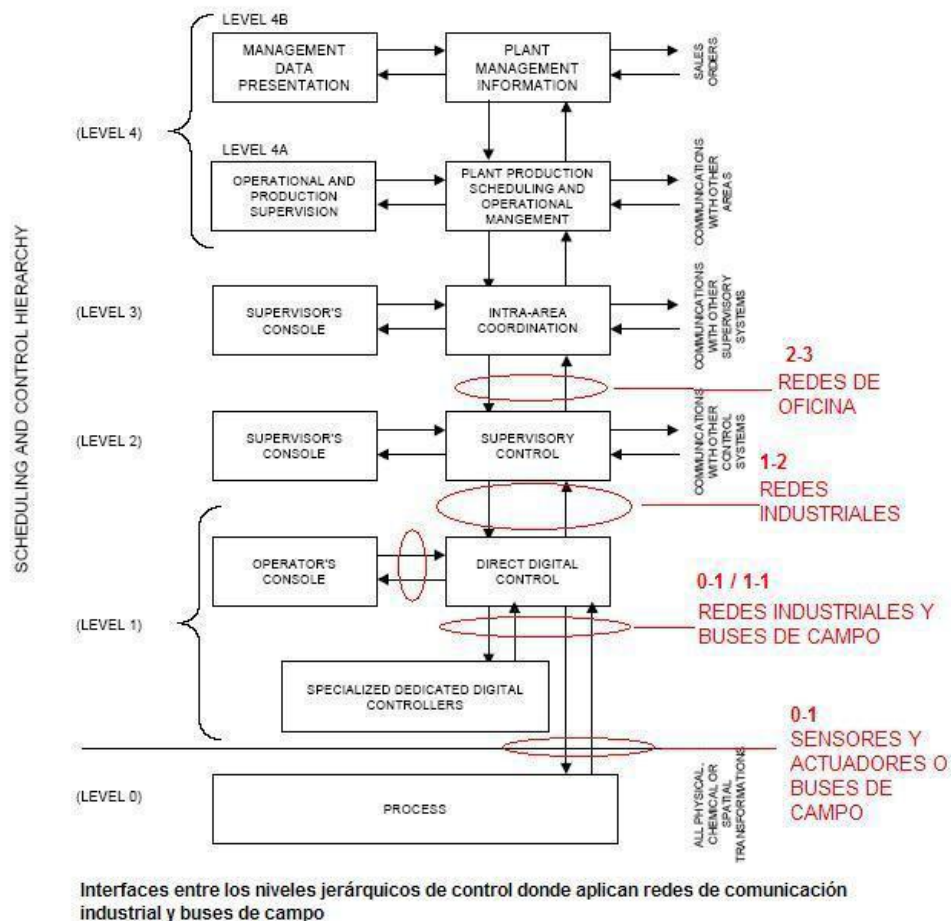


Fig. Nro: 3 Redes de Comunicaciones entre los diferentes niveles ⁽³⁾

1.3 REDES DE CONTROL Y REDES DE DATOS

En el esquema piramidal, existen diferentes modelos de comunicación, cada uno de ellos con diferentes necesidades, por lo tanto la podemos dividir en de dos tipos de redes: **redes de control** y **redes de datos**. La primera esta ligada a la parte baja de la pirámide, mientras que la de datos (ofimática), esta ligada a la parte alta de la estructura.

Por lo general las **redes de datos** están orientadas al transporte de grandes paquetes de datos, que aparecen de forma esporádica (baja carga), y con un gran ancho de banda, para permitir un envío rápido de una gran cantidad de datos.

Las **redes de control** manejan un tráfico formado por un gran número de paquetes pequeños, que se intercambian con frecuencia entre un gran número de dispositivos que forman parte de la red y que muchas veces trabajan en tiempo real.

En función de lo expuesto, es necesario utilizar una arquitectura de red adaptada a las características particulares de este tipo de tráfico, como así también a los diferentes protocolos utilizados, la interoperabilidad, la topología y la facilidad de administración.

<p><u>Red de datos</u></p> <ul style="list-style-type: none"> - Tamaño grande de paquetes - Baja tasa de paquetes - Área extensa 	<p><u>Red de control</u></p> <ul style="list-style-type: none"> - Tamaño pequeño de paquete - Alta tasa de paquetes - Requisitos de tiempo real
<p><u>INTERFACE DE RED</u></p> <p>Procesador</p> <ul style="list-style-type: none"> * PC * Estación de trabajo * Mainframe <p>Entrada/Salida</p> <ul style="list-style-type: none"> * Terminal * Impresora, etc. 	<p><u>INTERFACE DE RED</u></p> <p>Procesador</p> <ul style="list-style-type: none"> * PC * Microcontrolador * Microprocesador <p>Entrada/Salida</p> <ul style="list-style-type: none"> * Sensor * Actuador

Tabla Nro.1: Comparación entre redes de datos y redes de control

Por lo tanto en las redes de control se pueden distinguir dos tipos de redes según la información que transporten: **Redes basadas en comandos** y **Redes basadas en estado**. En las **redes basadas en comandos**, la información consiste en una orden emanada de un nodo para el control de funcionamiento de otro nodo.

El problema que se presenta, es que si se dispone de un amplio conjunto de nodos diferentes, habrá un aumento exponencial del número de comandos y sobrecarga de procesamiento.

En las **redes orientadas a estado** las cosas son más sencillas, en este caso la funcionalidad de un nodo no depende de otro, cada uno enviara mensajes en los que indicara a los demás nodos el estado en que se encuentra, por lo tanto los nodos que reciban estos mensajes, modificaran su estado en función de la nueva información. Existen implementaciones que combinan ambos métodos.

Con respecto al tipo de topología a adoptar por las redes de control, cabe destacar que cualquiera de las topologías clásicas de las redes de datos es valida (Como se muestra en la figura Nro: 4, bus, estrella, anillo, etc.).

Cada una de ellas con sus ventajas y limitaciones. La elección a efectuar, esta determinada en función por el control de acceso al medio y al tipo de medio que se empleara, esto afecta prácticamente a cualquier otro aspecto de la red de control: costo, instalación, prestación, fiabilidad, facilidad de mantenimiento y expansión de la red.

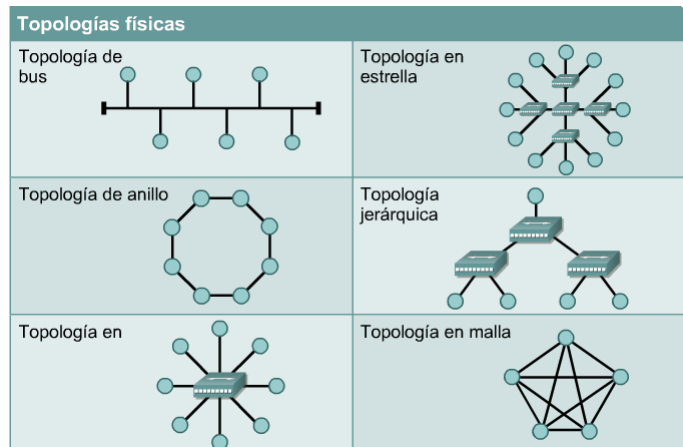


Fig. Nro: 4 Topologías físicas ⁽⁴⁾

Al seleccionar una topología hay que definir, el control de acceso al medio, que es muy importante de cómo los nodos accederán a la red. El principal objetivo es como reducir/ eliminar las colisiones, entre los diferentes paquetes de datos y reducir el tiempo en que el nodo tarda en acceder al medio y comenzar a transmitir. Lo que se pretenderá es maximizar la eficiencia de la red y reducir lo más posible el retardo de acceso al medio. Este último parámetro expuesto, es el factor principal a la hora de determinar si una red sirve o no para aplicaciones en tiempo real.

El direccionamiento de los nodos es otro aspecto clave. En una red de control, la información puede ser originada y/o recibida por cualquier nodo, la forma en que se efectuó influirá en la eficiencia y la fiabilidad del sistema de red. Existen tres tipos de direccionamiento a utilizar:

- a) **Unicast**: El paquete es enviado a un único nodo destino.
- b) **Multicast**: El paquete es enviado a un grupo de nodos simultáneamente.
- c) **Broadcast**: El paquete es enviado a todos los nodos de la red simultáneamente.

Los esquemas de direccionamiento **unicast** y **multicast** son eficientes, facilitan operaciones de acuse recibo y reenvío de paquetes, características que aumentan la fiabilidad del sistema. El direccionamiento **broadcast** presenta la ventaja de la sencillez. Es adecuado para redes basadas en información de estado, cada nodo informa a los otros nodos en que estado se encuentra. El principal inconveniente que presenta, es que los nodos deberán procesar paquetes que no le pertenecen.

Hay que tener presente que en las redes de tiempo real se requieren los tres modos de direccionamiento que se aplicaran a todas las capas del modelo OSI.

En redes de control, es habitual encontrar esquemas de direccionamiento **maestro-esclavo** y **cliente servidor**, como se puede observar en las figuras 5 y 6. Estos tipos de direccionamiento permiten plasmar aspectos jerárquicos de control, a la vez que simplifica el funcionamiento y abarata los costos de la interfaz física de la red. Además requieren la utilización de ciertos protocolos comunes, sobre todos protocolos de sistemas abiertos, para poder aplicar software y hardware de distintos fabricantes. En el modelo **cliente/servidor**, el cliente emite una demanda de servicio al servidor y este la trata y envía una respuesta al cliente. Es distinto al de **maestro-esclavo** en el que una

estación (**maestro**), actúa como director de las comunicaciones y el resto (**esclavos**) siguen el ritmo marcado por el.

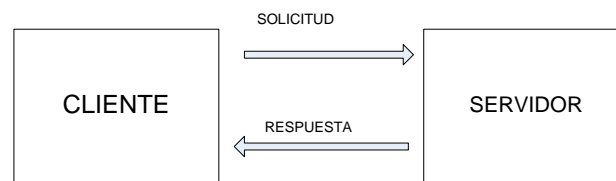


Fig. Nro: 5 Modelo Cliente – Servidor

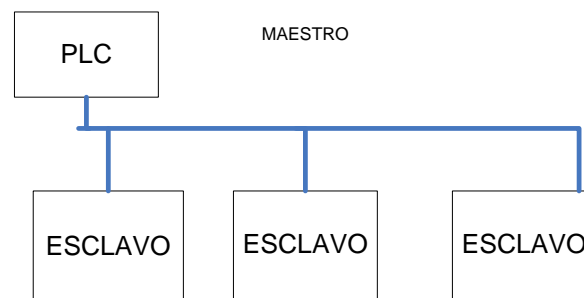


Fig. Nro: 6 Modelo Maestro-Esclavo

También hay que prestar mucha atención en la elección del **medio físico**, donde la mala elección afectará la velocidad de transmisión de datos, distancia entre nodos y la fiabilidad del sistema. En las redes de control se recurre a una mezcla de diferentes medios físicos, para poder cumplir con las necesidades de las diferentes secciones del sistema al menor costo posible. Se incorporan al sistema ruteadores, puentes o repetidores necesarios para asegurar el objetivo de una comunicación extremo a extremo transparente y sin que la integración disminuya las prestaciones.

Hay que tener presente el control de buenos tiempos de respuesta, que demandarán los sistemas (**control en tiempo real**), tomando como ejemplo el retardo entre la detección de un objeto en una línea de montaje de alta velocidad y el arranque de una máquina de pintado, que pueden ser del orden de decenas de milisegundos. En general las redes de datos no necesitan una respuesta en tiempo real cuando se envían grandes paquetes de datos a través de la red.

El control de acceso al medio y el número de capas implementadas en la arquitectura resultan determinantes a la hora de fijar la velocidad de respuesta de la red. Si se implementa un sistema con las siete capas del modelo OSI, demandará mayor potencia de proceso y por lo tanto mayor sobrecarga, comparándolo con un sistema simple que solamente posee 3 capas (física, enlace y aplicación). En ocasiones, los beneficios que aportan las capas adicionales compensan la sobrecarga adicional, sobre todo a medida que aumentan las demandas de la red y mejora la tecnología disponible. Cuando los **buses de campo** a utilizar requieren como parámetro esencial una velocidad mayor, el modelo puede aligerarse, ya que en ciertas aplicaciones las capas de red, transporte, sesión y presentación no son necesarias.



Fig. Nro: 7 Capas del modelo OSI/ISO.



Fig. Nro: 8 Modelo de 3 Capas

<u>TAREAS TIPICAS ASIGNADAS</u>		<u>REQUISITOS EN REDES DE CONTROL</u>
<u>APLICACION:</u>	<ul style="list-style-type: none"> - Semántica de usuario - Transferencia de ficheros 	<ul style="list-style-type: none"> - Objetos de datos - Estructuras estandarizadas de red
<u>PRESENTACION:</u>	<ul style="list-style-type: none"> - Compresión de datos - Conversión de datos de usuario 	<ul style="list-style-type: none"> - Estructuras de red - Interpretación de datos
<u>SESION:</u>	<ul style="list-style-type: none"> - Sincronización - Estructura de dialogo 	<ul style="list-style-type: none"> - Autenticación - Administración de red
<u>TRANSPORTE:</u>	<ul style="list-style-type: none"> - Transferencia de datos fiable - Comunicación extremo a extremo 	<ul style="list-style-type: none"> - Reconocimiento extremo a extremo - Detección de duplicados, reintento automático
<u>RED:</u>	<ul style="list-style-type: none"> - Direcciones lógicas, encaminamiento - Routers 	<ul style="list-style-type: none"> - Direccionamiento: unicast, multicast, broadcast - Routers
<u>ENLACE:</u>	<ul style="list-style-type: none"> - Mecanismos de acceso al medio - Corrección de errores y estructuración en tramas. 	<ul style="list-style-type: none"> - MAC, evitar/detectar colisión - Estructuración en tramas, codificación de datos - CRC, chequeo de errores.
<u>FISICA:</u>	<ul style="list-style-type: none"> - Definición del interface físico - Interface transceiver 	<ul style="list-style-type: none"> - Prioridad - Transceiver

Tabla Nro.2: Relación del modelo OSI con las redes de control

En la tabla Nro: 2, se observa las tareas típicas realizadas en cada capa del modelo OSI, y las correspondientes a las redes de control.

Otra forma de obtener tiempos de respuestas menores, es la capacidad para establecer mensajes con diferentes prioridades, de forma tal que mensajes como alarmas, tengan una mayor prioridad y facilidad de acceder al medio.

También hay que tener en cuenta, **la seguridad de la red**. Lo dividiremos en dos partes: **protección frente a los accesos no autorizados y protección frente a las fallas del sistema y averías**.

El primero es el, menos grave, ya que la mayoría de las redes de control no están conectadas a redes externas de la fabrica. Además en la práctica, la mayor parte de las veces, las redes pertenecientes a los niveles bajos de la pirámide CIM, no están conectadas con las redes de nivel superior dentro de la propia fábrica. En cualquier caso que se presentara, los mecanismos de protección son similares a los empleados en las redes de datos: claves de usuario y autenticación de los nodos de la red.

Hay que tener especialmente cuidado con la protección frente a fallas, ya que juega un papel muy importante, debido a que se debe evitar a todo costo, que esto afecte negativamente a la planta. Tomemos como ejemplo, los sistemas de refrigeración de una central nuclear, que no pueden bloquearse, porque una interfaz de comunicaciones de un nodo de la red quede fuera de servicio, por lo tanto es fundamental que los nodos puedan detectar si la red esta funcionando correctamente o no, y en caso de falla puedan acceder a un algoritmo de control que mantenga la planta segura.

Si el sistema a controlar es crítico, se deben incluir equipos redundantes, que reemplacen al averiado de forma completamente automática. Por lo tanto la **monitorización de la red** y la **capacidad de diagnóstico** representan dos puntos importantes a tener en cuenta en cualquier red de control.

También es de vital importancia tener en cuenta buenas **herramientas de mantenimiento, administración y puesta en marcha** de la red, no solo por lo dicho anteriormente sino, para poder aprovechar la mayor disponibilidad de datos, presentes en el sistema.

Hay que tener en cuenta, también la **generación de las señales eléctricas** de los datos a transmitir, y su posterior interpretación en el extremo receptor, luego de pasar por diversos sistemas de regeneración, como ser los repetidores de la red.

Tener especial cuidado en la **sincronización de las señales**, cuando empiezan a llegar a un dispositivo y su posterior finalización. De esta forma se permite realizar el establecimiento, el intercambio y la finalización de la comunicación.

Establecer un mecanismo que fragmente la información a transmitir y el orden de envío en el intercambio, para evitar los desbordamientos de paquetes de datos en ambos sentidos (**control de flujo**), incluyendo los tiempos de espera y turnos de transmisión.

REFERENCIAS BIBLIOGRAFICAS:

- **Pedro Morcillo Ruiz y Julián Cocerá Rueda.** “Comunicaciones Industriales” – Sistemas de Regulación y Control Automático. Editorial Paraninfo. (2004).
- **Ramón Piedrafita Moreno.** “Ingeniería de la Automatización Industrial”. 2da Edición Ampliada y Actualizada. Editorial Ra-Ma. (2004).
- **Emilio García Moreno.** “Automatización de Procesos Industriales”. Editorial Spupv. (1999).
- Siemens. “Comunicación Industrial para Automation and Drives”. Siemens AG. (2005).
- **Fabiana Ferreira.** “Seminario de Automatización”. Apuntes de la carrera de Ingeniería de Automatización Industrial de la Universidad Nacional de Quilmes. (2008)
- **Ing. Mariano López Figuerola.** Trabajo Integrador de: “Tecnologías de Telecomunicaciones aplicadas a transmisión de Datos de Procesos Industriales”. ITBA. (2007).
- **Cisco System.** Curso CCNA 4.0, Versión 3.1. Primer semestre. (2007).

REFERENCIAS DE FIGURAS:

- (1). Industrial Communication Automatización y comunicación a escala corporativa. Publicación Siemens. Abril 2008. Pág. 2 y 3.
- (2). Modelo CIM. Comunicaciones Industriales de Pedro Morcillo Ruiz. Editorial Paraninfo (Pág.8) (modificado).
- (3). Modelo jerárquico de comunicaciones para plantas complejas. Tomado de “Reference Model for Computer Integrated Manufacturing (CIM) Description from pointview of Industrial Automation” Purdue Research Foundation 1989.
- (4), (5), (6), (7) y (8). Cisco System. Curso del primer semestre CCNA 4.0. V.3.1 Cap.2

REFERENCIAS DE TABLAS:

Tabla Nro: 1 y 2. AAdeca. Seminario sobre “Comunicaciones Industriales”. (2007).

2. BUSES DE CAMPO

2.1 INTRODUCCION

Las Redes Industriales como fruto de la convergencia entre ordenadores y controladores, permiten el control distribuido de los sistemas de automatización. Todos los que intervienen en la supervisión y el control se comunican por el mismo medio (cable UTP, Fibra Óptica o la interfaz RS-485), a su vez los diferentes procesos de la planta se pueden supervisar y controlar utilizando aplicaciones como el SCADA, que utilizando una topología bus, admiten ramificaciones que pueden llegar hasta 2 Km., que es habitual hoy en día para este tipo de redes.

En los Niveles inferiores, los buses, representan el eslabón final entre los dispositivos de campo (sensores y actuadores) y los esquemas de control y de gestión de un sistema de fabricación integrado, por medio de comunicaciones industriales. Constituyen el nivel más simple y próximo al proceso dentro de la estructura de las comunicaciones industriales. Cada dispositivo de campo incorpora cierta capacidad de proceso, que lo convierte en un dispositivo inteligente, manteniendo siempre un costo bajo. Cada uno de estos elementos será capaz de ejecutar funciones simples de autodiagnóstico, control o mantenimiento, así como de comunicarse bidireccionalmente a través del bus.

El objetivo es reemplazar los sistemas de control centralizados, por redes de control distribuido, para mejorar la calidad del producto, reducir costos y mejorar la eficiencia. Para ello se basa en que la información que envían y reciben los dispositivos, es digital, lo que resulta más preciso que la información analógica del pasado. Además cada dispositivo de campo es inteligente y puede llevar a cabo funciones propias de control, mantenimiento y diagnóstico, de esta forma cada nodo de la red puede informar en caso de falla, y en general sobre cualquier anomalía asociada al dispositivo. Esta monitorización permite aumentar la eficiencia del sistema y reducir la cantidad de horas de mantenimiento.

2.2 BUSES DE CAMPO Y NIVELES OSI

Idealmente los buses de campo deberían cubrir los siete niveles OSI, pero en la realidad solo utilizan tres:

- **Nivel Físico:** Donde se especifica el tipo de conexión, naturaleza de la señal, tipo de medio de transmisión, etc. Normalmente las especificaciones de un determinado bus admiten más de un medio físico de comunicación.
- **Nivel de Enlace:** Especifica el protocolo de acceso al medio (MAC) y de enlace (LLC), define también los turnos de transmisión, el direccionamiento de las estaciones origen y destino de los datos y verificación de errores de las tramas.
- **Nivel de Aplicación, (Usuario):** Dirigido al usuario, que le permitirá ingresar al sistema de comunicaciones. Aquí se definen las funciones de las aplicaciones que se utilizarán para el envío de mensajes entre los dispositivos del bus, la comunicación entre sistemas de automatización y dispositivos de

campo. En este nivel se define el significado de los datos. Las aplicaciones suelen ser propias de cada fabricante. También permite la creación de programas de gestión y presentación, apoyándose en las funciones estándar definidas en el nivel de enlace.

2.2.1 NIVEL FISICO

Los buses industriales normalmente se comunican en banda base y codificación digital NRZ (Non Return to Zero), o Manchester. La señalización consiste en la transmisión diferencial de tensión de las variables físicas observadas. En el caso de comunicaciones serie sobre conductores eléctricos, las variables utilizadas son el resultado de la diferencia de potencial o de corriente entre los valores censados y uno de referencia. Normalmente la información a transmitir corresponde a la combinación de valores binarios “1” o “0”.

El medio físico por excelencia es el par trenzado, la fibra óptica se utilizará en aplicaciones que requieran alta inmunidad a las interferencias electromagnéticas. La comunicación en modo común (diferencia de potencial entre dos conductores y masa de referencia) se utilizara en enlaces no balanceados tipo RS-232 para cortas distancias, el cual resulta susceptible a las interferencias.

2.2.2 NIVEL DE ENLACE

La capa de enlace es la encargada de gestionar el envío de los paquetes de datos, al cual le agrega información redundante para el control de errores, que permitirá detectar y corregir el contenido de los paquetes mal recibidos en el receptor. En los buses de campo las tramas siguen formatos derivados del protocolo HDLC o similares. Como método de control y detección de errores se utilizan los códigos de redundancia cíclica (CRC) o la simple suma de comprobación de trama (Checksum). En los buses que utilizan comunicación asincrónica, cada palabra (byte), puede incluir un BIT de paridad que le permitirá el control de errores, además se incluye un CRC o checksum a nivel de trama.

Puesto que la mayoría de los buses industriales siguen una topología en bus, el control de acceso al medio es un tema importante, en el momento de elegir un bus industrial. Importante porque, a los requisitos de cualquier red de procesos de datos, se añaden requerimientos de tiempo real. Estos requisitos se traducen a una mayor necesidad de “determinismo”. Esto obliga a consideraciones adicionales, en los cuales podemos considerar los siguientes métodos de acceso al medio:

- Maestro-esclavo.
- Técnicas de Paso de Testigos.
- Técnica de CSMA/CD o variantes como ser CSMA/CA.
- Técnicas de división de tiempo (TDMA).
- Algoritmos de BIT dominante.

2.2.3 NIVEL DE APLICACIÓN

Debido a que no necesitan estructuras complejas, las capas de red, transporte, sesión y presentación no son consideradas, de esta forma se pasa directamente de la

capa de enlace de datos al nivel de **aplicación**. Pero también hay que tener en cuenta a veces que hay que realizar algún tipo de enrutamiento en la red, la gestión de envío de paquetes largos y consistentes de datos, el establecimiento de sesiones con un nodo o los cambios de presentaciones de datos, sin embargo esas características suelen incluirse como un aspecto de la especificación de la capa de aplicación y, en todo caso, se trata de reducirlas al máximo.

Por lo tanto un modelo OSI reducido (como se observa en la figura Nro: 1) a utilizar en los buses de campo estaría compuesto por: las capas físicas, de enlace de datos y de aplicación.

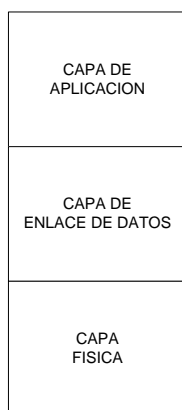


Fig. Nro: 1 Modelo OSI reducido

2.3 LA TECNOLOGIA DE LOS BUSES DE CAMPO

Físicamente podemos considerar a un bus como un conjunto de conductores conectando diferentes circuitos para permitir el intercambio de datos entre dispositivos. Es contrario a una conexión punto a punto donde solo dos dispositivos intercambian información. Un bus consta de un número de usuarios muy superior, que transmiten datos en forma serial. Para una transmisión serial se utiliza un número limitado de cables, generalmente tres conductores y la debida protección contra las perturbaciones e interferencias externas, que le permitirán su tendido en ambientes ruidosos.

2.4 BUSES PROPIETARIOS Y BUSES ABIERTOS

La existencia de un elevado número de buses diferentes se debe a que cada compañía venia utilizando un sistema propio para sus productos, pero en la actualidad se observa una tendencia a utilizar buses comunes.

Se pueden distinguir:

- **Buses Proprietarios:** Son propietarios de una cierta compañía, y para poder utilizarlos es necesario obtener una licencia.
- **Buses Abiertos:** Son todo lo contrario. Las especificaciones son públicas y disponibles a un precio razonable, sus componentes críticos también están disponibles como así también los procesos de validación y verificación.

2.5 CARACTERISTICAS

Las características fundamentales que los buses deben cumplir, en lo referente a la conexión de los diferentes dispositivos son las siguientes:

- **Interconectividad:** Deben poder conectarse de forma segura a dispositivos de diferentes fabricantes que cumplan con el protocolo.
- **Interoperatividad:** Los dispositivos de diferentes fabricantes deben funcionar en forma satisfactoria en el bus.
- **Intercambiabilidad:** Los dispositivos de un fabricante determinado, pueden ser sustituidos por otros equivalentes, de otros fabricantes y seguir funcionando normalmente.

2.6 VENTAJES Y DESVENTAJAS DE LOS BUSES

La principal ventaja que ofrecen los buses de campo, y la que los hace más atractivos a lo usuarios finales, es la reducción de costos de: instalación, mantenimiento y ahorros derivados de la mejora del funcionamiento del sistema.

Una de las principales características, es una significativa reducción en el cableado necesario para el control de una instalación. Cada célula de proceso sólo requiere un cable para la conexión de los diversos nodos. Se estima que puede ofrecer una reducción de 5 a 1 en los costos de cableado. En comparación con otros tipos de redes, dispone de herramientas de administración del bus que permiten la reducción del número de horas necesarias para la instalación y puesta en marcha.

El hecho de que los buses de campo sean más sencillos que otras redes de uso industrial, hace que las necesidades de mantenimiento de red sean menores, de modo que la fiabilidad del sistema a largo plazo aumenta, además permiten a los operadores monitorizar todos los dispositivos que integran el sistema e interpretar fácilmente las interacciones entre ellos, de esta forma la detección de la fuente de problemas en la planta y su corrección resulta mucho más sencilla, reduciendo los costos de mantenimiento y el tiempo de parada de la planta.

Ofrecen una mayor flexibilidad para el diseño de los sistema y su simplificación mejora las prestaciones y la adquisición de datos de los diferentes sensores distribuidos en toda la planta, además permiten comunicaciones bidireccionales entre los dispositivos de campo entre si y los sistemas de control.

Otra ventaja es que solo incluyen 3 capas (Física, Enlace y Aplicación), y un conjunto de servicios de administración. El operador solo necesita saber la funcionalidad, debe tener conocimiento de los servicios de administración de la red, ya que parte de la información generada, puede ser utilizada para la reparación de averías en el sistema.

Las desventajas que presenta el sistema de buses son mínima, y son las siguientes:

- Necesidad de conocimiento superior.
- Inversión en instrumentación y accesorios de diagnóstico.

- Costos globales iniciales grandes.

VENTAJAS	DESVENTAJAS
- Ahorro en cableado o instalación inicial.	- El total de dispositivos es más caro.
- Integración de la información.	- Más variables a controlar.
- Más flexible.	- Precisa de información añadida
- Fácil de modificar	- Proyecto más elaborado

Tabla Nro: 1 Ventajas y desventajas de los buses de campo

2.7 BUSES DE CAMPO EXISTENTES

Debido a la falta de estándares, cada empresa ha desarrollado diferentes soluciones, orientadas a diversos campos de aplicación y prestaciones, las cuales se podrían dividir en los siguientes grupos:

2.7.1 BUSES DE ALTA VELOCIDAD Y BAJA FUNCIONALIDAD

Estos fueron desarrollados para poder integrar dispositivos simples como ser: finales de carrera, fotocélulas, relés y actuadores, funcionando en tiempo real, y ubicados en la zona de proceso a nivel de maquina. Trabajan en la capa física y de enlace de datos del modelo OSI, manejando señales de patrones de BIT de las tramas. Algunos ejemplos pueden ser:

- **ASI:** Bus serie diseñado por la empresa Siemens para la integración a nivel de proceso (maquina), de sensores y actuadores.
- **CAN:** Bus utilizado originalmente, en aplicaciones sobre vehículos.
- **SDS:** Utilizado para la integración de sensores y actuadores, basado en el bus CAN.

2.7.2 BUSES DE ALTA VELOCIDAD Y FUNCIONALIDAD MEDIA

Basados en el diseño de una capa de enlace que permite un envío eficiente de tramas de datos de tamaño medio. Esto permite que el dispositivo posea mayor funcionalidad como ser: la configuración, calibración o la programación del mismo. Pudiendo controlar dispositivos de campo complejos en forma muy eficiente y a bajo costo. Estos buses incluyen, la especificación completa de la capa de aplicación, permitiéndole disponer de funciones, que pueden ser accedidas, cambiadas y controladas desde una PC, pudiendo variar la condición de los diversos dispositivos del sistema. Algunos incluyen funciones estándar para distintos tipos de dispositivos (perfiles), que facilitan la interoperabilidad de diferentes sensores y actuadores de diferentes fabricantes. Algunos ejemplos pueden ser:

- **DeviceNet:** Bus desarrollado por la empresa Allen-Bradley, utiliza como base el bus CAN, e incorpora una capa de aplicación orientada a objetos.
- **LONWorks:** Es una red desarrollado por INTEL.
- **DIN MessBus:** Bus alemán utilizado en instrumentación, basado en el protocolo RS- 232.
- **InterGus-S:** Bus de origen alemán, utilizado en aplicaciones medias.

2.7.3 BUSES DE ALTAS PRESTACIONES

Estos buses son capaces de soportar comunicaciones a nivel de fábrica, y son utilizados en diversas aplicaciones. Son buses de alta velocidad, pero algunos presentan problemas de sobrecarga, cuando son exigidos para que cumplan con diversas funciones operativas y de seguridad. La capa de aplicación de estos buses oferta numerosos servicios a los usuarios y poseen las siguientes características:

- Redes multimaestro con redundancia.
- Comunicaciones maestro-esclavo, según el esquema pregunta -respuesta.
- Altos niveles de seguridad de la red, con procedimientos de autenticación.
- Conjunto completo de funciones de administración de la red.
- Petición de servicios a los esclavos, basado en eventos.
- Capacidad de direccionamiento unicast, multicast y broadcast.
- Recuperación de datos desde el esclavo, con un límite máximo de tiempo.
- Descarga y ejecución remota de programas.
- Comunicación de variables y bloques de datos orientado a objetos.

Algunos ejemplos pueden ser:

- **Profibus.**
- **Fip.**
- **Fieldbus Foundation.**
- **Profinet**

2.7.4 BUSES PARA AREAS DE SEGURIDAD INTRINSECA

A estos buses se le modifico la capa física para que puedan cumplir con los requisitos específicos de seguridad intrínseca en ambientes con atmósferas explosivas. Esta seguridad brinda protección, de tal forma que el dispositivo no tiene ninguna posibilidad de provocar una explosión en la atmósfera circundante.

Por ejemplo los circuitos eléctricos tienen este tipo de seguridad, debido que cuando se produce una falla, por deficiencia en sus especificaciones o falla del material, no produzcan chispas o efectos térmicos, que puedan provocar una ignición.

Algunos ejemplos, pueden ser:

- **Hart.**
- **Profibus PA.**
- **Fip.**

2.8 FUNCIONALIDAD DE ALGUNOS BUSES ESTANDARIZADOS

2.8.1 CRITERIOS DE ELECCION

Los siguientes criterios, se tienen que tener en cuenta en la elección de un bus de campo:

-
- Costo del hardware del nodo.
 - Costo de desarrollo.
 - Tiempo de respuesta y flujo máximo de datos.
 - Características de tiempo real.
 - Fiabilidad.
 - Recuperación ante fallas. Funcionamiento en condiciones extremas.
 - Medios físicos que permite (par trenzado, UTP, fibra óptica, infrarrojos, WI-FI, etc.).
 - Capacidad para el funcionamiento multimaster, cliente-servidor o maestro-esclavo.
 - Topologías permitidas (bus, estrella, anillo, etc.).
 - Servicios de gestión de red, flexibilidad para la configuración de dominios y grupos.
 - Interfaces de programación (API). Disponible para el desarrollo de aplicaciones.
 - Normalización. Soporte a usuarios.

Estos, y otros posibles criterios deben ser ponderados en la elección de un bus, de acuerdo a la aplicación y a los sensores y actuadores a utilizar en la red industrial.

2.9 BUS ASI

2.9.1 INTRODUCCIÓN

AS-Interface o AS-i (Actuator-Sensor Interface --- EN 50295 - IEC 62026), fue diseñado en 1990 como una alternativa económica al cableado tradicional. El Objetivo fundamental fue determinar un sistema de comunicación único para todos los fabricantes de sensores y actuadores.

La idea original fue crear una red simple para sensores y actuadores binarios, capaz de transmitir datos y alimentación a través del mismo bus, manteniendo una gran variedad de topologías que faciliten la instalación de los sensores y actuadores en cualquier punto del proceso con el menor esfuerzo posible y que cumpliera con las normativas de seguridad.

Desde entonces, el concepto AS-Interface se ha extendido considerablemente y las especificaciones iniciales se han revisado para adaptar el bus a las nuevas circunstancias y necesidades del mercado.

Las especificaciones de AS-i se encuentran actualmente en su versión 3.0, y son de carácter abierto, lo que significa que cualquier fabricante puede obtener una copia de las mismas para elaborar sus productos conforme a dicho estándar.

La representación siguiente muestra la ubicación básica de una red AS-Interface o AS-i en el campo de automatización, en una empresa moderna, que utiliza el concepto CIM, para su comunicación.

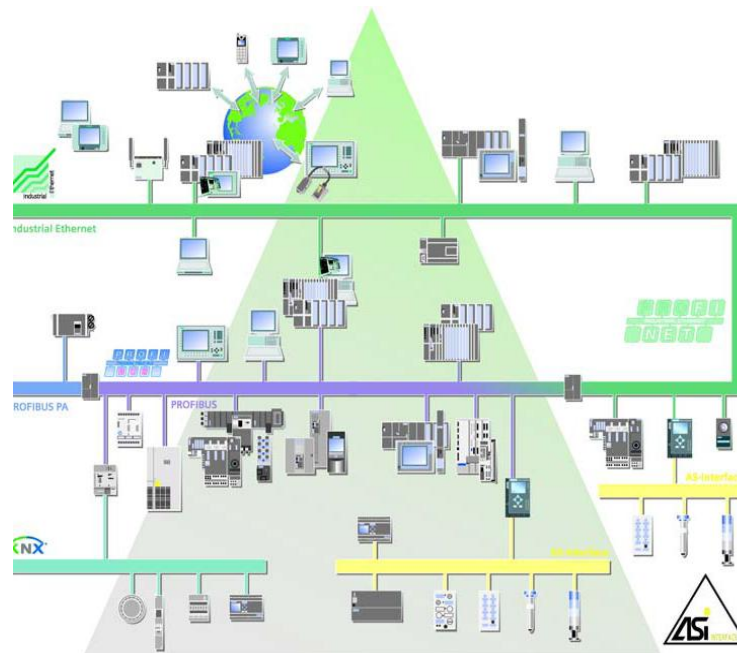


Fig. Nro: 2 Bus AS-i, en una Red Industrial (Manual Siemens C79000-G8778-04-2006)

2.9.2 CARACTERISTICAS PRINCIPALES DEL BUS

El bus se ubica en la parte inferior de la pirámide CIM, conectando los sensores y actuadores con el maestro del nivel de campo. Los maestros pueden ser autómatas o PCs situados en los niveles bajos de control, o pasarelas que comunican la red AS-Interface con otras redes de nivel superior, como Profibus o DeviceNet. AS-Interface supone un ahorro considerable en la instalación, planificación y en el mantenimiento de máquinas e instalaciones, principalmente en los costos relacionados con los tiempos de cableado. La eliminación del mazo de cables facilita la inspección de la instalación y el mantenimiento se facilita, ya que el maestro detecta fallas en los esclavos y defectos de alimentación. También se reduce el riesgo de incendio por la utilización de un único cable de alimentación, y se ahorra espacio en los armarios por la eliminación de gran cantidad de módulos de E/S y sus cables asociados.

2.9.3 OTRAS CARACTERISTICAS IMPORTANTES

- Acepta hasta 124 sensores y actuadores digitales.
- Con direccionamiento ampliado puede manejar hasta 248 sensores y actuadores.
- Con el nuevo perfil de la versión 3.0, se le pueden conectar hasta 496 entradas y salidas digitales.
- Detección de errores, en la transmisión y supervisión del correcto funcionamiento de los esclavos por parte del maestro de la red.
- Grado de protección IP-65/67, para ambientes exigentes.

2.9.4 RELACION CON EL MODELO OSI

Como está definido su uso en el nivel de sensores y actuadores, el bus se implementa a nivel de capa física y de enlace de datos, implementando además una capa de aplicación sencilla y limitada.

2.9.5 CAPA FISICA

Es el nivel de los medios, como se muestra en la Figura Nro: 3, donde se utilizan cables bifilares, sin apantallamiento y sin trenzar, como así también varios cables auxiliares para alimentación y uso en ambientes hostiles, con protección IP65/67.



Fig. Nro: 3 Cable bifilar AS-i. ⁽³⁾

Este nivel posee dos tipos de módulos, que se conectan a la red AS-I, los **módulos activos**, que tienen una dirección de red, para permitir su direccionamiento, extendido o estándar, utilizando para ello 3 o 4 BIT, que permiten conectar sensores y actuadores estándar, y los **módulos pasivos**, que no poseen electrónica integrada, con lo cual no poseen dirección de red, ya que serán los dispositivos conectados a él, que si la posean.

2.9.5.1 MODULACION DE LA SEÑAL

Se utiliza modulación por amplitud de pulso (PAM), para transmitir las diferentes señales de los maestros hacia los esclavos, y viceversa, la principal ventaja de este tipo de transmisión es su alta inmunidad al ruido y su facilidad de adaptación a los distintos ambientes de trabajo.

Este tipo de modulación hace variar la amplitud del pulso en función de los datos recibidos, manteniendo el ancho del pulso y su posición constante, de acuerdo con la amplitud de la señal.

Esta técnica de modulación junto con:

- las características eléctricas de los cables de transmisión,
- las topologías de red soportadas,
- La distancia máxima de transmisión.

Hacen que la duración de cada BIT pueda ser, a lo sumo de 6 microsegundos. Por lo tanto la velocidad de transmisión de información en la red de campo AS-i es de 167 Kbits/segundo.

En la Figura Nro: 4, se observa el proceso de modulación de la señal AS-i con su correspondiente codificación en el transmisor y su desmodulación en el receptor.

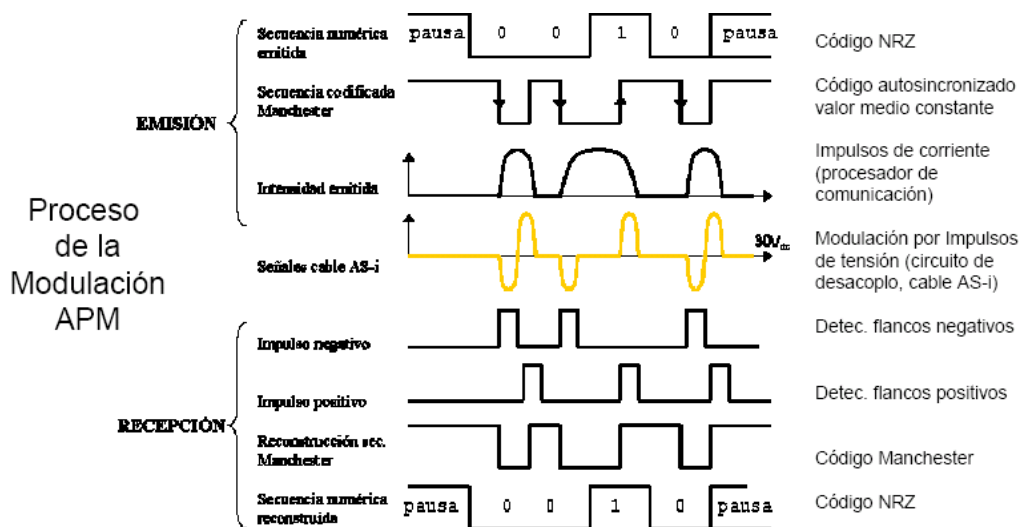


Fig. Nro: 4 Proceso de modulación de la señal AS-i⁽⁴⁾

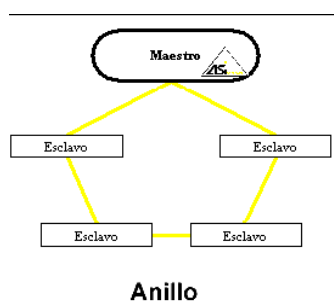
2.9.6 CAPA DE ENLACE DE DATOS

El bus AS-i es una red monomaestro que funciona mediante polling cíclico, quiere decir que hay un solo maestro que direcciona uno a uno a los esclavos y realiza la comunicación con ellos. El maestro de la red puede establecer con un esclavo una comunicación no cíclica, para poder adaptar su configuración en el arranque. Este tipo de redes es de difusión, por lo tanto en cada trama, tiene que colocarse la dirección del esclavo con el cual se establecerá la comunicación. El mensaje que envía el maestro hacia sus esclavos, esta compuesto por los datos o la función que debe realizar y es devuelto por estos con los datos solicitados por el maestro.

Debido al principio de funcionamiento que emplea el bus, se pueden utilizar las siguientes topologías:

- Bus
- Estrella
- Anillo
- Rama
- Árbol

Como se observa en la Figura Nro: 5, se pueden usar, variedades de topologías, que permite a los esclavos, conectarse al punto más cercano a la red, o al más accesible, facilitando su instalación. Para poder realizar ramificaciones o bifurcaciones en la red se deben emplear los módulos pasivos, ya que estos permiten mantener la protección y la seguridad de la red, utilizando el protocolo IP65.



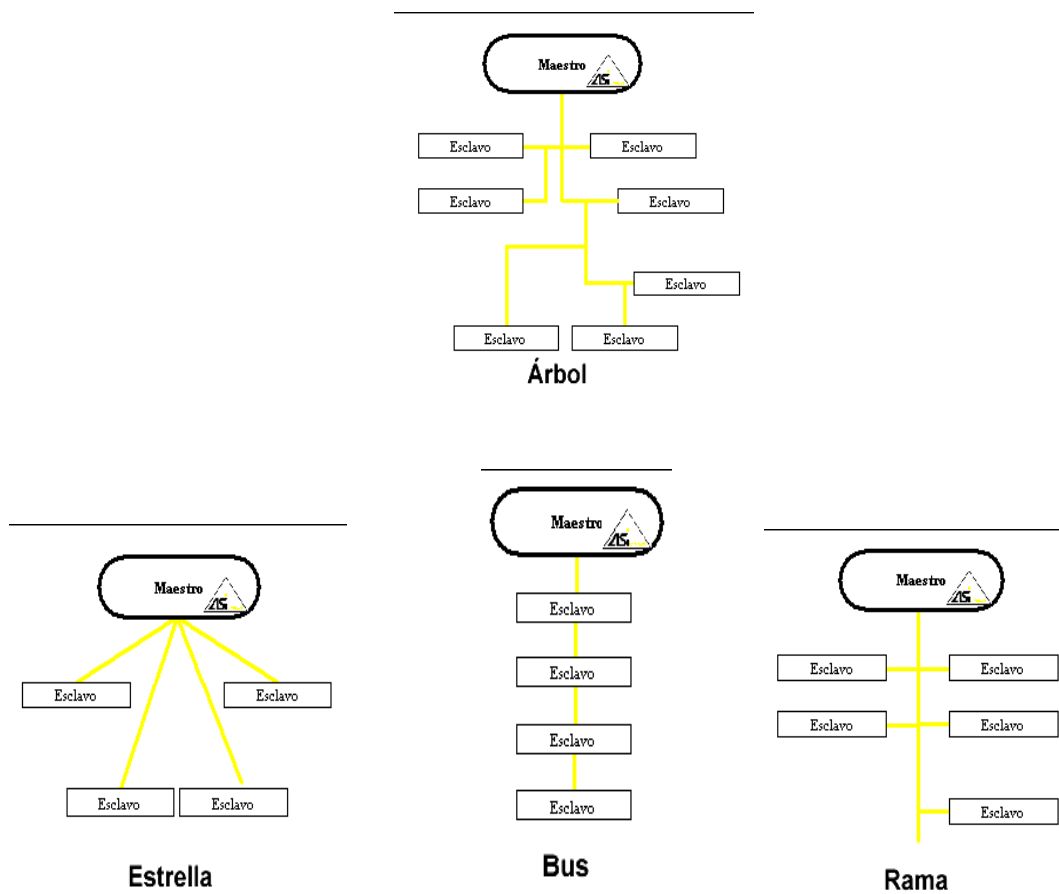


Fig. Nro: 5 Topologías a emplear en una red AS-i⁽⁵⁾

2.9.6.1 CONTROL DE ACCESO AL MEDIO

El esquema de comunicación empleado es maestro/esclavo, donde el maestro (el procesador principal), se comunica con los esclavos presentes en la red.

El proceso de comunicaciones es: (como se observa en la Figura Nro: 6), el maestro consulta en forma cíclica y por turno a todos los nodos subordinados, de esta forma recibe en cada ciclo el estado de cada uno de ellos y actualiza la información de los actuadores conectados, esto es llevado a cabo por el pasaje de mensajes entre el maestro y los esclavos. Sólo se puede transmitir un comando de control por ciclo.

Normalmente el maestro AS-i, gestiona las siguientes etapas principales:

- Inicialización
- Arranque
- Intercambios

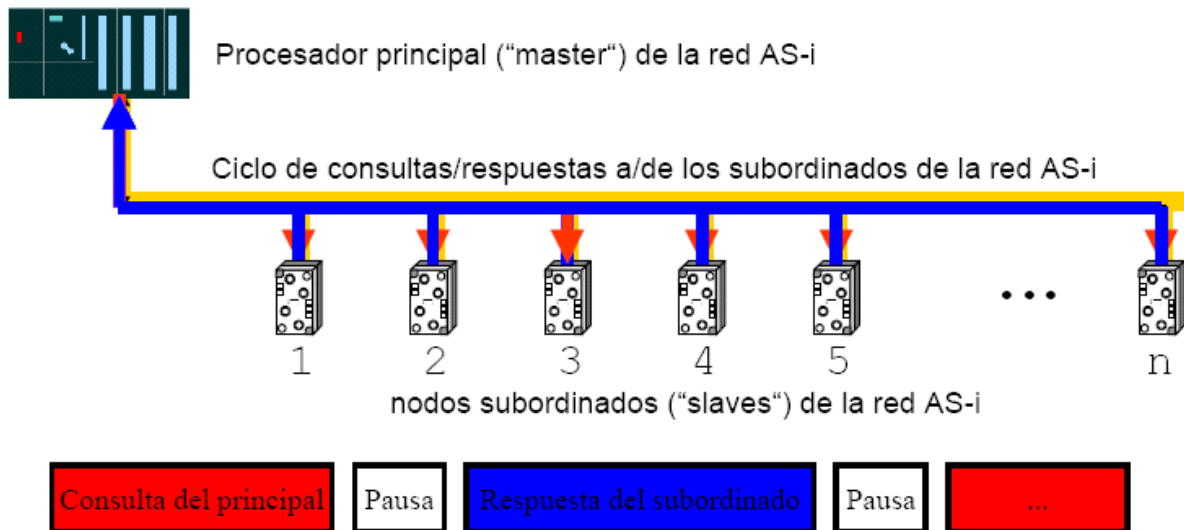


Fig. Nro: 6 Consulta Cíclica ⁽⁶⁾

El proceso de comunicación se lleva a cabo mediante el intercambio de información entre el procesador de comunicaciones principal y cada uno de los subordinados a través de mensajes con la siguiente estructura:

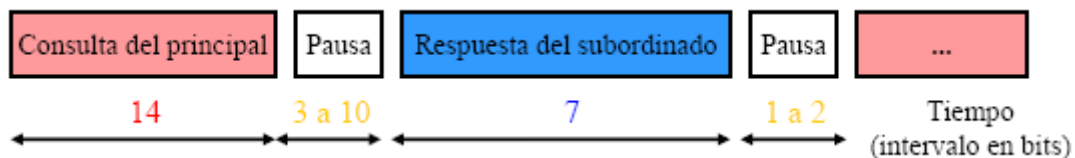


Fig. Nro: 7 Formato del mensaje AS-i ⁽⁷⁾

La unidad de tiempo para el envío de un BIT de información es de 6 μs . Por lo tanto, el tiempo dedicado por lo general a una transacción de información con un módulo subordinado del sistema es de:

$$(14 + 4 + 7 + 1) * 6 \mu\text{s} = 26 * 6 \mu\text{s} = 156 \mu\text{s}$$

2.9.7 CAPA DE APLICACIÓN

Esta capa esta formada por un conjunto de tablas de información compartida, para ello utiliza una memoria de accesos aleatorio doble –“Dual Port RAM”, entre el microprocesador de comunicaciones principal y el sistema de control. En ella se encuentran 4 tipos diferentes de tablas de acuerdo a la norma AS-i:

- 1- Tablas de los datos de usuarios (User Data).
- 2- Tablas de datos de configuración (Configuration Data).
- 3- Tablas de datos de configuración permanente (Permanent Config. Data).
- 4- Tabla de indicadores de estado AS-i (AS-i flags).

2.10 BUS DEVICENET:

Este bus es un enlace de comunicaciones de bajo costo, puede conectar diversos dispositivos industriales, evitando costosas y complejas instalaciones cableadas. Posee una conectividad directa que provee una mejor comunicación entre los dispositivos, y puede realizar un eficaz diagnóstico del sistema, durante una falla. DeviceNet es una red abierta, basada en el protocolo CAN (Controller Area Network), utilizado en automóviles, los protocolos y las especificaciones son abiertas, lo que permite a otros fabricantes utilizarlo en sus productos permitiéndoles conectar sus dispositivos al sistema.

Utilizado principalmente en la conexión de controladores industriales y dispositivos de entrada/salida (I/O), el protocolo sigue el modelo productor-consumidor, soporta múltiples modos de comunicación y posee prioridad entre mensajes. Es un sistema que puede ser configurado para operar tanto en una arquitectura maestro-esclavo o en una arquitectura distribuida punto a punto. Además de esto, define dos tipos de mensajes, I/O (datos de proceso) y explicit (configuración y parametrización). Tiene también mecanismos de detección de direcciones duplicadas y aislamiento de los nodos en caso de falla críticas. Una red DeviceNet puede contener hasta 64 dispositivos, direccionados de 0 a 63, donde un nodo es utilizado por el scanner maestro y el nodo 63 es reservado como el nodo por defecto, este número de nodos se puede ampliar, debido que la mayoría de los controladores industriales permiten conectarse a múltiples redes DeviceNet.

2.10.1 RELACION CON EL MODELO OSI

Se basa en el modelo OSI de 7 capas. En la capa de enlace utiliza el protocolo CAN, que es un protocolo orientado a mensajes, y en las capas superiores del modelo el protocolo CIP (Common Industrial Protocol), orientado a objetos.

Utiliza direccionamiento Punto a Punto con Multi-Punto, Multi-Maestro y Maestro-Esclavo y cambio de estado basado en eventos ocurridos en el sistema.

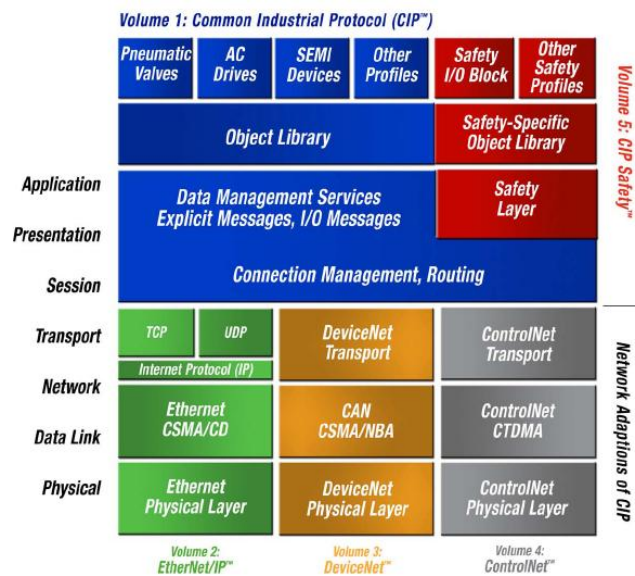


Fig. Nro: 8 Definición del modelo OSI para DeviceNet ⁽⁸⁾

2.10.1.1 CAPA FÍSICA

Utiliza una topología de red tipo árbol, que le permiten que la señal de datos y la alimentación de los diferentes componentes circulen por el mismo cable. La extensión de la red varía de acuerdo a la tasa de transmisión de datos, según la siguiente tabla:

TASA DE TRANSMISION	TAMAÑO DE LA RED	DERIVACION	
		MAXIMO	TOTAL
125 kbps	500 m	6m	156 m
250 kbps	250m		78 m
500 kbps	100 m		39 m

TABLA NRO: 2 Extensión de la red x tasa de transmisión

Se recomienda para evitar reflexiones en la red, utilizar resistores de terminación, en sus extremos, pues si no se los colocan pueden producir errores en la transmisión de los datos, también utilizan conectores especiales (taps) en las derivaciones.

2.10.1.2 CAPA DE ENLACE

Esta capa esta definida por la especificación CAN, la cual define dos estados posibles, “0” dominante y “1” recesivo. Cualquier nodo que quiera enviar información, colocara la red en estado dominante, caso contrario estará en estado recesivo.

El método de acceso al medio es CSMA/NBA (Acceso múltiple por detección de portadora/ Arbitraje de BIT no destructivo), significa que un nodo antes de transmitir escucha si hay alguna transmisión presente, y si el canal esta libre comienza a transmitir. En el caso que dos nodos transmitan al mismo tiempo, se le da prioridad al que tenga el identificador más bajo, el mecanismo es no destructivo, o sea el mensaje es preservado, aunque ocurra colisiones entre dos o más mensajes, el nodo a medida que esta transmitiendo se escucha a si mismo para verificar y detectar errores.

El protocolo CAN que define esta capa, tiene cuatro tipos distintos de mensajes (data, remote, overload, error). DeviceNet solamente utiliza: trama de datos (data frame) y la trama de errores (error frame). Los datos son intercambiados utilizando la trama de datos. La estructura típica de la trama es representada en la siguiente figura:

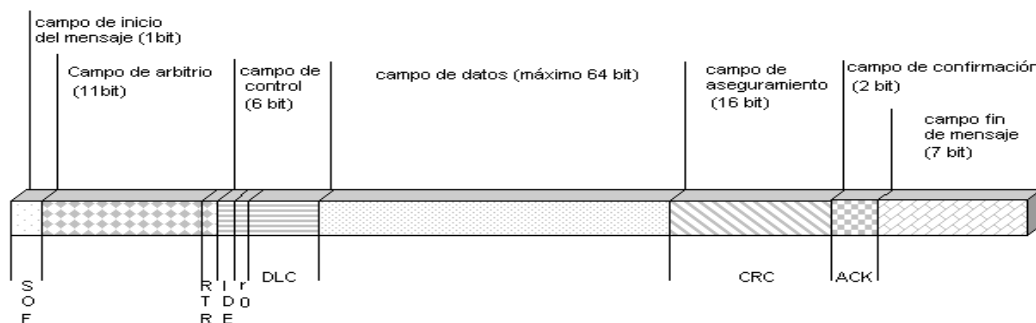


Fig. Nro: 9 Trama de datos CAN ⁽⁹⁾

La topología que soporta es “trunk-line/drop-line, que significa que los nodos pueden conectarse directamente a la línea principal o mediante derivaciones cortas (6 metros de longitud máxima). Cada nodo se identifica a través del identificador de 11 BIT.

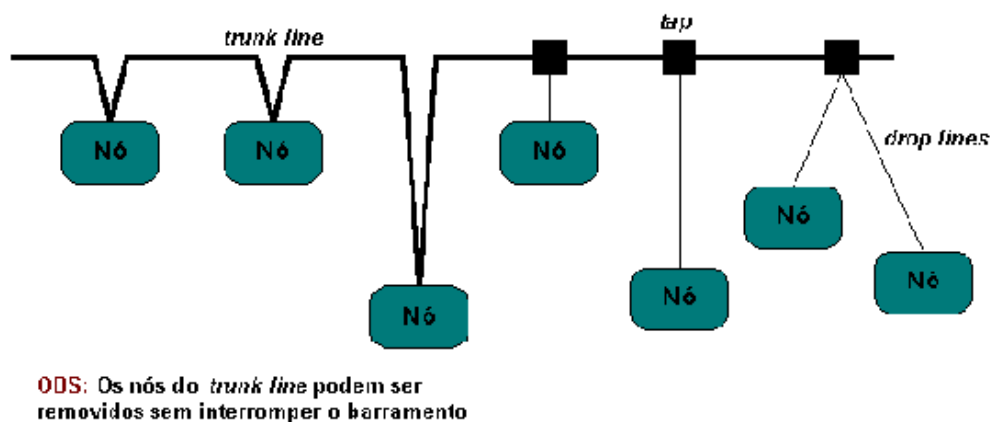


Fig. Nro: 10 Topología lineal “trunk-line/drop-line”⁽¹⁰⁾

2.10.1.3 CAPA DE RED Y DE TRANSPORTE

DeviceNet, necesita que este establecida la comunicación antes del intercambio de datos entre dispositivos, para establecer la comunicación cada nodo debe implementar (UCMMO) Unconnected Message Manager o el Group 2 Unconnected Port, estos mecanismos utilizan mensajes de tipo explicit o I/O para poder establecer la conexión, antes de la transmisión de los datos entre nodos.

Los mensajes son clasificados en grupos, que definen funciones y prioridades específicas, utilizando el campo identificador (11 bit), de la trama de datos CAN para identificarlos, garantizando así, el mecanismo de prioridades.

DeviceNet emplea fundamentalmente un modelo de mensajes punto a punto, pero los nodos pueden actuar como cliente, servidor o ambos, y a su vez pueden ser productores y consumidores de mensajes, o sea que el protocolo prevé diversas posibilidades de conexión entre los dispositivos. También dispone de recursos de detección de nodos con dirección (MAC IDE) duplicada.

2.10.1.4 CAPA DE SESION

Esta capa lleva el control de las conexiones abiertas y se encarga de enrutar los datos, en la trama se colocan los siguientes datos: MAC IDE, del nodo de donde se encuentra el objeto, el numero de clase e instancia y el servicio requerido, de tal forma que la capa inferior pueda realizar el ruteo.

2.10.1.5 CAPA DE PRESENTACION:

Se encarga de la traducción, de los datos introducidos por el usuario (aplicación) en un formato común para que puedan ser interpretados por las capas inferiores.

2.10.1.6 CAPA DE APLICACIÓN

DeviceNet utiliza en esta capa CIP (Common Industrial Protocol), este es un protocolo estrictamente orientado a objetos, utilizado también por ControlNet y por EtherNET/IP, o sea que es independiente del medio físico y de la capa de enlace de datos, de acuerdo a lo mostrado en la Figura Nro: 8.

El protocolo CIP tiene dos objetivos principales:

- Transporte de datos de control de los dispositivos de I/O
- Transporte de información de configuración y de diagnóstico del sistema que esta siendo controlado.

El nodo (maestro/esclavo), es modelado por un conjunto de objetos CIP, los cuales determinan su comportamiento, en función de los datos y servicios encapsulados, en las tramas respectivas.

2.11 BUS PROFIBUS

Profibus, es el numero uno de los buses de campo a nivel internacional, este bus permite la comunicación de proceso y de campo en redes de célula con pocas estaciones y para la comunicación de datos según la norma: 61158/EN 50170. Puede aplicarse en las siguientes áreas:

- Automatización manufacturera
- Automatización de procesos
- Automatización de edificios

Este potente y robusto bus de campo abierto, ofrece breves tiempos de reacción, y esta disponible para las aplicaciones más diversas.

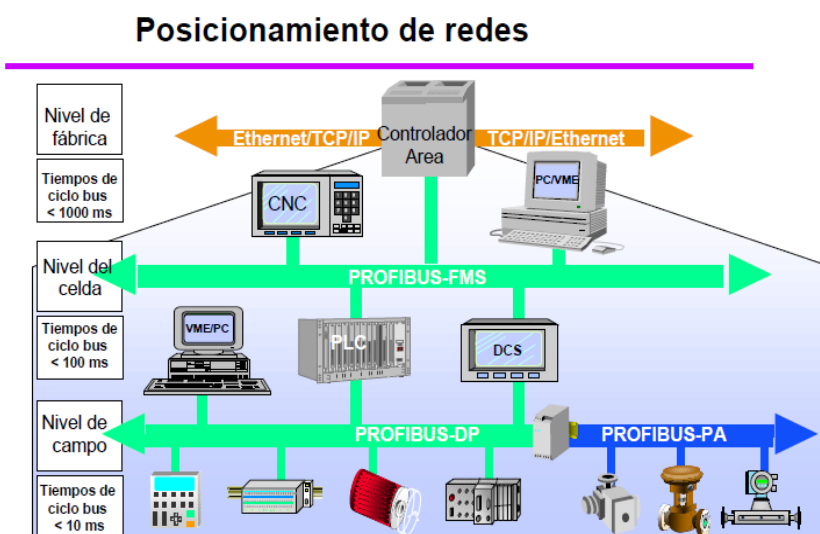


Fig. Nro: 11 Redes PROFIBUS ⁽¹¹⁾

Como se observa en la Figura, de acuerdo a los posibles sectores de aplicación se divide en:

- **PROFIBUS DP:** Sirve para conectar dispositivos de campo descentralizados con muy cortos tiempos de reacción, se aplica tanto a una maquina o a una instalación. En esta solución los actuadores y sensores se conectan directamente a los dispositivos de campo, utilizando el modelo maestro/esclavo para transmitir y recibir datos de los PLC o computadoras asociadas.
- **PROFIBUS PA:** Utilizado en aplicaciones de automatización de procesos en zonas que exigen seguridad intrínseca, ampliando las funciones de PROFIBUS DP, con respecto a la transmisión de datos y energía por el mismo conductor, de acuerdo a las normas internacionales IEC61158-2.
- **PROFIBUS FMS:** Utilizado para comunicación de datos entre dispositivos de automatización y aparatos de campo, permite la comunicación de datos con equipos de automatización de diversos fabricantes, permitiendo resolver de forma precisa y distribuida no solo tareas de control de movimiento sino también tareas generales de regulación y medición.

2.11.1 CARACTERISTICAS DE COMUNICACIÓN

En los sistemas PROFIBUS se diferencian dos tipos de estaciones, Maestros y Esclavos. Los maestros determinan la comunicación de datos a través del bus, enviando mensajes sin necesidad de recibir una petición externa para poder controlar el medio, se denominan estaciones activas.

Los esclavos o dispositivos periféricos, incluyen a los dispositivos de entrada/salida, válvulas, accionadores o dispositivos de medida, no tienen capacidad de acceder directamente al bus y solo pueden enviar acuses de recibo de mensajes enviados por los maestros, o contestar sus peticiones de datos, denominándose estaciones pasivas.

2.11.2 ARQUITECTURA DE PROTOCOLOS:

Este bus esta basado en normas internacionales reconocidas, su arquitectura protocolar esta orientada al sistema OSI de acuerdo a la norma internacional SO 7498, y utiliza para la transmisión de datos y proceso las capas física, enlace de datos y de aplicación.

2.11.3 RELACION CON EL MODELO OSI:

PROFIBUS DP, define la capa física y la de enlace, así como la interfaz de usuario. Las capa 3 a 7 no están definidas. El **DDL**M (Direct Data Link Mapper) proporciona una interfaz de usuario, sencillo para el acceso a la capa 2. Como medio físico se utiliza la tecnología RS-485, fibra óptica o ambas.

PROFIBUS FMS, define la capa física, de enlace y la de aplicación. La capa de aplicación consiste en **FMS** (Fielbus Message Specification) y el **LLI** (Lower Layer Interface). **FMS** contiene el protocolo de aplicación y proporciona al usuario un amplio conjunto de servicios y **LLI** proporciona una interfaz independiente a **FMS** del

dispositivo con la capa de enlace. Dicha capa implementa el protocolo de acceso al bus y la seguridad de datos. Como medio físico se emplea RS-485, fibra óptica o ambos.

PROFIBUS PA, utiliza el protocolo **PROFIBUS-DP** y le añade como característica particular la definición de los perfiles de los dispositivos. Como medio de transmisión utiliza el estándar IEC 1158-2, lo que permite su utilización en zonas de seguridad intrínseca. Mediante un puente es posible acoplar las redes PROFIBUS DP con las redes PROFIBUS PA.

2.11.4 CONTROL DE ACCESO AL MEDIO

Las tres versiones de PROFIBUS usan el mismo control de acceso al medio, incluyendo los aspectos relacionados con la seguridad de los datos y el manejo de los protocolos de transmisión y los telegramas. Esta capa 2, se denomina FDL (Fieldbus Data Link). La dirección de acceso al medio (MAC) es determinista, de modo que solamente una estación tiene derecho de transmitir en cada momento. Esta capa ha sido diseñada para cumplir dos objetivos fundamentales:

- En las comunicaciones entre maestros activos, en las tareas de control, se debe asegurar que cada estación tenga suficiente tiempo para ejecutar sus tareas de comunicación dentro de un intervalo de tiempo definido.
- Las comunicaciones cíclicas se implementaran de la forma más sencilla posible, para poder comunicar a cada maestro con uno o varios esclavos.

Como se observa en la Figura, el control de acceso al medio, incluye un sistema de paso de testigo en bus (Token Bus), entre los maestros, junto con un sistema de consulta maestro-esclavo, para la comunicación entre cada maestro y su periferia. Este mecanismo, garantiza el derecho de acceder al bus de cada maestro durante un determinado periodo de tiempo. El Token es un telegrama especial que permite la cesión al nodo que lo recibe, para poder acceder al bus y poder contactarse con su maestro, a su vez el maestro que posee el token le permite enviar mensajes a sus esclavos y leer las contestaciones de estos, de esta forma es posible tener un sistema con un único maestro y múltiples esclavos, un sistema formado solo por estaciones activas o un sistema híbrido.

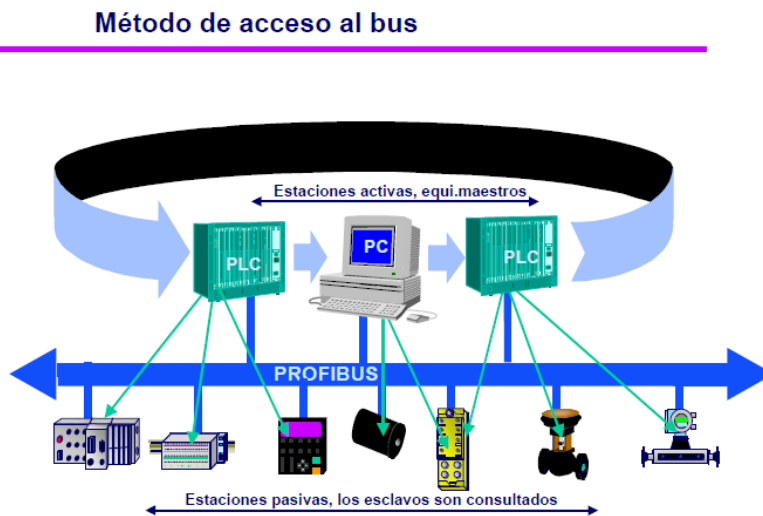


Fig. Nro: 12 Acceso al Medio ⁽¹²⁾

Esta capa también es la encargada de la seguridad de los datos, todos los telegramas tienen distancia Hamming 4, debido al uso de delimitadores de comienzo y fin de trama especial, así como un BIT de paridad para cada byte según se define en el estándar IEC 870-5-1.

El tipo de funcionamiento es sin conexión, por lo tanto permite direccionamiento unicast, multicast y broadcast.

2.11.5 CAPA DE APLICACIÓN:

El protocolo PROFIBUS establece las reglas de comunicación desde el nivel de enlace de datos hasta el nivel de aplicación, que permiten a los usuarios entrar en el sistema de comunicaciones. En esta capa se definen las funciones de las aplicaciones que se utilizarán, para confeccionar los mensajes entre los dispositivos del bus, la comunicación entre los sistemas de automatización y los dispositivos de campo. En FMS el protocolo de aplicación ofrece al usuario un grupo de servicios de comunicaciones amplio y potente. El protocolo LLI (Lower Layer Interface, interfase para el nivel inferior), permite a las aplicaciones acceder al nivel de enlace FDL (Fieldbus Data Link), del nivel de enlace de datos.

En el caso de PROFIBUS DP, las funciones de aplicación disponible para el usuario, se especifican en la interfaz de usuario (no especificada en el modelo OSI de 7 niveles), enlazándose directamente con la capa de enlace por medio de DDLM.

En la Figura se observa la relación de las distintas aplicaciones de Profibus con el modelo OSI.

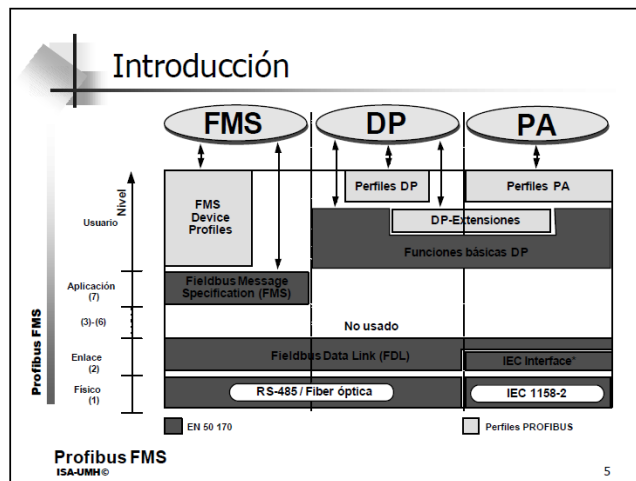


Fig. Nro: 13 Bus PROFIBUS (13)

2.11.6 TOPOLOGIAS

Las topologías empleadas, para la comunicación entre los maestros y los esclavos son:

Transmisión RS-485:

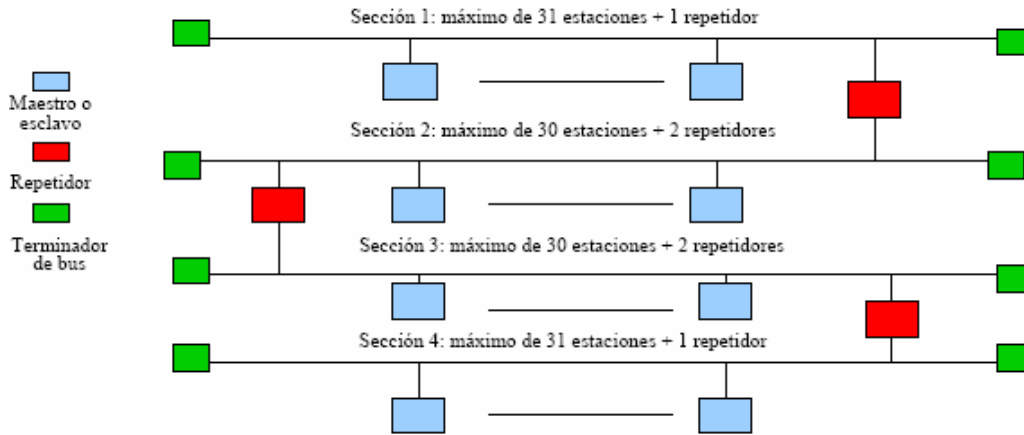
- **LINEAL:** Formado por varios segmentos y terminadores activos en ambos extremos.

- **ARBOL:** permite más de tres repetidores. Las ramas derivadas solo se permiten para velocidades menores de 1,5 Mbps.

Fibra Óptica:

- Es la opción para grandes distancias de transmisión o para ambientes industriales ruidosos y afectados con interferencias electromagnéticas. Permite topologías tipo bus, lineal, anillo y estrella.

⇒ LINEAL (3 repetidores y 122 estaciones, config. máx.)



⇒ ÁRBOL (127 estaciones, nº máx, y 5 > 3 repetidores)

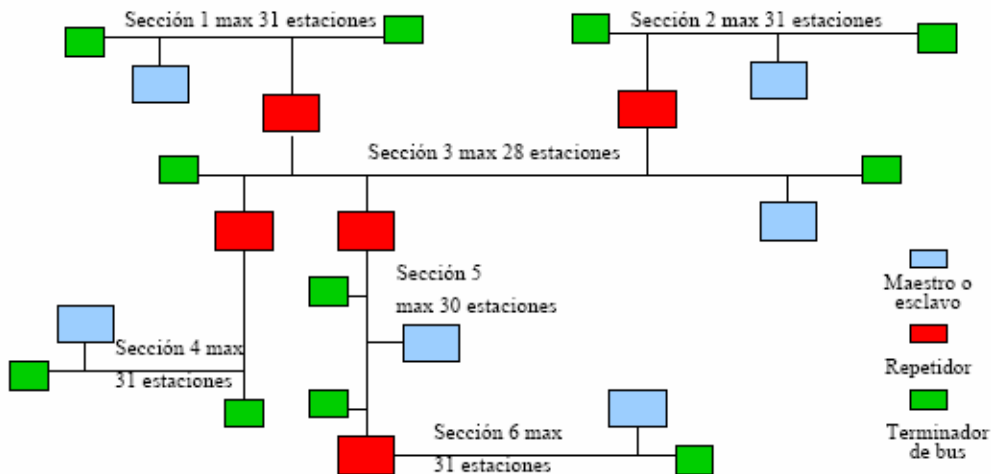


Fig. Nro: 14 Topologías lineal y árbol ⁽¹⁴⁾

2.12 COMPARACION DE BUSES DE CAMPO

En los siguientes cuadros se señalan los datos más destacados de los buses de campo. Para mayor información dirigirse a la siguiente página Web: <http://www.synergetic.com/compara.htm>.

Bus	Empresa/País	Estándar	Año
Device Net	Allen Bradley. USA	ISO 1189, 11519	1994
InterBus	Phoenix Contact USA-Alemania	DIN 19258	1984
Profibus	Profibus Internacional	EN 50170	1994
WorldFip	WorldFip. Francia	EN50170. ICC 1158-2	1968
CompoBusD	Omron Electronics Japón	Device Net	1996
SafetyBus p	PilZ. Alemania	Interbus S Profibus DP	1998

Tabla Nro: 3 Generalidades

Bus	Medio	Distancia en m sin repetidores	Nro. De dispositivos	Topología
Device Net	Par trenzado. Alimentación	500	64	Bus genérico. Árbol
InterBus	Par trenzado. Fibra óptica	400 > 10 Km.	256	Segmentos con derivaciones T
Profibus	Par trenzado. Fibra Óptica	100 > 20 Km.	127	Bus lineal, estrella y anillo lógico
WorldFip	Par trenzado	500 a 1000 m	127	Bus lineal, estrella lógica

Tabla Nro: 4 Características Físicas

Bus	Comunicación	Método de acceso	Tamaño máximo de transferencia de datos	Errores
Device Net	Punto a Punto. Principal-secundario	Detección de portadora CMSA	Variable desde 8 bytes	CRC-16 BIT
InterBus	Principal-secundario	Varios	Variable hasta 512 bytes	CRC-16 BIT
Profibus	Punto a punto Principal-secundario	Paso de testigo	Variable hasta 244 bytes	HDA-CRC
WorldFip	Punto a Punto	Centralizado	Variable hasta 256 bytes	CRC- 16 BIT

Tabla Nro: 5 Tipos de comunicación

Hay otras ofertas tecnológicas para la construcción de redes de comunicaciones industriales, son las redes que se organizan para la coordinación en el plano de área. En este nivel de comunicación trabajan coordinadamente PC, PLC y controladores especiales (Numéricos, CNC y robots), incluso impresoras en la mayoría de los casos. Estas redes son:

- **Ethernet Industrial**, estándar abierto, que utiliza la norma IEEE 802.3, y su versión inalámbrica (IWLAN), IEEE 802.11x, tema del desarrollo de la investigación.

REFERENCIAS BIBLIOGRAFICAS:

- **Pedro Morcillo Ruiz y Julián Cocerá Rueda.** “Comunicaciones Industriales” - Sistemas de Regulación y Control Automático. Editorial Paraninfo. (2004).
- **Ramón Piedrafita Moreno.** “Ingeniería de Automatización Industrial”. 2da Edición Ampliada y Actualizada. Editorial Ra-Ma. (2004),
- **Emilio García Moreno.** “Automatización de Procesos Industriales”. Editorial Spupv (SPUPV-99.4116). (1999).
- **Siemens.** Manual Bus AS-I. C79000-G8778-C089-04. (2006).
- **Siemens.** Manual Profibus según IEC 61151/EN50170. (2007)
- **Rolf Bedker.** “AS-Interface- La solución para la automatización”. Milán 2005.
- **Kuaper.** “Solución Can Avanzadas. Publicación empresa Kuaper. (2007).
- **Ing. Fabiana Ferreira.** Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008).
- **Universidad de Valencia- España.** Apuntes de la cátedra “Sistemas Distribuidos Industriales”. Universidad de Valencia. (2008).

REFERENCIA DE LAS FIGURAS:

- (2). Bus AS-i en una Red Industrial. Pagina 10- Manual Siemens C79000-G8778-C089-04. (2006).
 - (3). Cable Bifilar AS-i. Manual Siemens C79000-G8778-C089-04. (2006).
 - (4). Proceso de modulación de la señal AS-i. “AS-Interface- Pagina 64-La solución para la automatización”. Milán 2005.
 - (5). Topologías a emplear en una red AS-i. “AS-Interface- Cap. 2, Pagina 19- La solución para la automatización”. Milán 2005.
 - (6). Consulta Cíclica. “AS-Interface- La solución para la automatización”. Cap. 3, pagina 105, Milán 2005.
 - (7). Formato del mensaje AS-i. “AS-Interface- La solución para la automatización”. Milán 2005. Cap. 3, pagina 105.
 - (8). Definición del modelo OSI para DeviceNet. Pagina 2- Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008).
 - (9). Tramas de datos CAN. Solución Can Avanzadas. Pagina 4 Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008).
 - (10). Topología “trunk-line/drop-line. Solución Can Avanzadas. Pagina 4. Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008).
 - (11). Redes PROFIBUS. Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. Pagina 8. (2008).
 - (12). Acceso al Medio. www.aisa.uvigo.es. Presentación cátedra departamento de sistema y automática. Pagina 25. (2007).
 - (13). Bus PROFIBUS. www.aisa.uvigo.es. Presentación cátedra departamento de sistema y automática. Pagina 28. (2007).
 - (14). Topologías lineal y árbol. Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. Pagina 5. (2008).
- <http://www.synergetic.com/compara.htm> .Comparación buses de campo.

REFERENCIAS DE TABLAS:

Tabla Nro: 1. Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008). Ventajas y desventajas de los buses de campo.

Tabla Nro 2. Apuntes Seminario de Automatización y control industrial. Universidad de Quilmes. (2008). Extensión de la red x tasa de transmisión.

Tabla Nro: 3, 4 y 5. <http://www.synergetic.com/compara.htm> .Comparación buses de campo.

3. ETHERNET INDUSTRIAL

3.1 INTRODUCCION

Ethernet es el estándar universal diseñado por Xerox Corporation y registrada posteriormente por Digital e Intel. Bajo el estándar IEEE 802.3, nació y se desarrollo exclusivamente para las redes de oficina, por lo tanto su naturaleza inicial no la hacía apta para su utilización en el ámbito industrial. Sin embargo en los últimos años han sido desarrollados diferentes medios físicos, nuevas tecnologías, protocolos y el gran avance en el sistema de conmutación (switches), permiten su utilización en el ámbito industrial.

La tecnología Ethernet asociada a la tecnología de full duplex y autosensing permiten adaptarla a la red industrial. Como se observa en la Figura Nro: 1, es compatible con el modelo OSI en las capas 1, 2 y 7, y permite diferentes topologías, como ser bus, anillo, estrella. La velocidad de transmisión puede elegirse en función de sus necesidades, desde 10 Mbps a 10 Gbps (Giga Ethernet), ya que su escalabilidad le permite introducirla paso a paso en los nuevos avances tecnológicos.

- Capa física: Especifica el medio de transmisión. Seria el sustituto digital de la señal 4-20 [mA] en el entorno de proceso.
- Capa de enlace: Especifica comunicación entre dispositivos de un mismo bus, el método de acceso a este y chequea posibles errores.
- Capa de aplicación: Encargada de dar formato de mensaje a los datos, de forma que sean entendibles por el dispositivo receptor y emisor. También ofrece servicios a la capa de usuario.
- Capa de usuario: Ofrece a las aplicaciones finales funciones especificas de control e identificación automática de dispositivos.

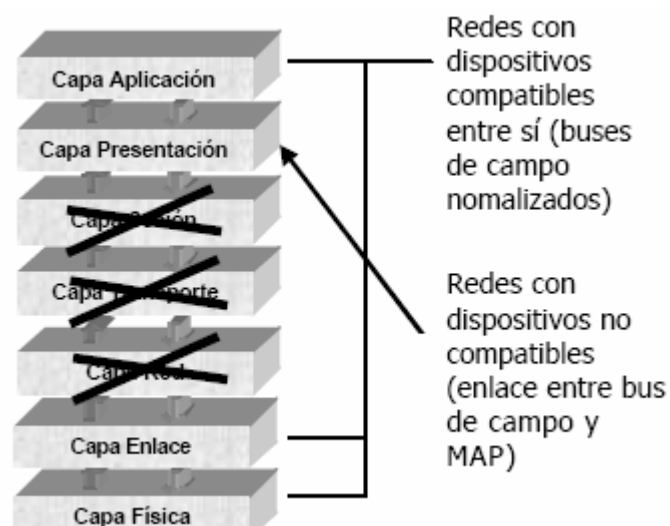


Fig. Nro: 1 Capas Ethernet Industrial ⁽¹⁾

Internacionalmente, varios fabricantes ya la han adoptado, como plataforma de funcionamiento de sus redes industriales. Los ejemplos más característicos son: Modbus/TCP de Scheneider, Ethernet IP de Rockwell, EtherCAT de Technology

Group, etc. Prácticamente hay una total convergencia hacia las redes Ethernet para su utilización como capa de información.

Ethernet Industrial es similar a la Ethernet convencional, pero está rediseñada para ser utilizada en plantas de procesos continuos como de manufactura. La misma utiliza componentes y medios de la Ethernet convencional, para reemplazar a los tradicionales medios utilizados en las redes industriales, y para satisfacerlos incorpora características de robustez, redundancia y durabilidad, que permiten a los dispositivos seguir conectados a pesar de las condiciones en que a menudo se trabaja en una planta.

Ethernet Industrial permite a las empresas tomar datos de una línea de manufactura y utilizarlos con software corporativo, como por ejemplo las aplicaciones de control de inventarios y gestión de activos, estos datos en tiempo real se ofrecen vía navegador Web a los encargados de las tareas de diagnóstico y monitorización remota del proceso de fabricación. Todos los dispositivos de I/O, pueden trabajar con la Web, que con solo tener un número de IP, toda la información de diagnóstico sobre los mismos estará disponible en la red en tiempo real.

Hoy en día ha crecido en forma exponencial, de tal forma que está presente en todos los niveles de comunicación del modelo CIM.

Las razones para utilizar Ethernet en la industria son:

- Costos reducidos y amplia aceptación.

Ethernet es un protocolo ampliamente aceptado que cuenta con el apoyo de la IEEE y de los comités internacionales de estandarización. Además cuenta con una importante difusión en aplicaciones ofimáticas.

- Velocidad.

Los últimos avances de la tecnología Ethernet incluyen Fast Ethernet y Giga Ethernet. Fast Ethernet (100 Mbps) es actualmente una tecnología de vanguardia, pero Giga Ethernet (1/10 Gbits), la esta suplantando actualmente en la mayoría de las aplicaciones y es considerada la tecnología del futuro.

- Integración con Internet/Intranet.

Todas las redes Ethernet instaladas son compatibles con protocolos de comunicaciones que implican una sofisticada transferencia y administración de datos. El protocolo más utilizado es el TCP/IP, y debido a sus cualidades de conexión a Internet y a Intranet corporativas, las “islas” de control son, por lo tanto una reliquia del pasado.

Ethernet permite implantar una comunicación universal desde el nivel de campo hasta el nivel de gestión (Pirámide CIM), e incluso abarcar todo el mundo.

3.2 REQUERIMIENTOS PARA SU UTILIZACION EN PLANTA

Ethernet, originalmente se diseño para redes de oficina, no era aplicable directamente en ambientes industriales, ya que los requerimientos son diferentes. Los

protocolos y principios básicos son los mismos, pero requieren de la incorporación de nuevos diseños para hacerla más robusta y confiable como así también adaptaciones de los medios físicos.

Los medios físicos de Ethernet, el cable, los conectores utilizados en las computadoras de oficina, impresoras y demás periféricos, permiten que los usuarios compartan archivos, accedan a impresoras, envíen e-mail, naveguen por Internet y realicen todo tipo de transferencia de datos. Sin embargo, las necesidades a pie de fábrica son mucho más exigentes y demandan requerimientos especiales. En este nivel (nivel de proceso), los controladores tienen que acceder y transferir datos entre los sistemas operativos, estaciones de trabajo y dispositivos I/O. En una situación normal (de oficina), el sistema deja al usuario esperando un cierto tiempo mientras realizan la tarea de procesamiento, pero en planta es muy distinto, el tiempo es crucial y ello requiere una comunicación en tiempo real. Por ejemplo parar un robot soldador o llenar una botella en su tiempo justo requiere un ajuste de tiempo sumamente preciso, comparado a lo que se exige para acceder a un archivo en un servidor remoto o sencillamente bajar una página de Internet de un servidor Web.

3.3 CONSIDERACIONES DE LA CAPA FISICA DE ETHERNET INDUSTRIAL

Lo primero que hay que tener en cuenta en una red industrial Ethernet es la capa física, que esta compuesta por: los medios de comunicación (cableado), conectores, interfaces de red, etc.

El primer medio utilizado fue el 10Base5, cable coaxial grueso, actualmente, al igual que las redes de ofimática se popularizó 10BaseT, 100Base TX y 1000BaseT, utilizando como medio de transmisión el par trenzado no blindado UTP (Unshielded Twisted Pair), el par trenzado blindado STP (Shielded Twisted Pair) y el par trenzado apantallado ScTP (Screened Twisted Pair).

Hay que tener en cuenta, que tanto los cables a utilizar y los conectores actuales usados en las redes de computadoras, adolecen de la robustez mecánica, inmunidad al ruido e interferencia electromagnéticas, requeridos en los ambientes industriales. Además también hay que tener en cuenta las vibraciones mecánicas presentes que tienden a aumentar los falsos contactos, tan frecuentes en este tipo de estructuras.

Los puntos más importantes a tener en cuenta, presentes en un ambiente industrial y que no fue pensado para la Ethernet original son los siguientes:

- Goteos y filtraciones de agua, aceites u otros líquidos.
- Condiciones extremas de temperatura y humedad.
- Ruido eléctrico (interferencias electromagnéticas).
- Sobretensiones.
- Radiaciones.
- Golpes, esfuerzos y vibraciones mecánicas.
- Suciedad, partículas y polvo.
- Acción de vapores y/o productos químicos corrosivos.

Los efectos más nocivos son indudablemente físicos, provocando deterioro y degradación, reduciendo la vida útil de los componentes que forman parte de la red,

provocando falsos contactos, aperturas y cortocircuitos, que producen fallas intermitentes o permanentes. Además las interferencias electromagnéticas siempre presentes en ambientes industriales, no sólo producirán errores en la transmisión de datos sino también daño en los equipos si no están especialmente aislados.

Las fallas producidas, no serán como las ocurridas en una red de oficina, donde una falla por lo general implica tan solo que algunas estaciones de trabajo no puedan comunicarse entre si o enviar correo electrónico por algunos minutos, en una aplicación industrial, cuando un dispositivo conectado a la red sufre una falla que lo aísla del resto, aunque sea por un brevísimo periodo de tiempo, puede producir grandes perjuicios económicos y afectar la integridad de personas e instalaciones.

3.4 HARDWARE NECESARIO

3.4.1 MEDIOS Y CONECTORES

Los medios y conectores a utilizar en Ethernet industrial son los siguientes:

- Cable STP, par trenzado blindado y el ScTP, par trenzado apantallado.
- Conectores RJ-45, con protección especial según norma IP-67,
- Recientemente conectores DB y M12, de máxima seguridad.
- Fibra Óptica, es la más recomendable, con las siguientes ventajas con respecto al cable de cobre:
 - Mayor ancho de banda.
 - Inmunidad a las interferencias electromagnéticas
 - Menor mantenimiento.
 - Mayor seguridad
 - Adaptación a nuevos estándares LAN/WAN.
 - Cables más livianos y con mayor resistencia a la tracción.
 - Para la aplicación en planta es suficiente con la utilización de fibra multimodo, aunque para grandes distancias y telecomunicaciones se utiliza la monomodo.

Características de transmisión:

- Cat.5 / Clase D: hasta 100 MHz: para 100BASE-TX
- Cat.6 / Clase E: hasta 250 MHz: para 1GBASE-T
- Cat.6A / Clase EA: hasta 500 MHz: para 10GBASE-T
- Cat.7 / Clase F: hasta 600 MHz: para 10GBASE-TX



Fig. Nro: 2 Conectores según Norma IEC 61076-3-106 ⁽²⁾

3.4.2 PLACAS DE INTERFAZ O NIC

Son similares a las utilizadas en las computadoras, adaptadas a las PC industriales, o integradas a los PLC, controladores, sensores y actuadores. Cumplen los mismos requerimientos que en las redes de ofimática: direccionamiento, firmware, etc., además poseen una construcción especial que las hacen aptas para trabajar en ambientes industriales.

3.4.5 SWITCHES

Única opción viable en las comunicaciones industriales a nivel de capa de enlace, pieza central en la infraestructura de una red Ethernet Industrial, su funcionamiento se basa en construir una tabla con las direcciones MAC (dirección de acceso al medio), para poder direccionar correctamente los paquetes de información, logrando así la conformación de redes dinámicas, con un alto grado de determinismo y evitando colisiones.

De construcción robusta e inmune al ruido eléctrico y a las vibraciones mecánicas. Son deseables las siguientes características:

- Alimentación redundante.
- Aislación galvanica en sus puertos (recomendable hasta por lo menos 3000 V).
- Amplio rango de tensión de alimentación.
- Conectores robustos de los puertos.
- Gabinete estanco, con nivel de protección IP-67 y montaje sobre riel DIM.
- Plug and Play.

En la siguiente Figura, se puede observar, parte de una red industrial, formada por controladores (PLC) y distintos dispositivos (paneles de control, PC, etc.), enlazados por Switches.

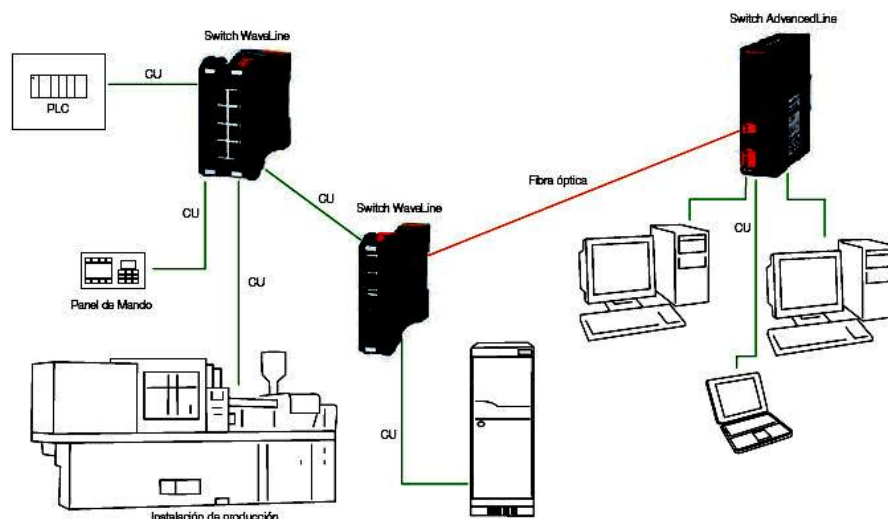


Fig. Nro: 3 Red Industrial con Switch ⁽³⁾

3.4.6 ROUTERS

Estos dispositivos de capa 3, permiten interconectar redes de igual naturaleza (por ejemplo TCP/IP), y conexiones a Internet, son dispositivos protocolo-dependientes y por lo tanto son utilizables en los casos en donde la red es homogénea. Permiten separar redes Ethernet por razones de seguridad de los datos o para una configuración sencilla. Además de poseer los mismos requerimientos de los switches, son deseables además las siguientes características:

- Watch-dog y auto recuperación.
- Reconfiguración dinámica de las tablas de ruteo.
- Señales discretas de alarma para indicar fallas de campo.
- Mensajes de alarma (por ejemplo e-mail).
- DHCP Server incorporado.
- Soporte SNMP.
- Soporte para VLANs.
- Utiliza una pasarela transparente, el cual posee los drivers integrados para poder comunicarse con la mayoría de los PLCs:
 - o Modbus TCP, Modbus RTU.
 - o Fins de Omron.
 - o DF1, Unitelway, MPI-Profibus y AS511.
- También permite formar sistemas integrados con modems para poder integrarse a redes celulares GSM/GPRS, con lo cual puede establecer enlaces virtuales punto a punto o punto multipunto, alcanzando distancias mayores de comunicación.
- OPC Server.

Se puede observar en la figura, redes de maquinas y redes privadas, comunicadas a través de routers.

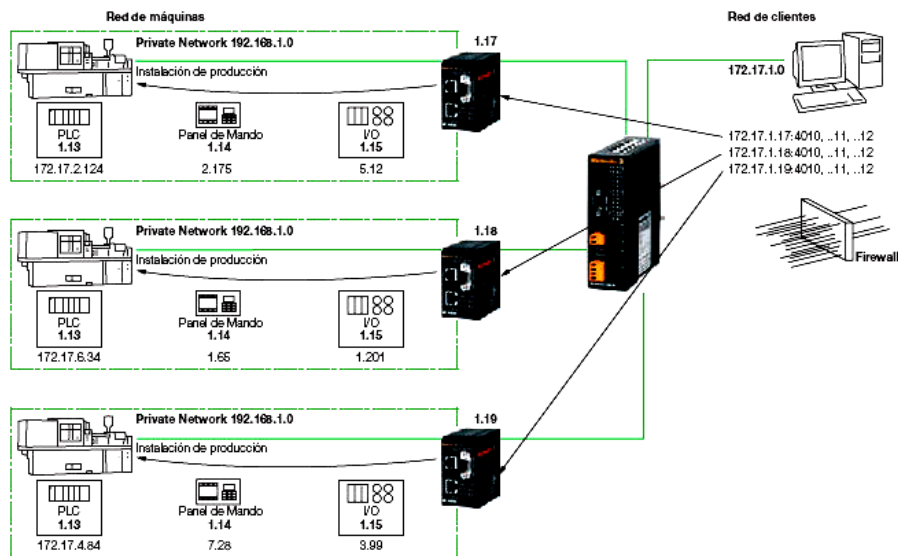


Fig. Nro: 4 Utilización de router en red Ethernet Industrial ⁽⁴⁾

El OPC Server,(OLE for Process Control) es un estándar de comunicaciones universal en el campo de control y supervisión de procesos utilizado en los sistemas SCADA para la conexión remota desde cualquier cliente (generalmente una computadora) que quisiera modificar parámetros, configuraciones o variables, sin disponer de los drivers específicos para el dispositivo en cuestión. Este estándar permite que diferentes fuentes de datos envíen datos a un mismo servidor OPC, al que a su vez podrán conectarse diferentes programas compatibles con dicho estándar, con solamente disponer de un driver OPC

3.4.6.1 FUNCIONAMIENTO DE OPC

Basado en la tecnología OLE/COM (Object Linking and Embedding/Component Object Model) de Microsoft, constituyen la base de la tecnología OPC, es una arquitectura cliente servidor que brinda una muy buena plataforma para extraer datos de una fuente (en este caso un equipo industrial) y a través de un servidor comunicarlo a cualquier aplicación cliente de manera estándar. Los fabricantes de hardware pueden desarrollar servidores optimizados para recoger datos de sus dispositivos, dando al servidor una interfaz OPC que permite a cualquier cliente acceder a dichos dispositivos.

En la figura Nro 5, se muestra la arquitectura simplificada de un sistema de control distribuido tradicional, en este se ve como cada aplicación de usuario debe tener su propio driver para comunicarse con los dispositivos físicos. Aquí se pueden presentar dificultades en dos niveles, en primer lugar se deben desarrollar un controlador de dispositivos, que es un programa encargado de hablar directamente con el equipo industrial a monitorear y/o controlar. Si por ejemplo el dispositivo es un PLC, entonces se debe programar (o en su defecto adquirir) un programa que sea capaz de hablar directamente con el PLC para pedirle datos o configurar su funcionamiento.

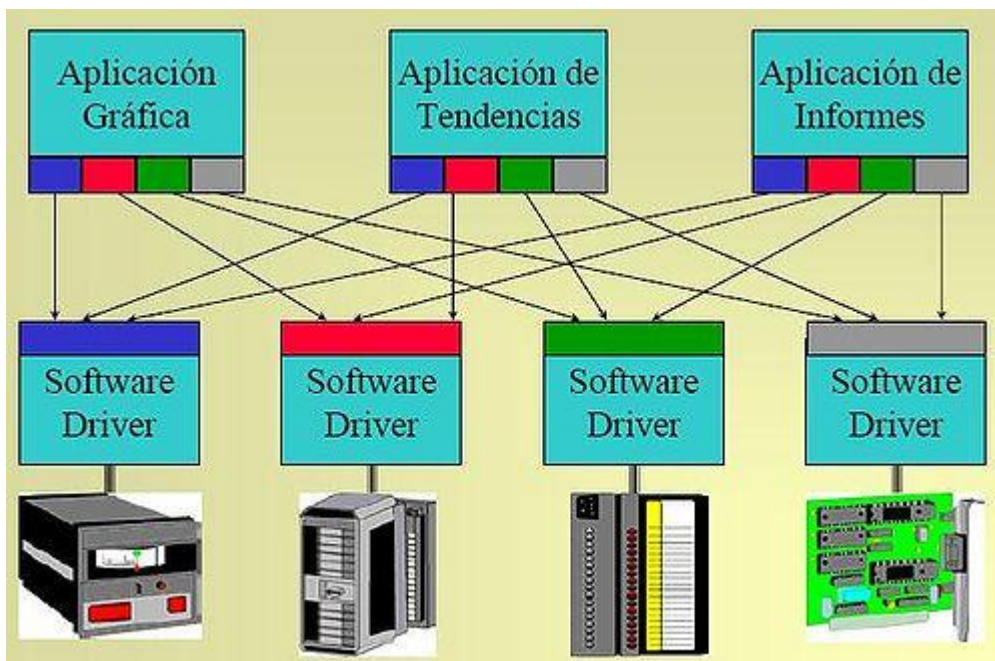


Fig. Nro: 5 Sistema tradicional de control distribuido de procesos ⁽⁵⁾

Por otro lado se debe desarrollar un driver que pueda “hablar” con el controlador del dispositivo para enviar y recibir los datos que cada aplicación requiera. Una de las aplicaciones podría consistir en un programa sencillo, que solo reporta datos de producción a un ejecutivo encargado de supervisar el control de calidad, la otra aplicación podría ser un programa más complejo en que el ingeniero encargado de programar la producción, pueda visualizar información y mediante alguna interfaz segura (para evitar problemas , como ser la intromisión de un Hacker que logre introducirse en la red de la empresa), pueda configurar aspectos importantes del proceso productivo, por ejemplo modificar los parámetros de un controlador o el programa almacenado en la memoria de un PLC.

Podemos observar en la Fig: 6, una arquitectura simplificada de un sistema de control distribuido que incorpora tecnología OPC, para que un sistema como este pueda funcionar adecuadamente, el equipo industrial debe soportar la comunicación con un servidor OPC, este servidor, no es más que un programa ejecutándose localmente en el mismo computador donde ocurre la aplicación de monitoreo y control o remotamente en otro equipo que actúe de servidor (Ejemplo, un router), este funciona como una pasarela de información (Gateway) entre las aplicaciones de software de monitoreo y control y el equipo industrial, haciendo que la comunicación sea totalmente transparente.

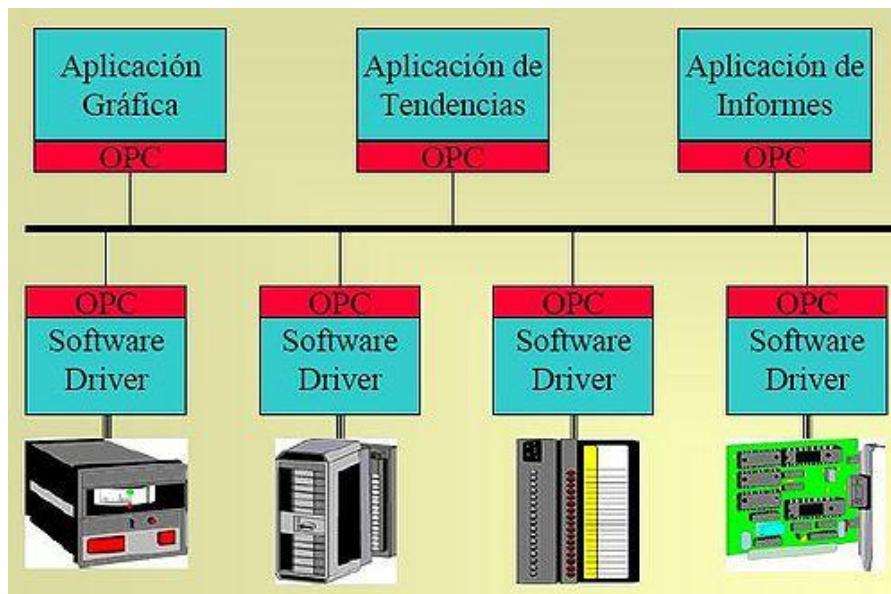


Fig. Nro: 6 Sistema de control distribuido que incorpora tecnología OPC ⁽⁶⁾

OPC está desarrollado para que sea independiente de las tecnologías de transporte de datos que puedan existir en una empresa, es así como el programador no debe preocuparse si los datos se transmiten por buses seriales tipo RS-232 o RS-485, o si los equipos y los computadores están interconectados usando redes LAN de estándar industrial, OPC tiene la robustez suficiente para que un fabricante pueda garantizar una comunicación de tipo “Plug & Play” entre un equipo que soporte OPC y su respectivo servidor OPC.

La comunicación entre los Clientes y Servidores OPC es transparente y se ha diseñado de tal manera que pueda funcionar virtualmente sobre cualquier medio de

transmisión de información, por lo tanto contar con un Servidor de OPC en la red industrial permite de manera rápida y fácil el control y monitoreo del sistema.

3.4.7 GATEWAYS

Son dispositivos de Internetworking que cumplen las mismas funciones que un router, pero se utilizan para interconectar redes de diferente naturaleza, ya que convierten protocolos, por lo tanto trabajan en todas las capas del modelo OSI. Son muy importantes en las redes industriales, ya que es normal encontrar diferentes plataformas instaladas, especialmente en las conexiones de Ethernet. Cobran enorme importancia en el caso de redes industriales, ya que es normal encontrar diferentes plataformas instaladas, más aun en el caso de la interconexión a Ethernet.

Deben ser diseñados específicamente para aplicaciones industriales, por ser los protocolos utilizados no habituales en redes comerciales estándares.

3.4.8 GPRS

Es una técnica de conmutación de paquetes, comparable con el protocolo TCP/IP usado en Internet, cuya función es avisar, informar y teleasistencia. Como se observa en la Figura Nro: 7, es usado en la gestión de alarmas del sistema. Es una evolución de las redes GSM actuales, permitiendo transferencias de datos hasta 144 Kbps.



Fig. Nro: 7 Sistema de alarma con GPRS ⁽⁷⁾

3.4.9 CONVERTIDORES DE FIBRA-COBRE

Cuando los trayectos de comunicación son largos, desde la estación de campo hasta la zona de procesamiento de la información, se aconseja utilizar la tecnología de Fibra Óptica, por lo tanto se utilizan convertidores de fibra óptica-cobre, como se observa en la Figura, que transforman la señal eléctrica de un puerto RJ-45 a una señal óptica y viceversa.

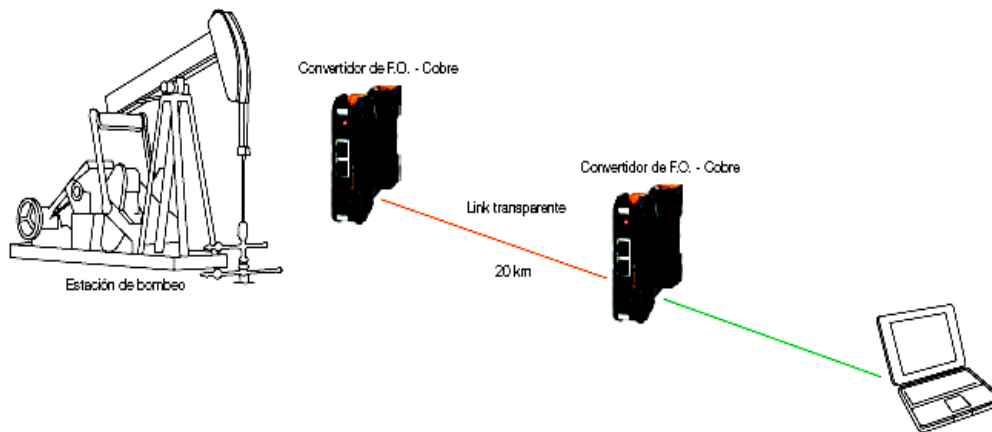


Fig. Nro: 8 Convertidor Fibra-Cobre⁽⁸⁾

3.4.10 COMSERVER

Son dispositivos utilizados para integrar los elementos finales a la red Ethernet industrial, como ser instalaciones de producción, paneles de mando y control, computadoras, etc. En la Figura, se observa la integración de un Comserver, con una instalación de producción, un panel de mando y una PC industrial.

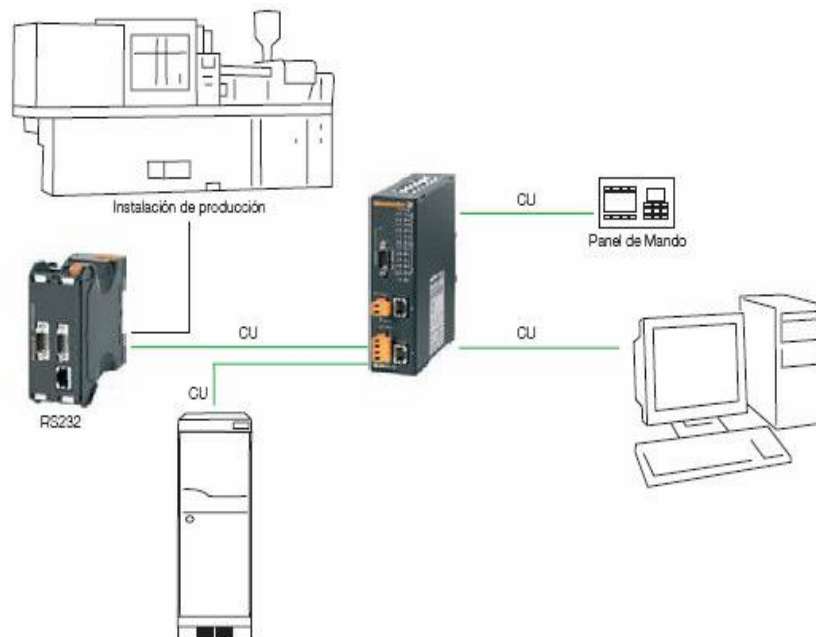


Fig. Nro: 9 COMServer⁽⁹⁾

3.4.11 IWLAN (REDES INALÁMBRICAS INDUSTRIALES)

Sistema de comunicación de datos inalámbrico, flexible, muy utilizado como alternativa de las redes LAN cableadas o como extensión de estas.



Fig. Nro: 10 Redes IWLAN⁽¹⁰⁾

En la Figura se observa, una integración, entre una red inalámbrica y una red cableada de control.

3.5 TOPOLOGIAS EMPLEADAS

3.5.1 TOPOLOGIA BUS

En la topología bus (como se observa en la Figura Nro: 11, todas las estaciones se conectan a un mismo tramo de cable y todas escuchan los paquetes que se difunden por el canal de transmisión.

Presenta las siguientes ventajas:

- La falla de la interfaz de cualquier estación de la red no afecta por lo general al resto de la red.
- La inserción de nuevos dispositivos es sencilla.
- Se consiguen altas velocidades de transmisión con tasas de errores muy bajas.
- El acceso al medio y la transmisión es muy rápida si la carga del trabajo de la red es baja.

Presenta las siguientes desventajas:

- El mecanismo de acceso al medio, tiene que ser muy elaborado para permitir un límite de tiempo de acceso al canal.
- Al agregar nuevos nodos al bus puede ser que se interrumpa el tráfico.
- La rotura del bus puede bloquear el tráfico de todas las estaciones.
- Bajo cargas de trabajo altas, las prestaciones caen drásticamente.

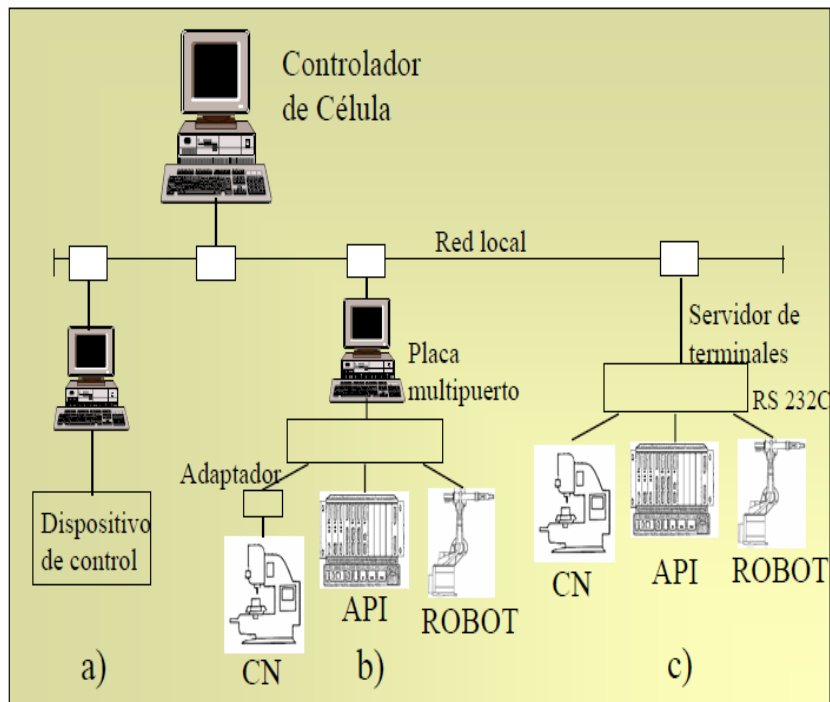


Fig. Nro: 11 Topología Bus⁽¹¹⁾

3.5.2 TOPOLOGA ANILLO

Como se observa en la Figura Nro: 12, en esta topología cada dispositivo esta unido físicamente al anterior y al posterior, la estación siempre recibe los mensajes del anterior, y cuando no están dirigidos a el, la interfaz lo transmite al siguiente sin ningún tipo de modificaciones, por lo tanto la información circula siempre en el mismo sentido dentro del anillo.

Presenta las siguientes ventajas:

- El acceso a la red esta asegurado en un periodo de tiempo máximo limitado.
- Se simplifica los mecanismos de acuse recibo, por ejemplo haciendo que el dispositivo que transmite una trama sea la encargada de retirarla.
- Proporciona velocidades de transmisión altas con tasas de errores muy bajas.
- Este tipo de redes se comporta bien en condiciones de tráfico intenso en la red.
- Todos los nodos tienen acceso a la información que circula por el anillo, lo que permite la priorización de tramas.

Presenta las siguientes desventajas:

- La falla de una estación o dispositivo puede llegar a interrumpir la comunicación del resto, por lo cual hay que buscar la forma de puentear estaciones averiadas o inactivas.
- La incorporación de nuevas estaciones a la red o la ampliación del alcance de la misma se torna complicada, si no existe un diseño de la conexión adecuado.

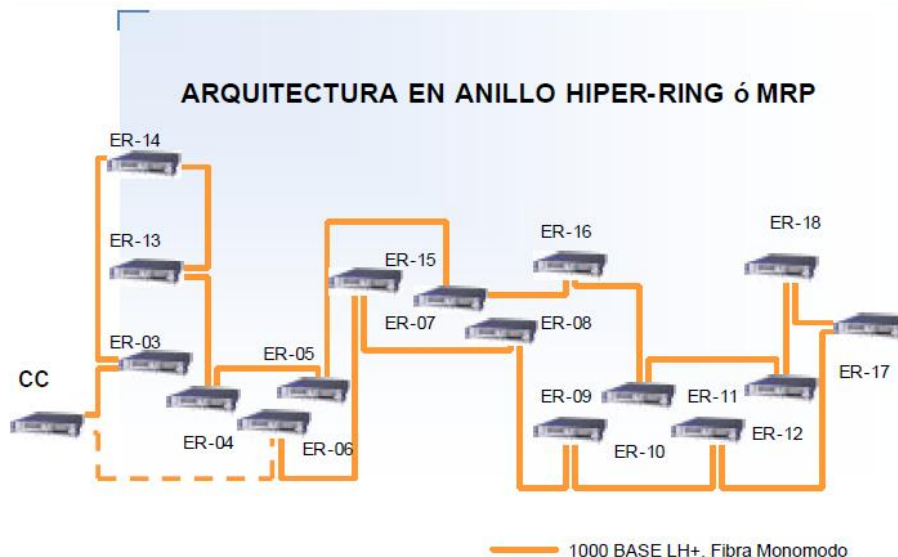


Fig. Nro: 12 Topología Anillo ⁽¹²⁾

3.5.3 TOPOLOGIA ESTRELLA

En la topología estrella todo el tráfico pasa a través de un concentrador o un nodo central, que puede ser activo o pasivo. La conexión en cascada de los concentradores, permite ampliar la red, que da lugar a una topología jerarquizable en forma de árbol.

Pueden utilizarse concentradores pasivos (Hub), que simplemente repiten la señal que recibe a cada uno de los segmentos conectados a él, o los activos (switch/router), que almacenan y retransmiten la trama hacia cada nodo en función del direccionamiento de la trama, de esta manera el nodo central realiza el control centralizado, que consiste en interrogar a los nodos periféricos, procesar la información y encaminarla.

Presenta las siguientes ventajas:

- Fácil inserción de nuevos dispositivos.
- Alta seguridad ante la violación de la misma.
- Fácil detección de nodos fallados.
- Se pueden conectar dispositivos con diferentes protocolos de comunicación y diferentes velocidades de transmisión si el nodo central es activo.
- El direccionamiento nodo a nodo es sencillo.
- El nodo central activo puede establecer prioridad de tramas.

Presenta las siguientes desventajas:

- La falla del concentrador bloquea la red.
- Si el nodo central es activo, está dedicado exclusivamente a las comunicaciones.
- La actividad del nodo central activo, retrasa el tráfico en la red.

En la Figura siguiente, se observa una topología estrella/árbol, compuesta Switches y servidores industriales.

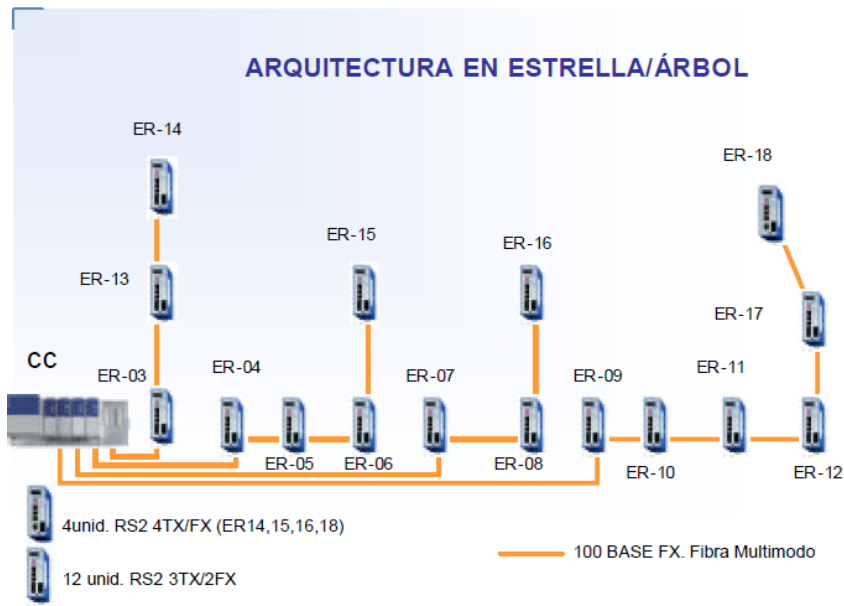


Fig. Nro: 13 Topología estrella/árbol ⁽¹³⁾

3.6 METODO DE ACCESO AL MEDIO

Es un método de control de acceso al medio físico (Red) no determinístico. Ethernet utiliza un medio físico único, compartido entre todos los dispositivos que desean intercambiar información, y para lo cual todos tienen igual prioridad. Por lo tanto debe existir algún mecanismo para evitar conflictos en el envío de los paquetes de datos y proteger su integridad. Cada nodo determina cuando la red está disponible para el envío de los paquetes. Siempre existe la posibilidad que dos o más nodos intenten transmitir al mismo tiempo, produciendo una colisión, como se observa en la Figura Nro: 14.

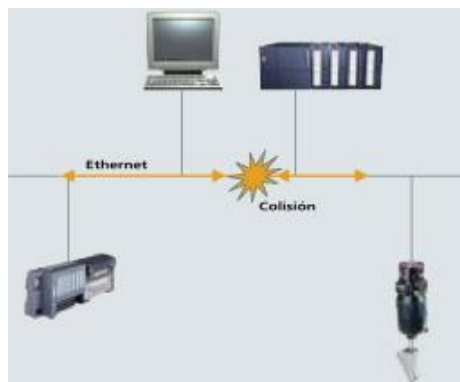


Fig. Nro: 14 Colisión en la red ⁽¹⁴⁾

Reducir al mínimo o eliminar las colisiones es un factor crucial en el diseño y la operación de las redes de datos industriales. Un aumento de las colisiones es

consecuencia de que varios nodos en la red, estén compitiendo entre si por el ancho de banda disponible, esta situación reduce la prestación de la red, haciéndola más lenta, una de las formas de reducirla es segmentando la red utilizando Bridges o switch, con lo cual se consigue mejorar esta situación desfavorable.

En su inicio Ethernet era half-duplex y estaba concebida para una topología de tipo bus compartido. Esto obligó a incluir un mecanismo para administrar el acceso al medio físico compartido, permitiendo “detectar y eliminar las colisiones”. El mecanismo elegido fue CSMA/CD, Acceso Múltiple por Detección de Portadora con Detección de Colisiones (Carrier Sense Múltiple Access with Collision Detection). Este método resuelve las colisiones mediante la emisión de una señal de “jamming” y la ejecución de un algoritmo de espera exponencial aleatoria.

La principal desventaja de CSMA/CD, en lo que se refiere a su utilización en entornos industriales, es que no garantiza un acceso al medio eficiente ya que es un mecanismo probabilístico. Esto sí se puede garantizar en el caso del paso de testigo o los sistemas con un único maestro que son mecanismos deterministas. Sin embargo hay que tener en cuenta que esto es solo cierto cuando el canal de transmisión esta libre de errores, ya que los errores convierten cualquier sistema de comunicación en probabilístico. Con bajas cargas de trabajo, la probabilidad de errores en estas redes es similar a las que ocurren en las que utilizan el mecanismo de CSMA/CD.

Con el fin de salvar los inconveniente de retrasos en la transmisión de mensajes y no estén tan acotados, se buscaron alternativas al mecanismo de acceso al medio CSMA/CD, una de estas alternativas es el mecanismo CSMA/DCR (Deterministic Collision Resolution).

Se trata de un protocolo idéntico al estándar de Ethernet, excepto en el método de resolución de colisiones. El periodo de resolución de una colisión se divide en un número programable de “slots”, asignándosele un “slot” a cada estación (como se observa en la Figura). El primer “slot” comienza inmediatamente después de que el canal queda libre, tras la señal de “jamming” y el tiempo de espera obligado de canal en silencio entre paquetes. Cada estación emitirá en el “slot” que le corresponda. Cuando se detecta una transmisión se abandona la cuenta de “slots” para reanudarla cuando finalice. Todas las estaciones han de detectar la colisión, incluso las que no participan en ella, de manera que estas también podrán transmitir su “slot” correspondiente.

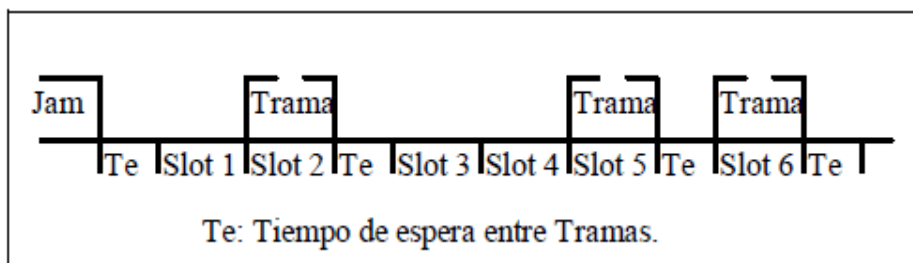


Fig. Nro: 15 Resolución de colisiones CSMA/DCR ⁽¹⁵⁾

Cuando las condiciones de carga son altas, los periodos de colisión se suceden sin periodos intermedios, dando lugar a una especie de multiplexación en el tiempo del canal de transmisión, esto permite a través de la siguiente expresión la utilización

máxima del canal (S_{\max} = **rendimiento máximo**) y el retraso máximo en el acceso de un paquete al canal de transmisión (T_{\max} = **tiempo máximo de acceso al medio**). El valor de γ , representa el tiempo que transcurre en una colisión desde que la primera estación comienza a transmitir hasta que todas las estaciones detectan el canal libre y que es aproximadamente igual para todas las estaciones.

N	Número de estaciones.
P	Longitud de la información de los paquetes (bits).
H	Longitud de la cabecera y cola de los paquetes (bits).
C	Velocidad de transmisión de la red (bits/s).
τ	Tiempo total de propagación de la señal a lo largo del bus.
$\tau/3$	Tiempo de propagación promedio entre las estaciones.
ϵ	Tiempo estimado que tarda la estación en detectar la colisión.
TEP	Tiempo de espera entre paquetes.
Jam	Tiempo de duración de la señal de “jamming”.

$$\gamma = 2\tau + Jam + \epsilon$$

$$S_{\max} = \frac{N \frac{P}{C}}{N \left(\frac{P+H}{C} + \frac{\tau}{3} + TEP \right) + TEP + \gamma}$$

$$T_{\max} = N \left(\frac{P+H}{C} + \frac{\tau}{3} + TEP \right) + \gamma$$

Fig. Nro: 16 Cálculo del rendimiento máximo en una red con CSMA/DCR ⁽¹⁶⁾

3.7 ACCESO DETERMINISTICO – SWITCH ETHERNET

Otra forma de reducir la probabilidad de una colisión, es disminuir el número de nodos conectados al mismo segmento de red. Al disminuir el número de nodos, la probabilidad de que dos nodos inicien una transmisión simultánea disminuye, y si se pudiera conectar un único nodo de red a cada segmento las colisiones se eliminarían. Esto se consigue utilizando un switch Ethernet. Un switch es un equipo especializado que tiene múltiples puertos Ethernet, un procesador dedicado, un bus interno de alta velocidad y una memoria rápida de lectura/escritura. Inicialmente cada una de las tramas recibidas por el switch es reenviada a todos sus puertos. Pero al recibir las respuestas, “aprende” sus direcciones físicas (MAC Address) asociándolas. A partir de ese momento, el switch reenviará las tramas considerando la dirección física de destino para decidir por cual de sus puertos las reenviará (solamente por ese puerto). Estas características lo diferencian de un Hub el cual, ya que éste también posee una cierta cantidad de puertos, pero sólo actúa como repetidor de las tramas recibidas.

Ethernet puede ser visto como una red “igualadora”, ya que todos los dispositivos interconectados (PC, servidores, PLCs, sensores, actuadores, terminales de dialogo, etc), en la misma red (LAN), se encuentran en igualdad de condiciones para enviar y recibir información.

Esto es así, porque hay una cantidad máxima de datos que se pueden enviar por una red Ethernet, en cada una de las transmisiones y por otro lado el primero que toma control de la red es el primero en utilizarla. En la red corporativa los ingenieros de planta a través de las diferentes computadoras y los dispositivos y utilizando herramientas de gestión, les permiten acceder a Internet y tener contacto con otros medios a través de correo electrónico, permitiéndoles también acceder a información relevante de otras áreas de la planta, muy útiles para llevar a cabo sus tareas de supervisión y control.

Un switch Ethernet Industrial puede ser usado para aislar efectivamente aquellos dispositivos claves del sistema de automatización en su propio dominio de colisión, trabajando en modo full-duplex, en este tipo de aplicación cada dispositivo es conectado a un puerto exclusivo del switch, aislándolo del resto del tráfico de la red, de este modo el switch Ethernet multipuerto permite la conexión de PLC con sus sensores y actuadores. Salvo por esporádicos accesos para su configuración y/o reprogramación por medio de otros nodos, el switch mantiene al PLC y sus elementos asociados totalmente aislados del resto de la red.

Todos los switch Ethernet poseen puertos que pueden operar a 10, 100 Mbps, 1 Gbps y 10 Gbps, permitiendo la interconexión de dispositivos que operan a diferentes velocidades, sin afectar a los más rápidos, como ser los enlaces que se efectúan entre dispositivos que operan en full-duplex a una velocidad de 1Gbps, que permiten el intercambio de datos en forma simultánea con 10 switches de 100 Mbps, sin que se produzcan colisiones.

También existe la opción de la conexión a través de fibra óptica, que brinda como ventaja principal la absoluta inmunidad al ruido eléctrico e interferencias electromagnéticas, permitiendo superar el límite de los 100 metros impuestos en la utilización de cable UTP o STP, pudiendo extenderse hasta distancias de varios kilómetros.

Los switch industriales operan de la siguiente forma:

- Identifican la dirección física (MAC address) de cada uno de los dispositivos conectados a sus puertos mediante tablas internas.
- Utilizan un buffer para almacenar y reenviar los paquetes de cada uno de los puertos, mediante un bus interno de alta velocidad.
- Esta información permite establecer redes dinámicas entre cada uno de los puertos involucrados.
- Trabaja a nivel de capa 2 (enlace), del modelo OSI.
- Utiliza las direcciones físicas de las tarjetas adaptadoras de red (MAC address).

Cuando es necesario utilizar un switch en una red industrial:

- Cuando es necesario un eficiente uso de cada uno de los puertos disponibles del switch.
- Disponer de un ancho de banda suficiente para las aplicaciones industriales (tramas de menor tamaño pero con mayor tráfico).
- Aislar la red de planta de la administrativa.
- Aislar dispositivo que por su velocidad operan en half-duplex, etc.
- Proveer de un enlace de alta velocidad entre diferentes “dominios” de colisiones.
- Recuperación rápida de la tabla interna, adecuada para aplicaciones industriales (< 1 seg. vs. 1 min. o más)
- A través de conversores de medio a fibra óptica, poder enlazarse con dominios de colisiones alejados y brindar alta inmunidad al ruido e interferencias.

3.7.1 CARACTERISTICAS ADICIONALES DE LOS SWITCH INDUSTRIALES

Los switch industriales deben poseer las siguientes características:

- **Priorización de los mensajes** según IEEE 802.1, que permite dar prioridad a los datos provenientes de determinado dispositivo con respecto a otros conectados en la red, acelerando la transferencia de datos, permitiendo que las tramas de alta prioridad no sean interrumpidas por el tráfico de menor prioridad, permitiendo al switch procesar los datos y enviar todos los paquetes de mayor prioridad antes de los de menor prioridad o alternar entre ambos.
- **Priorización de los puertos**, que en función del puerto de origen se le asigna prioridad a cada mensaje, sin tener en cuenta la asignada por los dispositivos conectados a él. Permite asignar prioridades a dispositivos que no soportan la norma IEEE 802.1p, y con respecto a los paquetes sin información de prioridad (VLAN o marca de prioridad), se transmite según la prioridad asignada a cada puerto, también permite asignarle una prioridad diferente a cada uno de los puertos del switch.
- **Redes virtuales (VLANs)** según IEEE 802.1Q, están basadas en establecer vínculos lógicos, en vez de físicos y constituyen elementos flexibles en el diseño de las redes. Una de sus mayores ventajas es la posibilidad de crear grupos de usuarios de acuerdo con un criterio funcional y no por su ubicación física o forma de acceso a la red. Las mismas están definidas en el estándar IEEE 802.1Q, también incluye el filtrado de tramas de tráfico broadcast y multicast, limitándolos a nodos que integran la VLAN.
- **Refresco rápido de tablas de enrutamiento.** Al desconectar un dispositivo y perder el vínculo con el switch, todas las tablas almacenadas con las direcciones de enrutamiento son eliminadas, obteniéndose los siguientes beneficios:
 - Útil cuando un dispositivo es eliminado o cambia su ubicación.
 - No hay interrupciones (timeout).
 - La estación que cambio de puerto es configurada rápidamente.
 - Utiliza para ello algoritmos “Spanning Tree” y de anillos redundantes.
- **Recuperación rápida de fallas funcionales.** Mayor confiabilidad de los switches industriales. Al considerar las comunicaciones en el ámbito industrial, la mayor confiabilidad no solo significa un gabinete robusto y la tolerancia a las temperaturas extremas, sino que también se refiere a una mayor tolerancia a las fallas funcionales, porque en un ambiente de oficina una falta de comunicación de tres minutos apenas causa inconvenientes, pero en una instalación industrial puede ser catastrófica, por lo tanto las funciones de auto recuperación resultan esenciales para mantener la red en funcionamiento.
- **Reportes dinámicos.** Debido a que los dispositivos en la red Ethernet pueden estar ubicados en puntos extremos en función de la topología y de los medios empleados, no siempre es posible conocer su estado de funcionamiento en lo que hace a la comunicación, por lo tanto los dispositivos empleados deben poseer los mecanismos adecuados par poder informar a los encargados de mantenimiento de cualquier desperfecto, utilizando mensajes de alarma en tiempo real, con lo cual le permiten estar informados del estado de todos los dispositivos de la red en forma instantánea.

La forma convencional de determinar su estado es interrogarlos periódicamente, aunque esto no garantiza un reporter de excepción en tiempo real, por lo tanto el sistema debe poder generar mensajes de advertencia disparados por estos eventos de excepción.

3.7.2 FUNCIONES DE ADMINISTRACION

Los switches industriales deben contar con las siguientes funcionalidades para poder administrar en forma conveniente los datos en una red Ethernet industrial.

- **Poder utilizar un navegador Web** para poder acceder a todas las funciones de configuración y administración.
- **Verificación de la integridad** de la red, utilizando el comando “ping” para la búsqueda de fallas en una red que presenta problemas de interrupción de la comunicación entre dispositivos, ya que estas pueden detener las líneas de producción o comprometer la seguridad de los operarios e instalaciones, este comando permite al personal de mantenimiento encontrar rápidamente de forma confiable el segmento de red con fallas, por lo tanto este comando es una herramienta esencial de diagnóstico.
- **Análisis remoto de datos** para poder determinar el comportamiento local de la red desde una ubicación remota, esta herramienta puede residir tanto en una PC, como en los dispositivos claves de la red, la misma le permite iniciar la captura de tramas con determinadas condiciones de disparo, registrar las mismas con marca de tiempo y filtrarlas según las condiciones más convenientes de cada caso. Las herramientas de captura que corren en la PC (Sniffers), permiten además realizar un análisis de cada trama a nivel de cada uno de los protocolos involucrados.
- **Configuración de “puertos espejos” para una mejor supervisión de la línea de datos.** En la puesta en marcha de una nueva aplicación, es necesario analizar el tráfico entre dos o más dispositivos. Por las características básicas de los switch, esto no es posible, por lo tanto el espejado permite configurar algunos puertos para que repitan el trafico de otro, facilitando el uso de las herramientas de captura y análisis.
- **Asignación de números de IP** a los dispositivos conectados y reemplazo de dispositivos dañados. Esto se hace a través de un servidor DHCP (incluido en el mismo switch), le asigne números de IP a los dispositivos de la red, también permite la configuración de un dispositivo nuevo cuando se reemplaza uno similar que fallo. Esto se hace asignándole un “**nombre de rol (rol name)**” a cada dispositivo, este nombre es asignado a través de la opción 82 del servicio DHCP y el protocolo TFTP, facilitando en forma notable las tareas de mantenimiento del personal no especializado en las tecnologías de informática.
- **Control de flujo de acuerdo a la norma IEEE 802.3x.**
- **Soporte SNMP** para simplificar el análisis y la administración de la red, permitiendo:
 -
 - Contraseñas encriptadas.
 - Claves de encriptación basadas en algoritmos robustos, lo que dificulta los “ataques de fuerza bruta”.
 - Encriptación de la información de administración que viaja en la red.

-
- Reportes por excepción de condiciones particulares de funcionamiento por medio de “traps”.
 - Administración por medio de “OPC Server” para una integración con los sistemas HMI/SCADA.

3.8 PROTOCOLO SPANNING -TREE

Este algoritmo es empleado en la determinación de los caminos posibles en una red Ethernet compleja. Está especificado en la norma **IEEE 802.1 D**. Este algoritmo impide la circulación de tramas, cuando existen caminos múltiples (redundantes), deshabilitando los puertos que sean necesarios, determinado el camino óptimo entre dos posibles. Cuando se produce una falla o interrupción el algoritmo elige un camino alternativo, el tiempo que tarda la nueva reconfiguración está entre los 30 y 90 segundos aproximadamente.

El Spanning-Tree, evita la formación de lazos cuando se conectan los switches entre sí por caminos múltiples, el algoritmo garantiza que en todo momento haya un único camino activo entre dos dispositivos de la red.

A cada switch se le asigna un grupo de IDs, uno para el switch en sí y otro para cada puerto del switch. El identificador del switch, denominado ID de Bridge (BID) tiene 8 bytes de largo y contiene una prioridad de Bridges (2 bytes) junto con una de las direcciones MAC del switch (6 bytes). Cada ID del puerto tiene 16 bits de largo y consta de dos partes, una configuración de prioridad de 6 bits y un número de puerto de 10 bits.

Se le adjudica un valor de costo de la ruta a cada puerto. El costo se basa típicamente en una guía establecida como parte de 802.1d, de acuerdo a la especificación original el costo es de 1000 Mbps (1 Gigabit) dividido por el ancho de banda del segmento conectado al puerto. Por lo tanto, una conexión de 10 Mbps tendría un costo de 100 (1000 dividido 10).

Cada switch comienza un proceso de descubrimiento para escoger que rutas de la red deberá utilizar, esta información es compartida entre todos los switches que utilicen tramas de la red denominadas **bridge protocol data units** (BPDU).

Todos los switches están enviando constantemente BPDUs entre sí intentando determinar la mejor ruta entre diversos segmentos. Cuando un switch recibe una BPDU proveniente de otro switch que sea mejor que aquel para el cual está haciendo broadcasting, dejará de hacer broadcasting de su BPDU hacia el mismo, en lugar de eso almacenará la BPDU del otro switch para referencia y para hacer broadcasting a los segmentos inferiores.

Un bridge raíz se elige basándose en los resultados del proceso de la BPDU entre los switches. Inicialmente, cada switch se considera a sí mismo el Bridge raíz. Cuando un switch se enciende por primera vez en la red, envía una BPDU con su propia BID como BID raíz, y cuando los otros switches la reciben, comparan con la que tienen almacenada, si la nueva tiene un valor inferior, reemplazan a la guardada, pero si la guardada es inferior se le envía una BPDU al nuevo switch con esta BID como la BID raíz. Cuando el nuevo switch la recibe, se da cuenta que no es el raíz, por lo tanto

reemplaza en su tabla, la suya por la que acaba de recibir. El resultado es el switch que tiene la BID más baja es el elegido como Bridge raíz.

Estado de los puertos:

Los estados en los que puede estar un puerto son los siguientes:

- **Bloqueo:** En este estado sólo se pueden recibir BPDU's. Las tramas de datos se descartan y no se actualizan las tablas de direcciones MAC (mac-address-table).
- **Escucha:** A este estado se llega desde Bloqueo. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualizan las tablas ARP. Se procesan las BPDU.
- **Aprendizaje:** A este estado se llega desde Escucha. Las tramas de datos se descartan pero ya se actualizan las tablas de direcciones MAC (aquí es donde se aprenden por primera vez). Se procesan las BPDU.
- **Envío:** A este estado se llega desde Aprendizaje. Las tramas de datos se envían y se actualizan las tablas de direcciones MAC (mac-address-table). Se procesan las BPDU.
- **Desactivado:** A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

Cada switch tiene una tabla de BPDUs que actualiza continuamente. Ahora la red esta configurada como un único Spanning Tree con el Bridge raíz como troncal y todos los otros switch como ramas. Cada switch se comunica con la raíz a través de los puertos raíz y con cada segmento a través de los puertos designados para mantener una red libre de bucles. En el caso de que el Bridge raíz comience a fallar o tenga problemas de red, STP permite a los otros switch la reconfiguración inmediata eligiendo otro Bridge raíz. Este proceso asombroso proporciona a una empresa la capacidad de contar con una red compleja que sea tolerante a fallas y aun así fácil de mantener.

Una variante a mejorada de este algoritmo es el **Rapid Spanning-Tree (RSTP)**, permite un tiempo de recuperación más corto del orden del segundo.

Es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. Especificado en IEEE 802.1w, es una evolución del Spanning tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

Roles de los puertos RSTP: (Figura Nro: 17)

- **Raíz** – Un puerto de envío elegido para la topología Spanning Tree.
- **Designado** – Un puerto de envío elegido para cada segmento de la red.
- **Alternativo** – Un camino alternativo hacia el Puente Raíz. Este camino es distinto al que usan los puertos raíz.
- **Respaldo** – Un camino de respaldo/redundante (de mayor costo) a un segmento donde hay otro puerto ya conectado.
- **Deshabilitado** – Un puerto que no tiene un papel dentro de la operación de Spanning Tree.

Los puertos raíz y designado forman parte de la topología activa. Los puertos alternativo y de respaldo no están incluidos en la topología activa

RSTP monitorea el estado de todas las trayectorias:

- Si una dirección activa se cae, RSTP activa las direcciones redundantes.
- Configura de nuevo la topología de la red adecuadamente.

Objetivos del RST

- Disminuir el tiempo de convergencia cuando un enlace falla.
 - De 30 ó 60 segundos a milisegundos.
- Soporta redes extendidas.
 - 2048 conexiones o 4096 puertos interconectados en comparación con 256 puertos conectados en STP.
- Compatibilidad con STP.

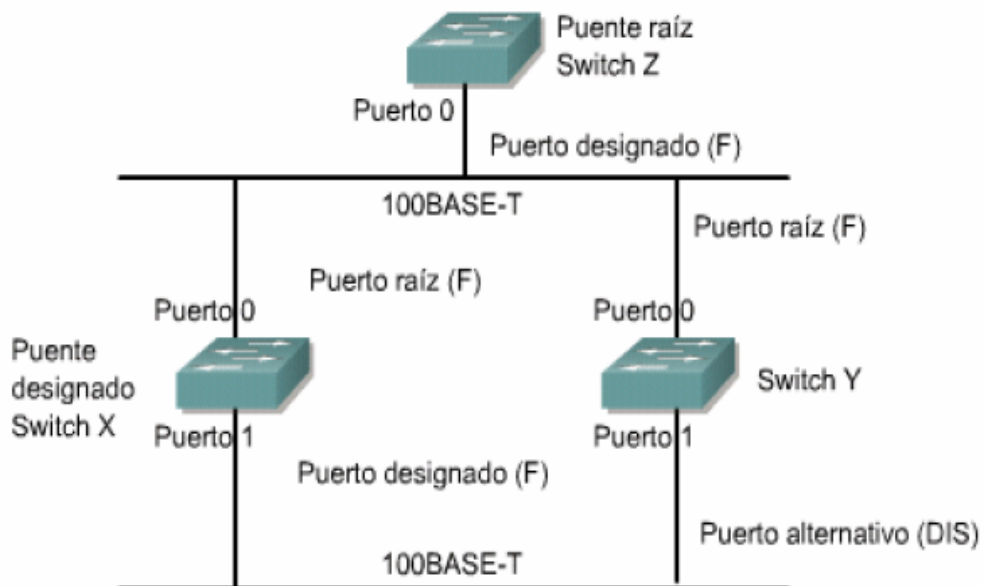


Fig. Nro: 17 Estándar Rapid Spanning Tree⁽¹⁷⁾

3.9 OTRAS SOLUCIONES

Para poder mejorar la velocidad de respuesta existen soluciones alternativas, desarrolladas por cada fabricante, basadas en estructuras en anillo.

Como se observa en la Figura Nro: 18, en esta arquitectura cada componente de la red se conecta a un anillo formado por switches, uno de ellos es responsable de administrar el anillo y evitar la circulación de tramas, los restantes switches pueden ser de tipo comercial y/o no administrables, pero es aconsejable utilizar switches industriales por su mayor velocidad de reconfiguración de sus tablas internas.

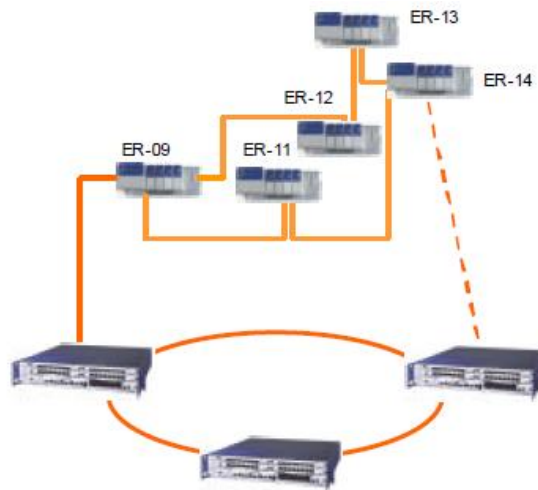


Fig. Nro: 18 Acoplamiento en anillo ⁽¹⁸⁾

Otra opción sería la utilización de switches redundantes los cuales permiten establecer vínculos duplicados entre los segmentos de la red, esta funcionalidad combinada con la arquitectura en anillo permite lograr una alta confiabilidad de la red.

3.10 ETHERNET BASADO EN TIEMPO REAL

Históricamente los buses de campo fueron empleados para cumplir con requisitos específicos para una determinada aplicación industrial, lo que limitó su funcionalidad, ya que no poseían la característica de transmisión de datos en tiempo real, tan necesarios en los eventos de las redes industriales. Se observó que los tiempos de retraso no eran debido a la red sino a la capa de aplicación de los protocolos. Con la utilización de Ethernet en las comunicaciones industriales y los diferentes protocolos que fueron apareciendo se solucionaron estos problemas.

3.11 PROTOCOLOS DE LA CAPA DE APLICACIÓN PARA ETHERNET INDUSTRIAL

La disponibilidad de soluciones en tiempo real resulta crucial para que Ethernet sea aplicada en el sector de la automatización. Actualmente, diferentes protocolos pueden utilizarse y la elección del mismo se encuentra íntimamente ligada al estándar adoptado para las capas de los dispositivos de control, este requisito está contemplado en varios protocolos que a continuación se detallan:

- **ETHERCAT:** Significa "Ethernet para el Control de Tecnología de automatización." Se trata de un código abierto, de alto rendimiento que pretende utilizar protocolos de Ethernet en un entorno industrial.
- **PROFINET:** Se aplica a los sistemas de automatización distribuida basados en Ethernet que integran los sistemas de bus de campo existentes, por ejemplo PROFIBUS, sin modificarlos.
- **ETHERNET POWER LINK:** El objetivo del desarrollo de Ethernet Powerlink consistió en aplicar la tecnología Ethernet estándar a la ingeniería de automatización, en condiciones de tiempo real adversas.

-
- **ETHERNET/IP:** A principios de 1998 un grupo de interés especial de Control Net International definió un procedimiento para el uso en Ethernet del protocolo de aplicación CIP (DeviceNet).
 - **MODBUS TCP/IP:** Es una variante o extensión del protocolo Modbus que permite utilizarlo sobre la capa de transporte TCP/IP. De este modo, Modbus-TCP se puede utilizar en Internet, de hecho, este fue uno de los objetivos que motivó su desarrollo.
 - **SERCOS INTERFACE:** SERCOS III combina los mecanismos en tiempo real establecidos de SERCOS y estandarizó el sistema del parámetro con las comunicaciones universales basadas en Ethernet industrial.
 - **CC-LINK IE:** Es un nuevo estándar para el Ethernet industrial abierto gestionado por la CC-Link Partner Association (CLPA). Su diseño se ha realizado a partir de las exigencias de los fabricantes y de los usuarios de procesos a escala mundial.

3.11.1 ETHERCAT

EtherCAT es el sistema Ethernet de tiempo real para la automatización industrial, se caracteriza por una topología flexible y una manipulación sencilla. Posee un rendimiento extremadamente elevado, que posibilita el control y la regulación de los datos, que no son posibles de realizar con los sistemas clásicos. Debido que junto al puerto Ethernet estándar no se necesita ninguna tarjeta adicional especial, EtherCAT se adapta especialmente a los niveles de control pequeños y medianos.

EtherCAT significa "Ethernet para el Control de Tecnología de automatización." No solo es totalmente compatible con Ethernet, sino que también a través de "by design", le permite integrarse con dispositivos como impresoras y terminales de registros operacionales a través de una conexión con un switch Ethernet. Las tramas Ethernet forman un túnel para pasar a través de EtherCAT, como es habitual en las tecnologías de VPNs, PPPoE, etc. En este caso la red EtherCAT es totalmente transparente, y por lo tanto no se ven afectadas las propiedades de la transmisión en tiempo real.

Se trata de un código abierto, es un sistema de alto rendimiento que pretende utilizar protocolos de Ethernet (el sistema favorecido por las redes de área local) en un entorno industrial. El principio funcional, hace a EtherCAT el sistema más rápido actualmente disponible. Los medios de EtherCAT se satisfacen bien para los ambientes del control puesto que puede funcionar con o sin los switch. EtherCAT es un estándar abierto que se ha publicado como especificación del IEC (Norma IEC/PAS 62407 - IEC 61800-7) basada en el grupo de la tecnología de EtherCAT.

Esta tecnología supera las limitaciones del sistema comparada con otras soluciones de Ethernet. El paquete Ethernet ya no es recibido y copiado como proceso de datos en cada conexión, en lugar de ello el marco Ethernet se procesa sobre la marcha: el recién desarrollado FMMU (campo unidad de gestión de memoria) en cada nodo esclavo, lee los datos que le han dirigido, mientras el telegrama es enviado al dispositivo siguiente. Del mismo modo, los datos de entrada se añaden al telegrama, mientras pasan a través de él, estos solo retrasan la comunicación algunos nanosegundos.

El protocolo EtherCAT utiliza una asignación oficial denominada Ether-type dentro del marco Ethernet. El uso de este Ether-type permite el transporte de los datos de control directamente en el marco de Ethernet sin su redefinición. El marco esta formado por subtelegramas, cada uno ubicado en un área de memoria del proceso lógico, donde el tamaño de las imágenes puede llegar hasta un tamaño de 4 gigabytes. El direccionamiento de los terminales pueden estar en cualquier orden porque la secuencia de datos es independiente del orden físico, por la tanto la comunicación con los esclavos puede ser del tipo broadcast y multicast.

La transferencia directa de datos en el marco Ethernet se utiliza en los casos donde los componentes de EtherCat, operan en la misma red donde se encuentra el controlador maestro y donde el software de control tiene acceso al controlador Ethernet. EtherCAT no se limita solamente a aplicaciones en sistemas de control sino también en el manejo de datagramas UDP/IP, permitiendo a los dispositivos de Ethernet direccionarse con los dispositivos EtherCAT, de otras subredes utilizando un router, cuyo rendimiento dependerá de la comunicación en tiempo real, las características de control y también de la implementación del protocolo Ethernet.

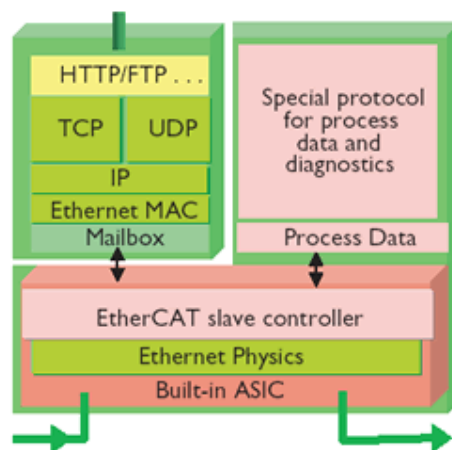


Fig. Nro: 19 Protocolo EtherCAT⁽¹⁹⁾

Soporta varias topologías como ser: bus (Figura Nro: 20), árbol, estrella, línea de buses (E-bus) y anillo, si el dispositivo maestro tiene dos puertos Ethernet, en este caso, si se rompe el anillo el maestro detecta la falla y envía mensajes a los dos nuevos segmentos, continuando con la transferencia de datos en forma interrumpida.

El sistema utiliza como medio de enlace el típico cable UTP Categoría 5, posibilitando también una integración vertical. La utilización de fibra óptica se utiliza en aplicaciones especiales de transporte de datos, para adaptar los distintos tipos de medios se utilizan convertidores de medios de fibra óptica a UTP y para el enlace con los demás dispositivos el típico switch Ethernet adaptado. Si la distancia entre dispositivos a conectar es de 100 metros se utiliza para la transferencia de señales el modo Ethernet 100Base-TX y si la distancia es menor alrededor de los 10 metros el modo E-bus.

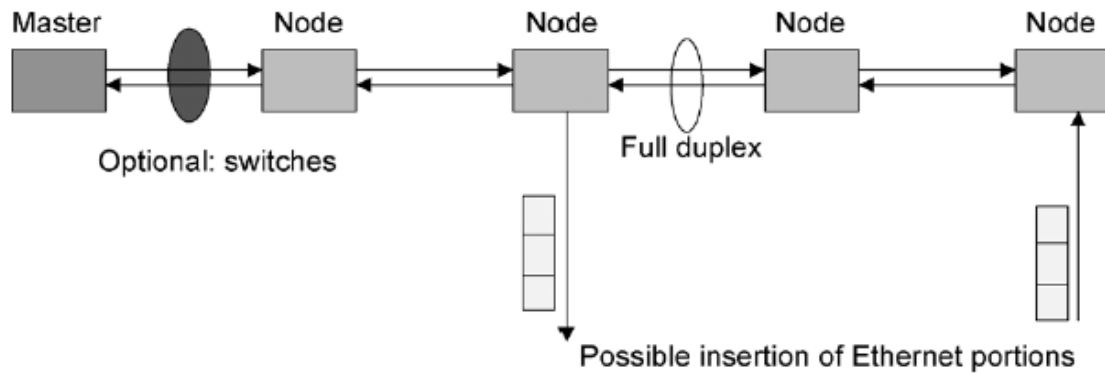


Fig. Nro: 20 Topología bus EtherCAT ⁽²⁰⁾

La tecnología EtherCAT es totalmente compatible con Ethernet, abierta, de muy alto rendimiento y fácil de implementar. Sus capacidades de sincronización y la plena utilización del ancho de banda son muy atractivos para la sincronización de aplicaciones en donde hay un gran número de unidades en movimiento.

Los dispositivos EtherCAT pueden manejar también otros protocolos, en la misma red física, en este caso el switch trabaja como un dispositivo de capa dos que encamina las tramas participantes en función de la información de su dirección. De este modo las diversas tecnologías de Internet, también pueden aplicarse en el entorno EtherCAT, como ser: servidores Web integrados, correo electrónico, transferencia de FTP, etc.

3.11.2 PROFINET (Profibus)

PROFinet es el estándar Industrial Ethernet innovador y abierto (IEC 61158) para la automatización industrial, se desarrolló con el objetivo de favorecer un proceso de convergencia entre la automatización industrial y la plataforma de tecnología de la información de gestión corporativa y redes globales de las empresas. PROFinet se aplica a los sistemas de automatización distribuida basados en Ethernet que integran los sistemas de bus de campo existentes, por ejemplo PROFIBUS, sin modificarlos. Es una solución de automatización distribuida: el modelo de componentes, se divide en módulos tecnológicos. El modelo de E/S de PROFinet contribuye a la integración de periféricos sencillos y a la visualización de componentes y de datos de E/S.

Dependiendo de los requisitos de comunicación y automatización, PROFinet ofrece tres modelos con distintas prestaciones:

- **Modelo TCP/IP y DCOM**, para aplicaciones en las que el tiempo no es crítico.
- **Tiempo Real Flexible (SRT – Soft real Time)**, para aplicaciones típicas de automatización en tiempo real (ciclo de tiempo del orden de los 10 ms.).

La funcionalidad de tiempo real se utiliza para datos de proceso donde el tiempo resulta crítico, es decir, con datos de usuario cíclicos o alarmas controladas por eventos. El protocolo utiliza un canal de comunicación en tiempo real optimizado para las necesidades de tiempo real de los procesos de automatización. De este modo se minimizan los tiempos de ciclo y se mejora el rendimiento a la hora de actualizar los datos de proceso. Las prestaciones son comparables a las de los buses de campo, y se permiten unos tiempos de respuesta de entre 1 y 10 ms, que se observan en la Figura

Nro: 21. Al mismo tiempo se reduce considerablemente la potencia de proceso necesaria en el dispositivo para la comunicación, debido a ello se pueden utilizar componentes de red estándar.

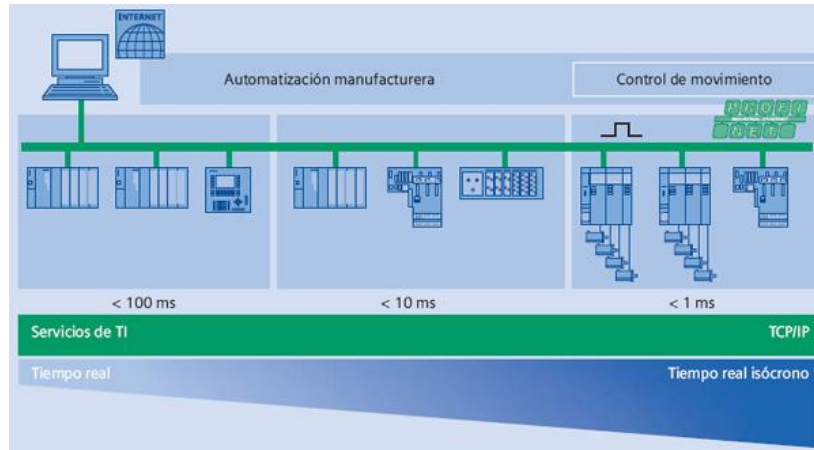


Fig. Nro: 21 Tiempo de respuesta PROFinet ⁽²¹⁾

Los Switch utilizados, permiten una transferencia de datos optimizada, para ello se establecen prioridades en los paquetes de datos según la norma IEE 802.1Q. En función de estas prioridades, los componentes de red controlan el flujo de datos entre los dispositivos. Para los datos transmitidos en tiempo real se utiliza la prioridad 6 (el segundo nivel más alto) como la prioridad estándar. Esto garantiza un tratamiento preferente con respecto a otras aplicaciones que tienen asignados niveles de prioridad más bajos.

- **Tiempo real isócrono (IRT)**, para aplicaciones de control de movimiento (ciclos de 1 ms.).

La comunicación en tiempo real asistida por hardware, conocida como isochronous Real – Time (IRT), esta disponible para aplicaciones especialmente exigentes, como el control de movimiento y aplicaciones de alto rendimiento en automatización manufacturera. Con IRT se consigue un tiempo de ciclo inferior a 1 ms. con una fluctuación de menos de 1 us. Para ello el ciclo de comunicaciones se divide en una parte determinista y otra abierta. Los telegramas IRT cíclicos se transmiten por el canal determinista; los telegramas RT y TCP/IP, por el canal abierto. Por lo tanto, los dos tipos de transmisión de datos coexisten sin interferirse. Por ejemplo, los usuarios pueden conectar un ordenador portátil a cualquier ubicación de la planta para acceder a los datos de los dispositivos sin que esto afecte al control isócrono.

La aceptación de PROFinet depende, entre otras cosas, de si los sistemas de bus de campo existentes pueden o no ampliarse con PROFinet sin incurrir en grandes gastos. Por ejemplo el sistema de bus de campo PROFIBUS puede integrarse de dos formas distintas:

-
- **Integración de unidades de bus de campo a través de proxies:** cada unidad de campo representa un componente PROFinet independiente, cuya comunicación con otros componentes se configura mediante el editor de conexiones de PROFinet. En este caso, el Proxy representa a todas las unidades de campo de la comunicación Ethernet.
 - **Integración de aplicaciones de bus de campo:** el segmento de bus de campo representa un componente PROFinet independiente y cuyo Proxy (por ejemplo, un controlador) incluye una interfaz PROFinet. De este modo se dispone de todas las funciones del bus de campo subordinado como si se tratase de un componente Ethernet.

Normalmente, los sistemas se componen de varios módulos tecnológicos, que funcionan de manera autónoma y se coordinan entre sí mediante un número gestionable de señales de sincronización, control de secuencia e intercambio de información. El modelo de componentes de PROFinet se basa en este tipo de módulos tecnológicos inteligentes, compuestos de una combinación de sistemas mecánicos, electrónicos y programas de usuario, formando las partes de una unidad inteligente. Externamente, la interfaz del componente se define de modo que pueda comunicarse con otros componentes pertenecientes al sistema distribuido.

Desde la interfaz solo se puede acceder a las variables necesarias para interactuar con otros componentes. En el caso de la ingeniería de sistemas, la comunicación con los componentes y sus dispositivos está definida por la interconexión entre las interfaces de los componentes y la aplicación específica.

Los componentes se interconectan con una aplicación a través del editor de conexiones de PROFinet, con solo pulsar el ratón en una librería determinada. Esta interconexión sustituye la dificultosa programación de las relaciones de comunicación por una sencilla configuración gráfica.

El modelo de componentes resulta adecuado para unidades de campo inteligente y controladores programables, y al igual que con PROFIBUS, la visualización de las entradas y salidas, permite acceder a la descripción de las unidades de campo, integrándose con los periféricos distribuidos de PROFinet. La principal función de la integración es para que el programa usuario del PLC procese los datos de entrada y salida de las unidades de campo distribuidas.

PROFinet I/O ofrece las siguientes funciones:

- Transmisión cíclica de datos productivos.
- Transmisión acíclica de alarmas.
- Transmisión acíclica de datos de proceso y de diagnóstico.

La definición de PROFinet I/O se basa en la norma IEC 61158. Esta especificación admite los siguientes requisitos: conversión sencilla de un dispositivo PROFIBUS DP contemporáneo (maestro o esclavo) a un dispositivo PROFinet I/O (controlador de E/S) y, siempre que sea posible, manteniendo la misma visualización de los dispositivos E/S que la disponible en la actualidad con dispositivos esclavos PROFIBUS DP (desde el punto de vista técnico, HMI, programa de usuario, servidor OPC, etc.).

La comunicación en tiempo real flexible (SRT), permite satisfacer las exigencias de tiempo real de la automatización en tiempos de ciclo inferiores a 10 ms., la versión 2 de PROFinet especifica un canal de comunicación en tiempo real optimizado basado en Ethernet (capa 2). Esta solución reduce los tiempos de ejecución de la pila de comunicación y mejora el rendimiento en lo que se refiere a la velocidad de actualización de los datos de automatización.

El tiempo real isócrono (IRT) esta disponible en la versión 3 de PROFinet, así responde a los requisitos de tiempo real estricto de las aplicaciones de control de movimiento (por ejemplo el movimiento de 150 ejes con tiempo de ciclo de 1 ms. y pulsaciones de 1 us.).

PROFinet permite las topologías de red usuales, como ser: estrella, árbol, bus y anillo. Permite aplicaciones WEB en formato HTML o XML. Independiente de las herramientas utilizadas, se puede acceder desde cualquier punto con un navegador de Internet corriente a la información del nivel de automatización, lo cual facilita considerablemente la puesta en marcha y el diagnóstico.

En la Figura Nro: 22, se observa la integración de una red Profinet (profibus), con una red Ethernet industrial y dispositivos de campo.

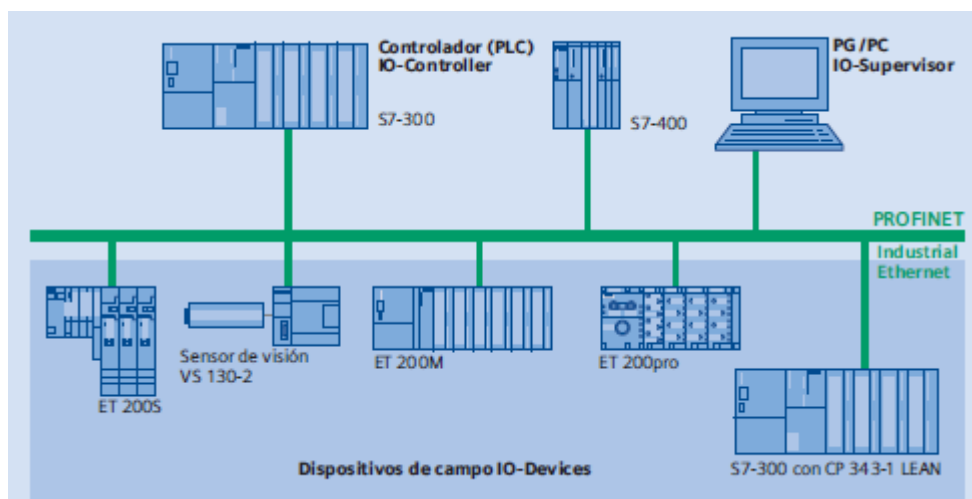


Fig. Nro: 22 Comunicación PROFinet ⁽²²⁾

La seguridad aplica un concepto escalonado, el cual el operario no necesita conocimientos especiales, que excluye en gran medida errores de manejo, acceso indebido y manipulaciones sin obstaculizar la producción, utilizando para ello dispositivos de hardware y software específicos. Utiliza el perfil de PROFIsafe probado en PROFIBUS (según norma de seguridad IEC 61508), que permite la transmisión de datos estándar y de seguridad en un cable de bus, esto permite a PROFinet realizar aplicaciones de seguridad con una configuración homogénea en toda la red, tanto en el diseño de instalaciones nuevas como en la ampliación de las ya existentes. Con la integración de PROFIBUS PA, se abarca la industria de proceso, llegando incluso a áreas clasificadas.

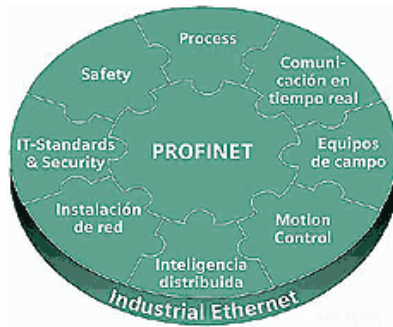


Fig. Nro: 23 Propiedades de PROFinet ⁽²³⁾

3.11.3 ETHERNET POWER LINK

Ethernet **POWERLINK** (conocido también con el acrónimo **EPL**) es un protocolo de comunicaciones en tiempo real basado en hardware estándar Ethernet.

Su principio de funcionamiento hace que el protocolo sea apto para aplicaciones de automatización industrial donde varios elementos de control, por ejemplo: (pantallas de operador, autómatas, módulos de E/S, variadores de frecuencia, servocontroladores, módulos de seguridad, sensores etc.) tengan que comunicarse entre ellos de forma rápida, isócrona y sobre todo precisa (es decir minimizando el tiempo de latencia de la red, garantizando desde luego que el proceso de comunicación sea fiable y repetitivo. **POWERLINK** no es un hardware, es un software que funciona sobre un hardware estándar.

En la siguiente Figura, se observa la relación de las capas del modelo OSI y Ethernet PowerLink.

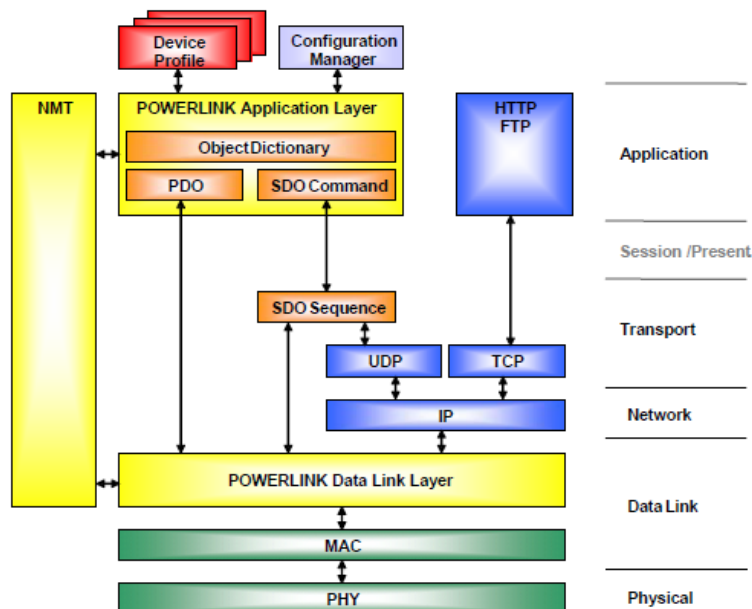


Fig. Nro: 24 Ethernet PowerLink y modelo OSI ⁽²⁴⁾

POWERLINK es un protocolo determinista de tiempo real de Ethernet, el objetivo del desarrollo consiste en aplicar la tecnología Ethernet estándar a la ingeniería de automatización, en condiciones de tiempo real adversas.

En una red Ethernet TCP/IP cada nodo decide de forma autónoma cuando escribir datos en la red. Esta “anarquía” es una posible causa de colisiones: si dos (o más) estaciones deciden al mismo tiempo acceder a la red se genera una colisión. Para evitarla, existe un mecanismo llamado CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) que hace que las estaciones retrasen su intento y vuelvan a intentar a escribir en la red después de un tiempo aleatorio. Esta forma de actuar lleva una desventaja: es imposible prever con exactitud cuando (o dentro que plazo de tiempo) llegará la información que se está esperando. En casos extremos (muy hipotéticos pero no imposibles) ésta podría no llegar nunca. Una funcionalidad de este tipo resulta inaceptable en automatización industrial, donde es fundamental poder contar con una comunicación fiable, repetitiva, rápida, sincronizada y sin retrasos. En Ethernet **POWERLINK** no hay colisiones, en cuanto todo está regulado por un nodo manager (MN - *Managing Node*) que gestiona la comunicación entre los varios nodos de control (CN - *Control Node*). El MN sincroniza todos los CN entre ellos por medio de una señal de reloj que se repite con una precisión inferior a 100 ns (tiempo de latencia), y que constituye el tiempo de ciclo. Durante cada ciclo, el MN envía a cada CN una petición de envío de sus datos (*Poll Request*). Los CN contestan inmediatamente a las peticiones (*Poll Response*) enviando sus datos a la red en forma de broadcast, para que todos los demás CN (y el mismo MN) los puedan escuchar sin que el MN tenga que hacer de pasarela.

Más en detalle, un ciclo de comunicación de **POWERLINK** consta de tres fases:

1. durante el *Start Period* el MN envía un *Start of Cycle* (SoC) a todos los CN para sincronizarlos.
2. el segundo periodo (*Cyclic Period*) sirve para el intercambio isócrono de los datos entre los nodos de la red.
3. finalmente el último periodo está reservado para la transmisión de datos asíncronos que no son críticos en el tiempo (*Acyclic Period*).

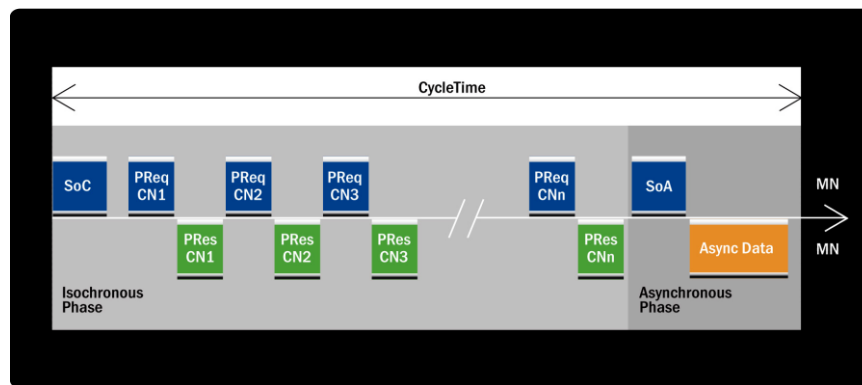


Fig. Nro: 25 Modelo del mecanismo *time-slot*. Un ciclo de comunicación consta de una parte en tiempo real con peticiones directas (*Poll Request*), respuestas de los nodos (*Poll Response*) y una parte asíncrona para los datos no cíclicos y no críticos.
(25)

Este mecanismo, llamado SCNM (*Slot Communication Network Management*), permite alcanzar tiempos de ciclos de unos cien microsegundos, durante los cuales varias estaciones tienen la posibilidad de enviar a la red sus datos. Además este sistema admite también la transmisión de datos asíncronos (por ejemplo tramas TCP/IP encapsuladas o datos de servicio, diagnóstico, debug) durante el mismo tiempo de ciclo. Esta tabla indica el número de estaciones que pueden comunicarse en un tiempo de ciclo:

- Redirección.
- Tiempo de ciclo Nr. nodos* 200 μ s 9 400 μ s 21 800 μ s 45

(*)Tramas de 46 byte/nodo, topología árbol

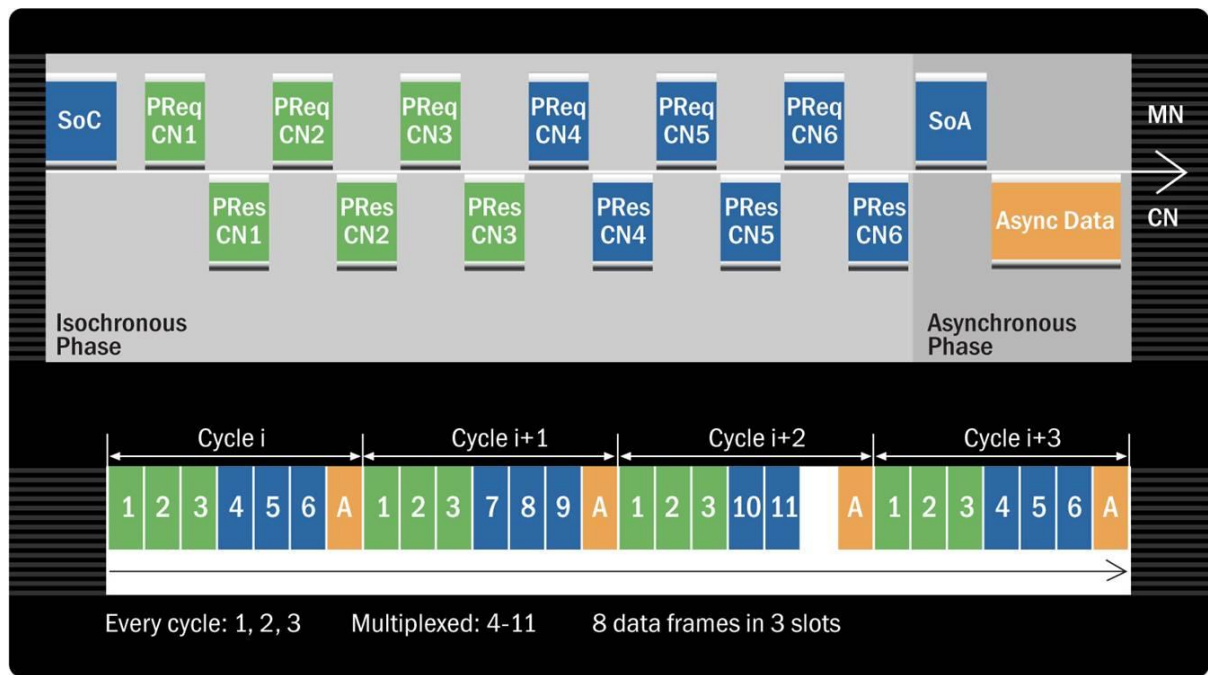


Fig. Nro: 26 Ejemplo de comunicación en POWERLINK donde las estaciones 1, 2 y 3 tienen prioridad máxima y envían datos cada ciclo. Las estaciones de 4 a 10 comparten 3 slots de comunicación y envían sus datos solo cada 3 ciclos de comunicación. ⁽²⁶⁾

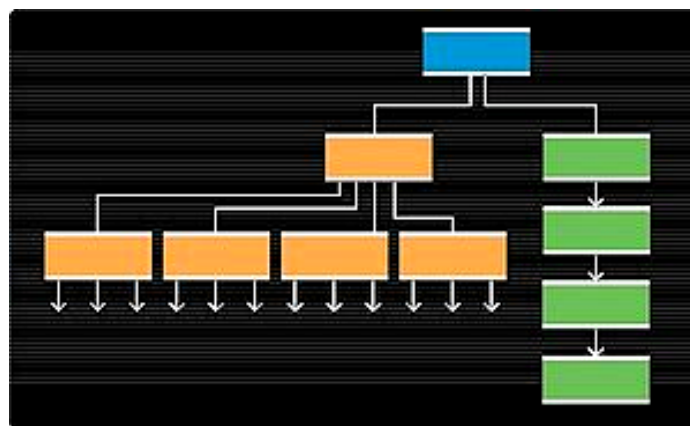
POWERLINK prevé también la posibilidad de multiplexar los nodos de más baja prioridad, con el fin de optimizar la comunicación. Por ejemplo, si en una red hay un eje maestro M1 que tiene que enviar su posición y su velocidad a tres ejes esclavos S1, S2 y S3, es importante que éste envíe sus datos cada ciclo de comunicación; la información proporcionada por los esclavos tiene prioridad más baja y puede ser más lenta. Por esto es posible configurar el bus de forma que los tres esclavos de éste ejemplo compartan alternativamente el mismo eslot de comunicación.

La comunicación resulta entonces:

- Ciclo i: el maestro M1 envía sus datos (posición, velocidad, estado etc.); el esclavo S1 también. Los esclavos S2 y S3 no envían nada.
- Ciclo i+1: el maestro M1 y el esclavo S2 envían sus datos; los esclavos S1 y S3 no envían nada.

- Ciclo $i+2$: el maestro M1 y el esclavo S3 envían sus datos; los esclavos S1 y S2 no envían nada.
- Ciclo $i+3$: igual que el ciclo i .

El protocolo **POWERLINK** admite topologías en estrella, anillo y árbol (mostrado en la Figura Nro: 27), en las redes estrella se utiliza Fast Ethernet, donde se utiliza cable UTP categoría 5, por lo tanto su longitud máxima es de 100 metros, para conexiones donde la red esta expuesta a gran interferencia electromagnética se usa fibra óptica, permitiendo alcances mayores. Estas topologías utilizan como medio de conexión a los switch, por lo tanto no se producen colisiones, para extender su alcance se conectan switch en cascada, permitiendo un máximo de 10 switch. Normalmente las unidades de campo disponen de un concentrador integrado aplicado a su estructura.



Recuadros: (verde- naranja y celeste). Son nodos (switches) de conexión.

Fig. Nro: 27 Topología Arbol PowerLink⁽²⁷⁾

El objetivo del desarrollo de Ethernet Powerlink consiste en aplicar la tecnología Ethernet estándar a la ingeniería de automatización, en condiciones de tiempo real adversas. Además de utilizar los componentes comercialmente disponibles y de garantizar un intercambio de datos transparente en todos los niveles de red, se pretende garantizar una respuesta predecible en el tiempo para las comunicaciones entre las diferentes secciones del sistema.

El concepto consiste en conectar todos los dispositivos a la red, desde el control en lazo abierto hasta los sistemas de control y actuador, pasando por el nivel de entradas y salidas, mediante una conexión Ethernet estándar en condiciones de tiempo críticas o convencionales. En ambos casos debe existir compatibilidad con los servicios de Internet más extendidos, como navegadores o intercambio de archivos vía ftp.

El uso deseado de Ethernet Powerlink en la automatización de equipos y sistemas permite considerar el intercambio de datos prioritarios en una red local de manera aislada. La conexión a la red empresarial tradicional puede realizarse mediante un puente. Con esta separación se evitan colisiones imprevisibles con dispositivos que no disponen de Ethernet Powerlink. En los casos en los que se opera con un tiempo real reducido, los dispositivos Ethernet Powerlink también pueden funcionar en red sin esta separación.

El intercambio de datos se organiza de manera estricta mediante procedimientos de ventanas temporales o Slot Communication Network Management (SCNM). Las pilas de comunicación del protocolo TCP/UDP/IP se sustituyen por las pilas en tiempo real de Powerlink. Una de las estaciones de la red Ethernet Powerlink asume la función de administrador, controlando las comunicaciones y determina la hora de reloj para la sincronización de todos los usuarios. El resto de las estaciones (controladores) sólo pueden realizar envíos si reciben autorización del administrador. Todas las demás estaciones pueden recibir los datos (emisión). El intercambio de datos en la red se realiza de manera determinista mediante ciclos isócronos. El administrador puede configurar el tiempo del ciclo.

Con la SCNM, el número de usuarios que como máximo pueden conectarse a la red Ethernet Powerlink depende del tiempo de ciclo establecido. No obstante, no suele ser necesario que todos los usuarios envíen datos prioritarios en cada ciclo. Por ejemplo, en el caso de una conexión controlador/ actuador, el eje master transmite las variables de posición y referencia de cada ciclo que, normalmente, serán recibidas por un eje esclavo que sólo ocasionalmente necesitará enviar su propia información de estado. Por lo tanto, en Ethernet Powerlink se definen dos tipos de usuarios:

Clase 1, Cíclico: el usuario realiza un envío en cada ciclo,

Clase 2, preescalado: el usuario realiza un envío cada n ciclos.

Es posible programar el número máximo de intervalos de clase 2 por ciclo, que está condicionado por el ciclo de tiempo y el número de estaciones de clase 1. Por este motivo, el resultado es un ciclo "preescalado". Ethernet Powerlink en un sistema conectado en red a través de Internet El uso de Ethernet en la automatización tiene como principal finalidad aportar flexibilidad y comunicación universal desde el nivel de coordinación al de E/S, sin limitaciones geográficas o de sistema mediante el uso del protocolo de Internet (IP).

La implementación de Ethernet Powerlink también responde a los siguientes requisitos: comunicación cíclica y acíclica mediante Ethernet Powerlink transmisión y recepción transparentes de la parte acíclica de las tramas estándar de Ethernet, de modo que todos los protocolos y aplicaciones de alto nivel, como TCP o UDP puedan utilizarlo sin modificaciones. Además, puede utilizarse una estación Ethernet Powerlink a través de una red Ethernet convencional mediante la misma conexión en el modo básico de Ethernet. Esto resulta útil en el caso de aplicaciones no prioritarias, como la programación, la asignación de parámetros y las pruebas de los dispositivos. Actualmente se está trabajando en un modo Ethernet Powerlink adaptado a condiciones de tiempo real menos exigentes.

El uso de Ethernet en la automatización tiene como principal finalidad aportar flexibilidad y comunicación universal desde el nivel de coordinación al de E/S, sin limitaciones geográficas o de sistema y mediante el uso del protocolo IP. Su implementación responde a los siguientes requisitos: comunicación cíclica y acíclica mediante Ethernet PowerLink, transmisión y recepción transparentes de la parte acíclica de las tramas estándar de Ethernet, de modo que todos los protocolos y aplicaciones de alto nivel, como TCP o UDP puedan utilizarlo sin modificaciones. Además puede utilizarse una estación PowerLink a través de una red Ethernet convencional mediante la misma conexión al medio básico.

Utiliza como protocolo de seguridad a Ethernet PowerLink Safety (EPLsafety), que fueron diseñados por un grupo de trabajo independiente. Todos los mecanismos de seguridad, se aplican a toda la red, se integra con hardware estándar y se comunica en tiempo real por medio de un único bus Ethernet PowerLink, compartiendo este mismo bus con los equipos y los módulos que no integran el plan de seguridad. Esta solución cumple con todos los requisitos marcados por la normativa IEC 61508 SII cat 3, utilizada en el sector de automatización. La tecnología de Ethernet PowerLink Safety es independiente del protocolo de transmisión de datos.

3.11.4 ETHERNET IP

Otro de los protocolos utilizados en las redes Ethernet Industrial es Ethernet/IP (DeviceNet) basado en las normas IEEE 802.3, IEC 61158 y IEC 61784. Es una red abierta y compatible con la tradicional familia TCP/IP. Este protocolo permite el uso de aplicaciones de control con el protocolo de control e información CIP, utilizado como protocolo de aplicación para E/S en tiempo real.

El protocolo CIP ofrece una amplia gama de servicios estándar para acceder a los datos y controlar los dispositivos conectados a la red a través de mensajes “implícitos” y “explícitos”.

CIP utiliza mensajes implícitos para regular el intercambio de datos cíclicos en los que las estaciones implicadas están al tanto de los datos que se esperan: bloques de datos puros muy compactos con muy poca cabecera, datos típicos de E/S a través de conexiones de E/S. Todos los mensajes individuales que se envían por única vez utilizan el tipo explícito asociado, por ejemplo, todos los mensajes pregunta-respuesta entre el cliente y el servidor.

Fundamentalmente, Ethernet/IP puede considerarse como la ampliación industrial de Ethernet TCP/IP, puesto que los mensajes CIP de la capa de aplicación se “empaquetan”, mediante encapsulación, en las tramas TCP/IP como datos de usuario. De este modo, una aplicación puede enviar sus datos a otra aplicación a través de Ethernet; en caso necesario, la aplicación genera automáticamente un mensaje CIP y lo encapsula para convertirlo en un paquete TCP/IP, algo similar a introducir una carta en un sobre. Este mensaje empaquetado se envía a través de Ethernet hasta el dispositivo de destino en el que, una vez recibido, el protocolo TCP/IP lo vuelve a enviar al protocolo de encapsulación para “desempaquetar” el mensaje original CIP (sacarlo del sobre) y volver a enviarlo, a través del protocolo CIP, hasta la aplicación receptora. En principio, es posible establecer este tipo de enlace de aplicación entre todos los usuarios del protocolo de aplicación CIP, incluso si proceden de distintos fabricantes o están ubicados en redes diferentes.

Esto significa que a través de TCP/IP, Ethernet/IP puede enviar “mensajes explícitos”, que es el nombre que reciben los mensajes a modo de telegramas que contienen información e instrucciones sobre el protocolo que necesita para su posterior utilización en el campo de datos. El receptor debe interpretar los mensajes explícitos como instrucciones, ejecutarlas y generar una respuesta. Este modo versátil de intercambio de datos se utiliza, por ejemplo, para la configuración, programación y diagnóstico de dispositivos con cantidades variables de datos. Para llevar a cabo esta transferencia de mensajes se utiliza el protocolo TCP.

En la Figura, se observa la comparación del modelo Ethernet IP, con las capas del modelo OSI.

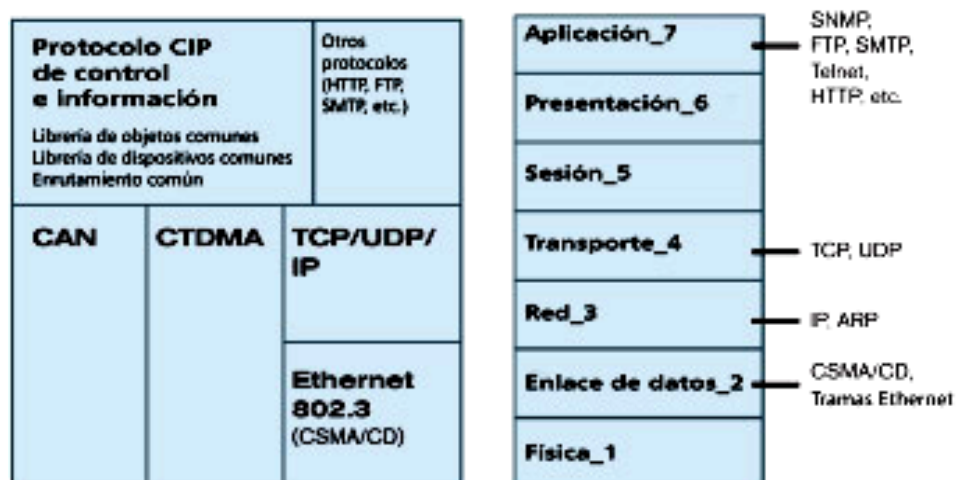


Fig. Nro: 28 Comparación con el modelo OSI ⁽²⁸⁾

No obstante, la comunicación en tiempo real impone requisitos algo distintos. En ese caso, Ethernet/IP no utiliza el protocolo TCP sino UDP vía IP (Internet Protocol). Básicamente, este protocolo resulta más compacto, por lo que es compatible con los denominados mensajes “multidifusión” (recepción simultánea por varios usuarios) y puede ser utilizado por Ethernet/IP para el envío de los denominados “mensajes implícitos”. En este tipo de mensajes telegráficos, los campos de datos ya no incluyen la información de protocolo sino sólo datos de entrada y salida en tiempo real. La aplicación receptora ya conoce cómo debe interpretar estos datos, puesto que ya lo ha negociado durante la configuración de la conexión. Es decir, que los telegramas implícitos se envían a través de una conexión virtual existente entre los usuarios y se actualizan de manera constante y cíclica en cortos intervalos de tiempo con señales de E/S y datos recientes y actualizados. En este caso la cabecera es mínima, a fin de que los mensajes se procesen muy rápidamente y con prioridad (ese es justamente el requisito de las tareas de control en las que el tiempo es crítico).

En consecuencia, Ethernet/IP combina el protocolo TCP/IP y los telegramas de datos UDP/IP para el transporte de paquetes de mensajes explícitos e implícitos, lo que significa que, en este caso, tanto los datos de entrada y salida en tiempo real para las tareas de control prioritarias (UDP) como los datos de información (TCP) de una red pueden utilizarse en paralelo.

Por consiguiente, Ethernet/IP resulta ideal para las tareas de control de E/S, configuración y diagnóstico, y para la adquisición de datos en entornos industriales, especialmente si se tiene en cuenta la interoperabilidad e intercambiabilidad de un protocolo internacional de automatización.

Dado que ControlNet, DeviceNet y Ethernet/IP utilizan el mismo protocolo de aplicación, también pueden acceder a perfiles de dispositivos y librerías de objetos compartidos. Gracias a estos objetos es posible la interoperabilidad plug & play de dispositivos complejos de fabricantes diferentes. Las definiciones de los objetos son compatibles con la transmisión en tiempo real de mensajes de E/S, la configuración, el

diagnóstico y la adquisición de datos a través de una misma red. Así, el usuario puede establecer fácilmente enlaces de comunicación con dispositivos inteligentes, tipo unidad/actuador y controles de robots, lectores de códigos de barras, sistemas de pesaje, etc., sin tener que recurrir a herramientas de software específicas. El resultado es una mayor rapidez en línea y una completa compatibilidad de diagnóstico.

Asimismo, Ethernet/IP permite combinar la transmisión de datos acíclicos (mensajes explícitos) con los datos de control transmitidos cíclicamente (mensajes implícitos). Gracias a las características fabricante/consumidor que garantiza el protocolo de control e información CIP, ahora Ethernet/IP es compatible con los principales mecanismos de comunicación para la conexión en una red de dispositivos, desde la interrogación secuencial hasta la activación en función del tiempo o de un evento, pasando por la multidifusión o las conexiones punto a punto para el acoplamiento de datos.

Por último, también es importante la aceptación de ControlNet y DeviceNet, ya que en la actualidad cerca de 400 fabricantes de todo el mundo han desarrollado más de 500 productos diferentes para estas redes. La combinación y complementación de estas redes produce prácticamente un único sistema universal (misma capa de aplicación), además del considerable apoyo de este grupo de fabricantes a Ethernet/IP.

Solamente EtherNet/IP con tecnología CIP Motion combina los requisitos de un control de movimiento de bucle cerrado determinista y en tiempo real con Ethernet estándar, ofreciendo un cumplimiento total de las normas de Ethernet, incluyendo IEEE 802.3 y TCP/IP.

EtherNet/IP con la tecnología CIP Motion proporciona una solución abierta, con un gran ancho de banda y gran rendimiento para el control del movimiento distribuido multieje. CIP Motion es una extensión de CIP (Common Industrial Protocol) que proporciona la capacidad necesaria para un movimiento sincronizado multieje de gran rendimiento. CIP Motion comprende una serie de perfiles de aplicación diseñados para permitir la configuración en un mecanismo de los bucles de posicionamiento, velocidad y par. Esto se combina con la tecnología CIP Sync de ODVA: sincronización de reloj de precisión conforme a IEEE-1588, encuadrado en el modelo de objeto CIP.

EtherNet/IP con CIP Motion permite que se puedan coordinar varios ejes para un control de movimiento con precisión sincronizado. Más aun, EtherNet/IP con CIP Motion es una solución dimensionable y completa que proporciona una interfaz y unos servicios de aplicación común para propósito general y mecanismos de control de movimiento utilizando el mismo perfil. EtherNet/IP con CIP Motion son compatibles con las topologías de Ethernet estándar como estrella y árbol.

El problema de determinismo podría parecer que descarta a Ethernet estándar sin modificar para el control de movimiento, pero ODVA ha superado esta limitación con EtherNet/IP sin tener que cambiar ninguna de las cuatro capas inferiores de Ethernet, utilizando Ethernet estándar sin modificar y TCP/UDP/IP. EtherNet/IP con CIP Motion resuelve el problema cambiando la estrategia de determinismo. Elimina el requisito de un determinismo estricto en la infraestructura de red y confía en los dispositivos finales la información de sincronización necesaria para

manejar las necesidades de control en tiempo real de la aplicación, esto permite la coordinación de 100 ejes con una actualización de red de 1 ms. para todos los ejes.

Respecto a la seguridad, CIP Safety proporciona integridad mediante el uso de un amplio conjunto de medidas de protección aprobadas por el organismo alemán TÜV. Garantiza la integridad de la transmisión al detectar errores de comunicación y permite la integridad de las aplicaciones al permitir a los dispositivos tomar las medidas apropiadas. En la mayoría de las aplicaciones, cuando se detecta un error el dispositivo entra en un estado de ausencia de energía, normalmente denominado estado de seguridad. El código de seguridad de cada dispositivo es el encargado de detectar estos errores de comunicación y se ejecuta en una sección de alta integridad de dispositivos de seguridad que normalmente emplea hardware redundante, con la aprobación de una agencia de certificación.

En la Figura Nro: 29, se muestra la comparación del modelo Ethernet/IP, con los protocolos industriales: CompoNet, ControlNet y DeviceNet.

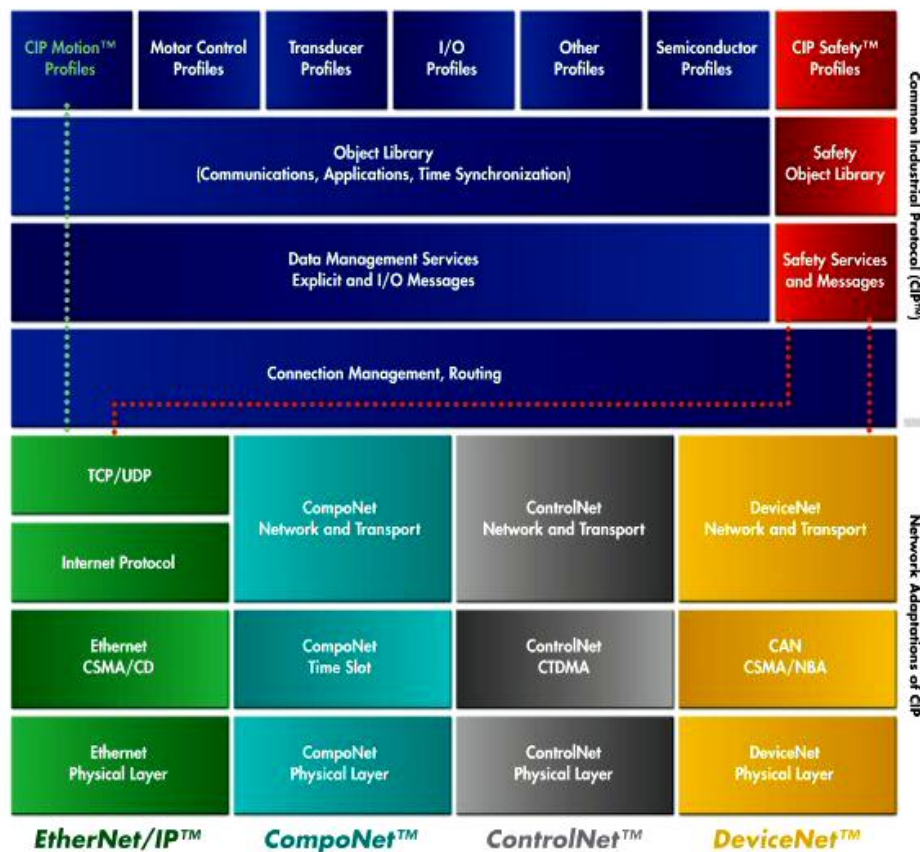


Fig. Nro: 29 Comparación del Protocolo Ethernet/IP con otros protocolos industriales ⁽²⁹⁾

El modelo completo de Ethernet/IP puede verse como un concepto autónomo, diferente a la estructura completa de 3 niveles utilizados por los otros protocolos, ya que la infraestructura se la considera como una sola y de hecho puede representarse en su conjunto por un único modelo de 7 capas, por más que los niveles inferiores sigan usando otras redes o buses. Este modelo posibilita la integración desde el nivel de proceso hasta la red comercial de la empresa.

En la práctica significa que la capa de aplicación “ve” y permite configurar todos los dispositivos de la red desde un único software, para ello utiliza un protocolo especial denominado **CIP (Control e Information Protocol)**, explicado anteriormente, el cual se encarga de organizar todos los mecanismos de red como una colección de objetos a los que llama “Perfiles de dispositivos”, sobre los cuales define propiedades, accesos y atribuciones. Estos perfiles luego pueden ser reutilizados en la creación de nuevos recursos.

3.11.5 MODBUS TCP/IP

Modbus/TCP es un protocolo de comunicación diseñado para permitir a equipos industriales tales como Controladores Lógicos Programables (PLCs), computadores, motores, sensores, y otros tipos de dispositivos físicos de entrada/salida comunicarse sobre una red. Modbus/TCP fue introducido por Schneider Automation como una variante de la familia MODBUS ampliamente usada, los protocolos de comunicación son simples y abiertos, destinados para la supervisión y el control de equipo de automatización. Específicamente, el protocolo cubre el uso de mensajes MODBUS usando los protocolos TCP/IP en un entorno de Intranet, o, Internet.

Posee las siguientes ventajas:

- Es escalable en complejidad. Un dispositivo que tiene simplemente un solo propósito, necesita solo implementar uno ó dos tipos de mensaje.
- Es simple para administrar y expandir. No se requiere usar herramientas de configuración complejas cuando se añade una nueva estación a la red Modbus/TCP.
- No se necesita equipo o software propietario específico. Cualquier sistema computador o microprocesador con una pila de protocolos TCP/IP puede usar Modbus/TCP.
- Puede ser usado para comunicarse con una gran base instalada de dispositivos MODBUS, usando productos de conversión, los cuales no requieren configuración.
- Es de muy alto desempeño, limitado típicamente por la capacidad del sistema operativo del computador para comunicarse. Puede lograr altas tasas de transmisión sobre una estación única, y las redes construidas pueden lograr tiempos de respuesta en el rango de los milisegundos.
- Se puede acceder a la red para efectuar, reparaciones o mantenimiento remoto desde la oficina utilizando una PC, reduciendo así los costos y mejorando el servicio al cliente.
- Los ingenieros de mantenimiento pueden entrar al sistema de control de la planta desde sus casas, evitando desplazamientos.
- Permite realizar la gestión de sistemas distribuidos geográficamente mediante el empleo de las tecnologías de Internet/Intranet.

MODBUS TCP/IP se ha convertido en un estándar industrial *de facto* debido a su simplicidad, bajo costo, necesidades mínimas en cuanto a componentes de hardware, y sobre todo a que se trata de un protocolo abierto. En la actualidad hay cientos de dispositivos MODBUS TCP/IP disponibles en el mercado. Se emplea para intercambiar información entre dispositivos, así como monitorizarlos y gestionarlos. También se

emplea para la gestión de entradas/salidas distribuidas, siendo el protocolo más popular entre los fabricantes de este tipo de componentes.

La combinación de una red física versátil y escalable como Ethernet con el estándar universal de interredes TCP/IP y una representación de datos independiente de fabricante, como MODBUS, proporciona una red abierta y accesible para el intercambio de datos de proceso.

Modbus/TCP simplemente encapsula una trama Modbus en un segmento TCP. TCP proporciona un servicio orientado a conexión fiable, lo que significa que toda consulta espera una respuesta.

3.11.5.1 ESTRUCTURA DEL PROTOCOLO

Describiré a continuación la forma general de encapsulación de una solicitud o respuesta de Modbus cuando es llevado sobre una red Modbus/TCP.

Todas las solicitudes son enviadas vía TCP sobre el puerto registrado 502 y en forma half-duplex, sobre una conexión establecidas. Es decir, no hay beneficio en enviar solicitudes adicionales sobre una única conexión mientras una respuesta esta pendiente, sin embargo, los dispositivos que deseen obtener altas tasas de transferencia puede establecer múltiples conexiones TCP al mismo destino.

El campo “dirección esclavo” de Modbus es reemplazado por un byte “identificador de unidad” el cual puede ser usado para comunicarse con dispositivos tales como: puentes y Gateway, los cuales usan una dirección IP única para soportar múltiples unidades terminales independientes.

Los mensajes de solicitud y respuesta en Modbus/TCP, poseen un prefijo o encabezado compuesto por seis bytes como se aprecia en la siguiente tabla:

Ref	Ref	00	00	00	len
-----	-----	----	----	----	-----

Tabla Nro: 1 estructura del prefijo de Modbus/TCP

El campo de referencia de transacción está representado por los dos bytes “Ref Ref”, es un número que no tiene valor en el servidor pero son copiados literalmente desde la solicitud a la respuesta a conveniencia del cliente. Este campo se utiliza para que un cliente Modbus/TCP pueda establecer simultáneamente múltiples conexiones con diferentes servidores y pueda identificar cada una de las transacciones.

El tercero y cuarto campo del prefijo representan el identificador del protocolo, un número el cual debe ser establecido en cero. El campo “len”, especifica el número de bytes que siguen. La longitud es una cantidad de dos bytes, pero el byte más alto vale cero, ya que los mensajes son más pequeños que 256.

De esta forma, un mensaje Modbus/TCP completo posee una estructura como se muestra en la siguiente tabla.

POSICION DEL BYTE	SIGNIFICADO
Byte 0	Identificador de transacción. Copiado por el servidor- normalmente 0.
Byte 1	Identificador de transacción. Copiado por el servidor – normalmente 0
Byte 2	Identificador de protocolo = 0
Byte 3	Identificador de protocolo = 0
Byte 4	Campo de longitud (byte alto)= 0. Ya que los mensajes son menores a 256
Byte 5	Campo de longitud (byte bajo). Numero de bytes siguientes.
Byte 6	Identificador de unidad (previamente “dirección esclavo”).
Byte 7	Código de función Modbus.
Byte 8 y mas	Los datos necesarios.

Tabla Nro: 2 Estructura del mensaje Modbus/TCP

En la Figura Nro: 30 se observa el encapsulamiento de la trama Modbus en el protocolo TCP.

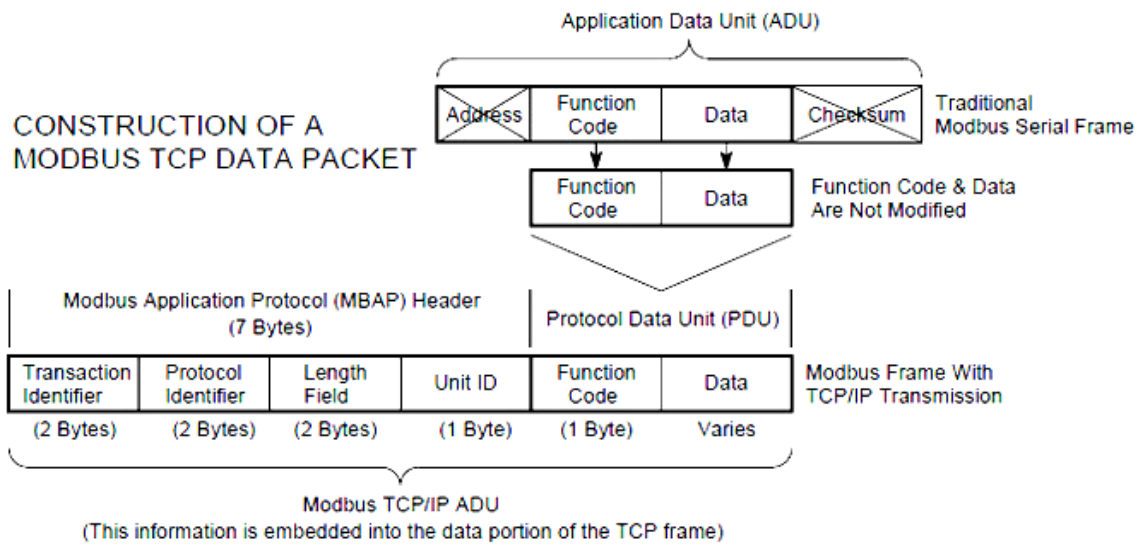


Fig. Nro: 30 Encapsulamiento de la trama Modbus en TCP ⁽³⁰⁾

Esta técnica de consulta/respuesta va perfectamente con la naturaleza Maestro/Esclavo de Modbus, añadido a la ventaja del determinismo que las redes Ethernet conmutadas ofrecen a los usuarios en la industria. El empleo del protocolo abierto Modbus con TCP proporciona una solución para la gestión desde unos pocos a decenas de miles de nodos.

Las prestaciones dependen básicamente de la red y el hardware. Si se usa MODBUS TCP/IP sobre Internet, las prestaciones serán las correspondientes a los tiempos de respuesta de Internet, que no siempre serán los deseables para un sistema de control. Sin embargo pueden ser suficientes para la comunicación destinada a depuración y mantenimiento, evitando así desplazamientos al lugar de la instalación. Si disponemos de una Intranet de altas prestaciones con conmutadores Ethernet de alta velocidad, la situación es totalmente diferente. En teoría, MODBUS TCP/IP, transporta datos hasta $250/(250+70+70)$ o alrededor de un 60% de eficiencia cuando se transfieren registros en bloque, y puesto que 10 Base T proporciona unos 1.25 Mbps de datos, la velocidad de transferencia de información útil será:

$$1.25M / 2 * 60\% = 360000 \text{ registros por Segundo}$$

En 100BaseT la velocidad es 10 veces mayor.

Esto suponiendo que se están empleando dispositivos que pueden dar servicio en la red Ethernet aprovechando todo el ancho de banda disponible. En los ensayos prácticos realizados por by Schneider Automation utilizando un PLC Ethernet Momentum™ con entradas/salidas Ethernet, demostró que se podían escanear hasta 4000 bloques I/O por segundo, cada uno con hasta 16 I/O analógicas de 12-bits o 32 I/O digitales (se pueden actualizar 4 bases por milisegundo). Aunque estos resultados están por debajo del límite teórico calculado anteriormente, pero debemos recordar que el dispositivo se probó con una CPU de baja velocidad (80186 a 50MHz con 3 MIPS). Además, el abaratamiento de los ordenadores personales y el desarrollo de redes Ethernet cada vez más rápidas, permite elevar las velocidades de funcionamiento, a diferencia de otros buses que están inherentemente limitados a una sola velocidad.

Puesto que MODBUS TCP/IP es simplemente un protocolo MODBUS encapsulado en TCP, es muy sencillo comunicar dispositivos MODBUS existentes sobre MODBUS TCP/IP. Para ello se requiere una pasarela que convierta el protocolo MODBUS a MODBUS TCP/IP.

3.11.6 SERCO III

SERCOS III (Serial Real-Time Communication System), definido por la norma IEC 61158/61784, y creado por el conjunto de empresas Rockwell, Bosch Rexroth, ABB y Siemens, combina los mecanismos de tiempo real establecidos por Sercos y los parámetros de comunicaciones basado en Ethernet Industrial. Es utilizado en la sincronización de equipos informáticos en movimiento, tales como maquinas herramientas multiaxiales, línea de impresoras electrónicas y empaquetadoras. Los paquetes de datos de SERCOS III se transmiten en paralelo con otros datos que no son de tiempo real.

SERCOS se ha optimizado para aplicaciones de alta velocidad determinista en sistemas de control de movimiento, que necesitan sincronizar exactamente varias unidades. Define una gran variedad de perfiles de control de movimiento para dispositivos de E/S, que en conjunto con Ethernet Industrial, resulto exitoso en múltiples aplicaciones industriales.

SERCOS utiliza Ethernet TCP/IP, en los buses de control de movimiento y como medio de transporte el económico cable de par trenzado de cobre (UTP), y en aplicaciones especiales en ambientes ruidosos utiliza fibra óptica.

La estructura de SERCOS, permite el enlace con la red de comunicaciones existente. Tiene una alta inmunidad al ruido, en función de los medios utilizados (UTP y Fibra Óptica). Las topologías utilizadas en las redes SERCOS son la de anillo o en línea, la utilización de topologías en anillo doble permite a los maestros y a los esclavos permanecer constantemente en contacto aunque se rompa un anillo. La tecnología de comunicación basada en IEEE 802.3, le permite tasas de transmisión de datos de 100 MBit/s, y libre de colisiones. Presenta diferencias con la Ethernet estándar, ya que los marcos son procesados por los esclavos, y estos insertan los datos en la trama cuando pasa a través de ellos.

SERCOS III - highly flexible and open for all types of communication

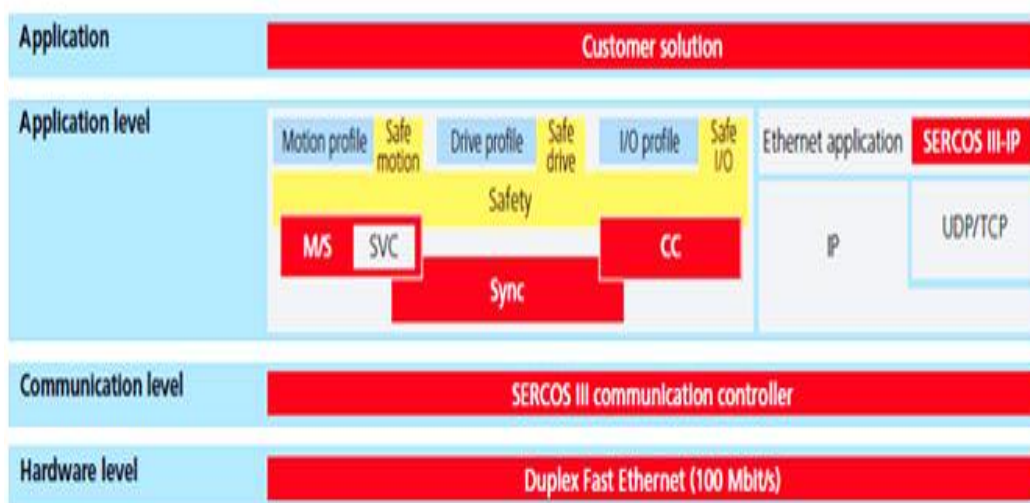


Fig. Nro: 31 Modelo de capas SERCOS III⁽³¹⁾

Las características más sobresalientes son las siguientes:

- Ciclo de tiempo mínimo de 31,25 us, con una fluctuación en torno a los nanosegundos.
- El protocolo es altamente eficiente y le permite manejar un alto número de esclavos con tiempo de ciclos cortos.
- Transmisión en paralelo de tramas de datos de tiempo real y no tiempo real.
- Sincronización de múltiples maestros.
- Permite conectar en caliente a los esclavos.
- Aumento de la seguridad de comunicación con cableado redundante (anillo doble).
- Utilización de TCP/IP, permitiéndole simplificar las configuraciones y operaciones de diagnóstico de la red.

Con respecto a la seguridad utiliza CIP Safety, que es un protocolo utilizado para transferir datos seguros sobre la interfaz SERCOS. En conjunto con ODVA, ha sido certificado para el cumplimiento con las normas IEC 61508 y SIL 3. Para la transmisión de datos seguros no hace falta un bus adicional, ya que estos se envían sobre la interfaz SERCOS en tiempo real.

En la Figura Nro: 32 se puede observar la integración de una red Ethernet Industrial con una red Sercos III, formada por dispositivos master (PLC) y esclavos (sensores, actuadores, etc.).

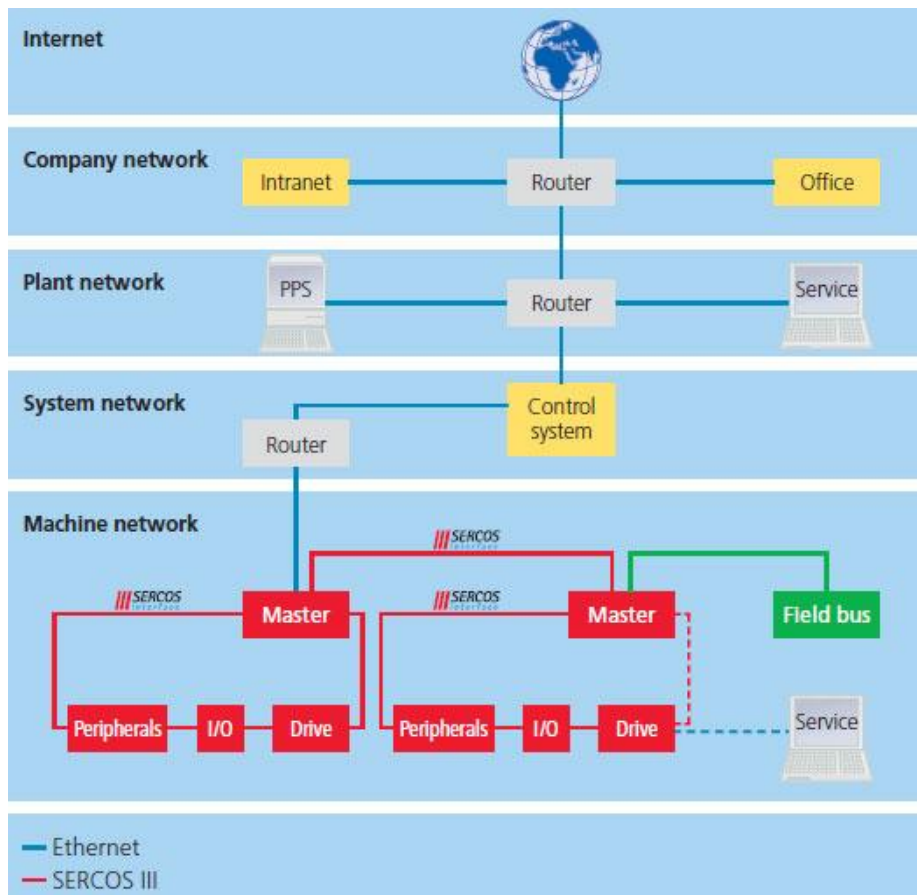


Fig. Nro: 32 Red Ethernet integrada con red SERCOS III ⁽³²⁾

3.11.7 CC-LINK IE

CC-LINK IE (Protocolo de Control y Comunicación – Ethernet Industrial), es la primera red Ethernet Industrial de 1 Gigabit/s completamente integrada para la automatización industrial. Lanzada al mercado por el CLPA (Asociación de Socios CC-Link). Se trata de una tecnología abierta a nivel de campo que proporciona alta velocidad, es una comunicación determinística con múltiples dispositivos de automatización conectados sobre un solo cable, es ideal para el nivel de máquina y de celda, en el control de procesos industriales, como ser: fabricación de semiconductores, alimentos, industria automotriz y productos farmacéuticos.

CC-Link IE, combina lo mejor de muchas tecnologías existentes y los aplica a los sistemas de redes industriales ópticas, para ello cuenta con una arquitectura redundante, que posibilita la transferencia de datos entre los diferentes controladores, de manera confiable y a altísima velocidad, mediante los protocolos de Ethernet. La velocidad alcanzada por este protocolo, es más que suficiente para el manejo de las comunicaciones en tiempo real de las industrias manufactureras actuales.

Además de posibilitar la transmisión de datos entre computadoras, interfaces de usuarios de PLC y controladores de movimiento. **CC-Link IE**, hace realidad la transmisión ininterrumpida de datos entre los diferentes niveles de comunicación, desde el nivel de piso de manufactura hasta los niveles gerenciales de la pirámide CIM.

La frecuencia de las comunicaciones cíclicas es independiente de la carga de la red, haciéndola predecible y determinista, esto significa que las actualizaciones de datos no disminuyen su velocidad cuando el tráfico es pesado. Así como durante operaciones importantes de la planta o emergencias. Tiene la particularidad que los datos se pueden enviar desde cualquier estación a otra estación, gracias al esquema de memoria compartida, incluso a través de redes interconectadas. Además de esta forma, los cambios de configuración o el intercambio de datos es una tarea sencilla en el marco del concepto de memoria compartida. También permite monitorear, programar, restablecer y reprogramar cualquier estación desde otra dentro de la misma red.

Las redes que utiliza ofrecen redundancia en base a una arquitectura de anillo doble, que asegura la continuidad de la comunicación si se corta un cable o se pierde una estación. Esta arquitectura “auto-repara” el problema presentado ya que permite la transferencia de datos en dirección directa e inversa garantizando su continuidad.

La topología en anillo, como la mostrada en la Figura Nro: 33, permite redes extensas, de hecho, una red simple puede tener una extensión de 66 kilómetros, utilizando cableado de fibra óptica, sin perder velocidad de comunicación. Es posible integrar hasta 120 estaciones, con una distancia máxima de 550 metros entre dos estaciones contiguas en cada una de las 239 redes que soporta el protocolo, interconectándolas entre si creando sistemas con más de 14.000 kilómetros de extensión y 25.000 nodos integrados, suficientes para poder solucionar cualquier problema que se le presente a los usuarios.

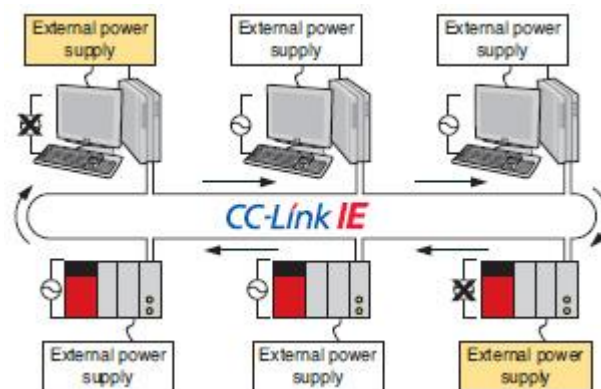


Fig. Nro: 33 Red CC-Link IE⁽³³⁾

Una de las ventajas de la utilización de fibra óptica es su alta inmunidad al ruido electromagnético, que es clave en los entornos industriales, donde estas interferencias están presentes en todo momento. Cuando se utilizan redes con cable de cobre, el protocolo de transmisión garantiza la protección de la integridad de los datos recibidos.

El protocolo de comunicación es extremadamente estable en el tiempo, y esta basado en dos opciones distintas:

- Comunicación cíclica: Datos en tiempo real.
- Comunicación de mensajes: Resto de los datos.

El proceso de comunicación es el siguiente: cada nodo por ejemplo un PLC, inserta la información cíclica y no cíclica en cada trama de transmisión, de forma que el sistema garantiza la comunicación en tiempo real a los datos que así lo requieran., mediante su inclusión en la trama exclusivamente cíclica. Por ejemplo las variables y alarmas de un determinado controlador podrían ser enviadas en tiempo real, utilizando la comunicación cíclica, mientras que la descarga de programas se podría hacer en forma fraccionada en mensajes no cíclicos.

CC-Link IE, utiliza la arquitectura de maestro-esclavo, por lo cual no requiere de herramientas sofisticadas para su administración y control. Posee el sistema de control “stand-by Red Master” que permite automáticamente asumir el control de las comunicaciones de red a otro controlador, en caso de que el maestro principal deje de funcionar.

Sus características más importantes son las siguientes:

- Garantiza la fiabilidad de respuesta determinista, control en tiempo real.
- Permite la programación, supervisión y monitoreo de los controladores de la red.
- Permite la conexión en caliente de los dispositivos de red.
- Restaura automáticamente los dispositivos fuera de línea.
- Proporciona información de diagnóstico para poder identificar problemas en la red.

En la Figura Nro: 34, se pueden observar los diferentes dispositivos que forman parte de la red **CC-Link IE**.

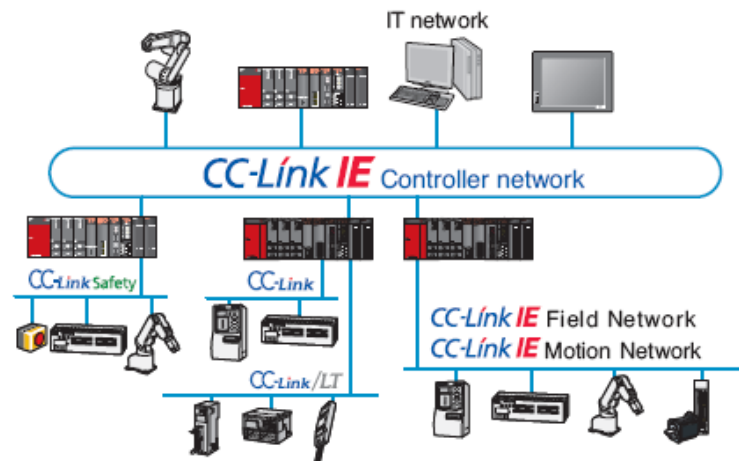


Fig. Nro: 34 Dispositivos que forman parte de una red **CC-Link IE** ⁽³⁴⁾

3. 12 PERSPECTIVAS DE ETHERNET INDUSTRIAL

Ethernet Industrial es un estándar basado en una red optimizada para satisfacer las necesidades de las comunicaciones industriales. Con los nuevos protocolos es ampliamente usado a nivel de campo y en aplicaciones de tiempo críticas, como el control de movimiento.

La integración de la conmutación en los dispositivos de campo, hace que vaya sustituyendo cada vez más el uso de los buses industriales, en las aplicaciones de control en la generación, distribución y el transporte de la energía eléctrica. Con el aumento en la velocidad de 1 a 10 Gigabit, no solamente se usa en el transporte de datos, sino que también en la transmisión de voz y de imagen.

Ethernet Industrial esta siendo actualmente el estándar de facto en los sectores industriales, especialmente en las industrias de proceso de fabricación de automóviles, donde es necesario robustez, fiabilidad, rendimiento y disponibilidad de la información en tiempo real.

Debido a la aparición de nuevos protocolos de comunicación y productos, y la integración con las redes inalámbricas industriales (IWLAN), su alcance en el futuro puede ser ilimitado.

REFERENCIAS BIBLIOGRAFICAS:

- **Pedro Morcillo Ruiz y Julián Cocerá Rueda.** “Comunicaciones Industriales”- Sistemas de Regulación y Control Automático. Editorial Paraninfo. (2004).
- **Ramón Piedrafito Moreno.** “Ingeniería de la Automatización Industrial”. 2da Edición Ampliada y Actualizada. Editorial Ra-Ma. (2004).
- **Emilio García Moreno.** “Automatización de Procesos Industriales”. Editorial Spupv. (1999).
- **Siemens.** “Comunicación Industrial para Automation and Drives”. Siemens AG. (2005).
- **Fabiana Ferreira.** “Seminario de Automatización”. Apuntes de la carrera de Ingeniería de Automatización Industrial de la Universidad Nacional de Quilmes. (2008)
- **Siemens.** Simatic Net, “Ethernet Industrial Basica”. White Paper V1.0/2005.
- **Martínez García.** “Comunicaciones en el entorno Industrial. Editorial UOC (2007).
- **ing. Diego M. Romero.** Seminario a introducción a Ethernet Industrial. AADECA (2008).
- **Empresa ISA España.** Setting the Standard for Automation. (2008).
- **Universidad Nacional de Colombia.** “OPC como alternativa a las tecnologías de Comunicaciones Industriales”. (2007).
- **www.infopl.net.** Informe sobre Ethernet Industrial. “Determinismo, el ser o no ser de Ethernet Industrial”. (2008).
- **www.profibus.com/pn/.** Informe sobre Profibus. (2008).
- **www.sercos.com/.** Informe sobre Sercos III. (2008).
- **www.modbus-ida.org.** Informe sobre Modbus/TCP. (2008).
- **www.odva.org.** Informe Ethernet/IP. (2008).
- **www.ethernet-powerlink.org.** Informe Ethernet-PowerLink. (2008).
- **www.profibus.com/pm.** Informe Profinet. (2008).
- **www.ethercat.org.** Informe EtherCat. (2008).

- www.cc-link.org. Informe sobre CC-Link IE. (2008).

REFERENCIAS DE FIGURAS:

- (1). Capas Ethernet Industrial. Seminario Automatización Industrial. Ing. Fabiana Ferreira. Universidad de Quilmes. Pagina 4. (2008).
- (2), (3), (4), (7), (8), (9), (10), (11). www.weimuller.es/docs/manuales y guías de instalación. Componentes activos y pasivos. Paginas: C2, B5, B27, B35, B40, B44, B38.
- (12), (13) y (18). **Empresa ISA España**. Setting the Standard for Automation”. Paginas: 21, 22 y 23. (2008).
- (5) y (6). Universidad Nacional de Colombia. “OPC como alternativa a las tecnologías propietaria se Comunicación Industrial. (2007).
- (14). www.infopl.net. Ethernet Industrial “Colisión en la red”. (2007).
- (15) y (16). Universidad de Oviedo. “Resolución de colisiones CSMA/DCR y CSMA/CD en entornos industriales”. Artículo Ing. López. Paginas 4 y 5.
- (17) Cisco System. Curso CCNA 4.0, tercer semestre.
- (19). www.ethercat.org. Informe sobre protocolo EtherCAT. (2008).
- (20) Curso de Ingeniería de Informática. Universidad de Oviedo. (2007).
- (21), (22) y (23). Siemens. Automatización y comunicación a escala corporativa. Profinet el estándar abierto de Industrial Ethernet. Paginas: 8, 10 y 20.
- (24). Ethernet Powerlink. Communication profile specification, Version 1.1.0. Pagina 29.
- (25), (26) y (27). www.ethernetpowerlink.org/. Informe sobre Powerlink. (2008).
- (28). **Ethernet/IP**. Network Infrastructure for Ethernet/IP. Introduction and consideration. Pagina 1-2. (2007).
- (29). www.odva.org. Informe sobre Ethernet/IP. (2008).
- (30). www.modbus-ida.org/. Informe sobre Modbus/TCP. (2008).
- (31) y (32). www.sercos.com/. Informe sobre Sercos III. (2008).
- (33) y (34). www.cclinkamerica.org. Artículo de Ethernet Industrial Book. Pagina 6 y 7 (ISSN 1470-5745).

REFERENCIAS DE TABLAS

Tabla Nro: 1. www.modbus-ida.org. Estructura del prefijo de Modbus/TCP.

Tabla Nro: 2. www.modbus-ida.org. Estructura del mensaje Modbus/TCP

4. REDES INALAMBRICAS (WI-FI)

4.1 INTRODUCCION

Actualmente las redes de comunicaciones industriales como EtherCAT, PROFinet, Ethernet/IP o los buses de campo: Device Net, ASi, Profibus, etc., tienen un amplio rango de aplicación en los procesos de control industrial, debido a su buen funcionamiento en tiempo real y costos. Sin embargo, las redes cableadas se han transformado en un obstáculo para algunas aplicaciones industriales, con lo que se ve beneficiado la utilización del medio inalámbrico. La tecnología de red de área local inalámbrica WLAN ofrece algunas ventajas como la movilidad, flexibilidad y la reducción del cableado. El concepto de IWLAN (Redes Lan Industriales Inalámbricas), hace uso de recursos estandarizados como “reserva de datos” y “mecanismos de traspaso”, necesarios para equipos con movilidad.

Las redes inalámbricas son cada vez más populares, el alto grado de flexibilidad y su reducido costo de instalación, le permite ser utilizada en automatización de procesos y manufactura; industria de alimentos y bebidas; depósitos y logística; transporte (ferrocarril, rutas, túneles y puentes); grúas y aplicaciones de transporte de carga.

Si no se posee una conexión inalámbrica a la red de comunicación principal, muchas aplicaciones donde existen equipos en movimiento no serían posibles, o solo se podrían implementar con poca eficiencia.

En una red inalámbrica, los datos de producción y de servicio están disponibles prácticamente en toda la fábrica y por ello están a disposición de ser accedidos cuando se desee, en forma simultánea por los ingenieros de planta para observar desde sus puestos de trabajo, e influenciar con sus acciones el proceso de toda la planta.

En aplicaciones industriales, la confiabilidad de la operación es de particular importancia, por ello se necesitan componentes de alta confiabilidad, que provean el soporte de funciones en tiempo real (garantizar los tiempos de transmisión) y características determinísticas (tráfico de datos predecibles). Esto significa que tiene que garantizar la transmisión de datos en condiciones críticas.

El estándar IEEE 802.11x (Wi-Fi), solo provee opciones limitadas para su aplicación a nivel industrial, por lo tanto hay que adicionarle **prestaciones especiales (“Industriales”)**, al estándar WLAN, manteniendo la total compatibilidad, de manera que los equipos comerciales compatibles con el estándar, se puedan integrar a la red industrial, igual que los dispositivos especialmente adaptados para ese contexto.

Además de utilizar dispositivos altamente confiables, la operatividad del sistema debe garantizar con una planificación de instalación óptima de los enlaces inalámbricos. Se debe tener muy en cuenta la intensidad del link inalámbrico, para que el usuario pueda confiar en la comunicación en ambientes de perturbaciones dinámicas y reservas apropiadas de señal para el caso de aplicaciones críticas, que se puedan llevar a cabo en equipos de transporte y en la elevación de contenedores metálicos, que pueden causar reflexiones y perturbaciones que alteren la eficacia del enlace.

Con respecto a la seguridad de los datos, dependerá de las políticas que adopten las compañías en estos casos. Es conveniente el encriptamiento de los datos transmitidos, debido a que el tráfico en un enlace inalámbrico puede ser interceptado utilizando antenas direccionales. Pero a veces no es suficiente con encriptar los datos, sino que hay que instruir al personal, indicándoles el uso de protocolos de comunicaciones adecuados.

Cualquier esquema de seguridad que se adopte, hay que tener en cuenta que este conformado por procedimientos de seguridad estandarizados, sin recurrir a protocolos propietarios. IWLAN utiliza mecanismos de seguridad que están precisamente definidos en el estándar IEEE y en las especificaciones de la WECA.

4.2 TECNOLOGIAS INALAMBRICAS

Las tecnologías inalámbricas disponibles en el mercado son las mostradas en la siguiente figura.

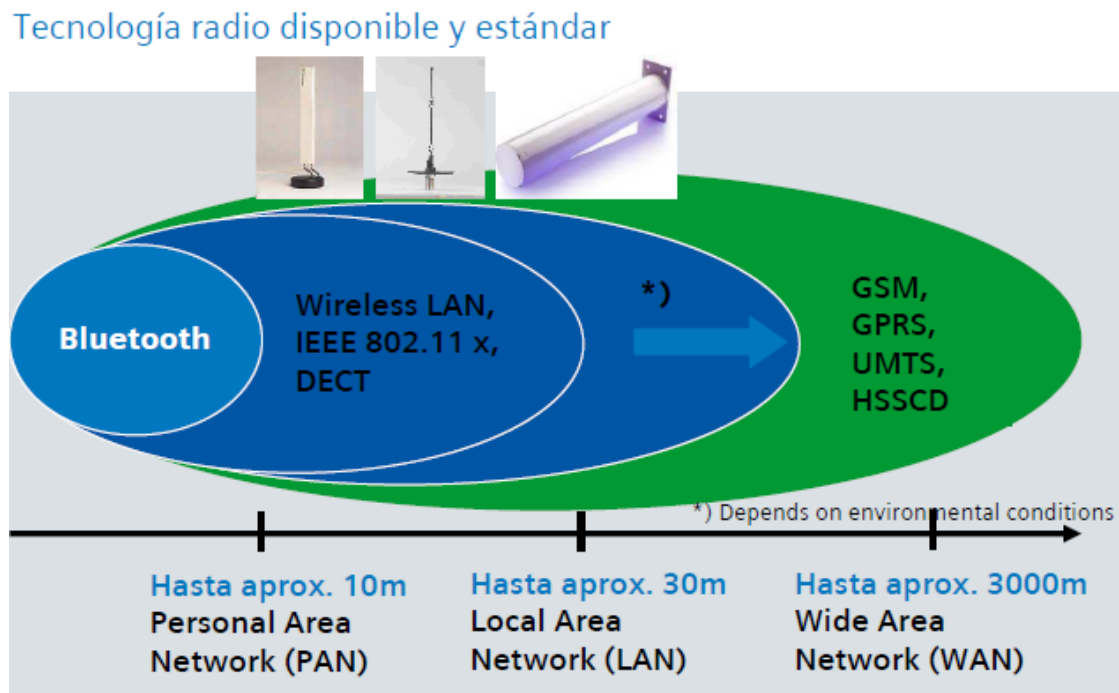


Fig. Nro: 1 Tecnologías inalámbricas disponibles ⁽¹⁾

A continuación paso a describir cada una de estas tecnologías inalámbricas, y su utilización en los distintos niveles de la pirámide CIM.

4.2.1 RED PAN (Personal Área Network)

Son las redes a nivel de proceso y maquina. El alcance máximo de estas redes es de aproximadamente de 10 metros, y se dividen en:

a) **Redes de sensores y captura de datos:**

- RFID.

-
- Red de sensores inteligentes. Tecnología ZigBee (IEEE 802.15.4).

b) Redes de sincronización

- Bluetooth (IEEE 802.15-1).

4.2.1.1 RFID

RFID (Radio Frequency Identification), Identificador por Radio Frecuencia, es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas o transportadores o tags **RFID**. El propósito de esta tecnología es transmitir la identidad de un objeto (similar a un número de serie único), mediante ondas de radio, esta tecnología se agrupa dentro de las denominadas Auto ID (automatic identification), identificación automática.

Estas etiquetas son dispositivos pequeños, que pueden ser aplicadas a un producto. Contienen antenas para transmitir y responder a peticiones solicitadas por cualquier dispositivo de control. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas si. Una de las ventajas de utilizar radiofrecuencia (en lugar de rayos infrarrojos) es que no requieren visión directa entre el emisor y el receptor.

El modo de funcionamiento es simple. La etiqueta que contiene los datos de identificación del objeto a cual se encuentra adherida, genera una señal de RF, que es captada por un lector de **RFID**, que se encarga de leer la información y pasarla a formato digital para ser procesada por la aplicación específica.

El sistema esta formado por tres componentes:

- Etiqueta **RFID** o transpondedor, que esta compuesta por un transductor de radio, una antena y un chip.
- Lector **RFID** o transceptor, compuesto por una transceptor, una antena y un decodificador
- Subsistema de procesamiento de datos o Middleware **RFID** es el que proporciona los medios de proceso y almacenamiento de datos.

El concepto de tags (etiqueta) **RFID** va asociado al de su ubicuidad. Esto supone que los lectores pueden requerir la selección de tags a explorar de entre muchos candidatos posibles. También podrían desear realizar una exploración de los tags de su entorno para realizar inventarios, y si están asociados a sensores pueden identificar condiciones de su entorno.

Para poder leer los datos de los tags, los lectores utilizan un algoritmo de singulacion basado en el recorrido de árboles, resolviendo las colisiones que puedan darse y procesando secuencialmente las respuestas. Los tags pueden trabajar en modo promiscuo, si responde a todas las peticiones sin excepción, o seguro, si requiere autenticación (necesita claves criptográficas y de acceso).

Los lectores encargados de un grupo de tags en un área pueden operar en modo autónomo en contraposición al modo interactivo. Si trabajan de esta forma, realizan una

identificación periódica de todos los tags en su entorno y mantienen una lista de presencia con tiempos de persistencia (timeouts) e información de control. Si una entrada expira, se elimina de la tabla.

Con frecuencia una aplicación distribuida puede utilizar tags activos o pasivos. Los pasivos no pueden realizar tareas de monitorización continua sino que realizan tareas bajo demanda cuando los lectores se lo solicitan. Son útiles para realizar actividades regulares y bien definidas con necesidades de almacenamiento y seguridad acotadas. Si hay accesos frecuentes, continuos o impredecibles, o bien existen requerimientos de tiempo real o procesamiento de datos, es conveniente utilizar los activos.

Los sistemas **RFID** se clasifican en función de la frecuencia de trabajo. Existen cuatro tipos:

- Frecuencia baja, entre 125 o 134,2 Khz.
- De alta frecuencia, de 13,56 Mhz.
- UHF de 868 a 956 Mhz.
- Microondas de 2,45 Ghz

Los estándares de **RFID** abordan 4 áreas fundamentales:

- **Protocolo de interfaz aéreo:** especifica el modo en que las etiquetas **RFID** y lectores se comunican mediante enlaces de radiofrecuencia.
- **Contenidos de los datos:** especifica el formato y semántica de los datos que se comunican entre etiquetas y lectores.
- **Certificación:** pruebas que los productos deben cumplir para garantizar que cumplan los estándares y pueden interoperar con otros dispositivos de distintos fabricantes.
- **Aplicaciones:** uso de los sistemas **RFID**.

Los beneficios y ventajas que posee esta tecnología es la siguiente:

- Combinación de diferentes tecnologías **RFID** con Internet.
- Proveedor de identificación y localización de artículos en la cadena de suministro más inmediato, automático y preciso de cualquier compañía, en cualquier sector y en cualquier parte del mundo.
- Lecturas rápidas y precisas.
- Seguimiento de: paquetes carretillas, etc., de manera más precisa.
- Etc.

Actualmente una de las aplicaciones más importante de la tecnología **RFID** es la logística. El uso de esta tecnología permite tener localizado cualquier producto dentro de la cadena de suministro. Una aplicación importante es el manejo de stock de productos en los depósitos, ya que las etiquetas pueden grabarse, con lo cual se puede conocer con exactitud el tiempo que estuvo almacenado un producto, en que sitios, etc. De esta manera se pueden lograr importantes optimizaciones en el manejo de los productos en las cadenas de abastecimiento teniendo como base el mismo producto, e independizándose prácticamente del sistema de información.

4.2.1.2 Tecnología ZigBee

La red **ZigBee**, (IEEE 802.15.4), es una red inalámbrica, flexible, de bajo costo y consumo de energía, por lo tanto es utilizada en muchas aplicaciones doméstica e industriales, donde se requiere una baja tasa de transmisión de datos. Estas características la convierten en una buena opción para el control de maquinas con piezas móviles o dispositivos donde no sea posible detener el proceso frecuentemente. Se utiliza en periféricos de computadoras, juguetes y sensores médicos, pero su objetivo esta orientado a las siguientes áreas:

- Automatización del hogar (domótica).
- Automatización de edificios.
- Automatización industrial.

El estándar define el hardware y el software, el cual ha sido descrito en los términos de conexión de redes, como la capa física (PHY) y la capa de control de acceso al medio MAC y LLC.

Algunas de sus características se resumen en la siguiente tabla:

Bandas de frecuencia y rango de transmisión de datos	868 Mhz : 20 kb/s 915 Mhz : 40 kb/s 2,4 GHz: 250 kb/s
Alcance	10 – 20 metros
Latencia	Por debajo de 15 ms.
Canales	868/915 MHz: 11 canales 2,4 GHz: 16 canales
Modos de direccionamiento	Todos los chips tienen 64 bits de direccionamiento
Canal de acceso	CSMA-CA
Seguridad	128 AES
Red	Hasta 2^{64} dispositivos
Rango de Temperatura	- 40° a + 85° C

Tabla Nro: 1 Característica de las redes ZigBee.

El estándar IEEE 802.15.4 soporta múltiples topologías para su conexión en red, entre ellas la topología tipo “Star” y la topología “Peer-to-Peer”.

La topología a usar es una elección de diseño y va a estar dado por la aplicación a la que se desee orientar, algunas aplicaciones como periféricos e interfaces de computadoras, requieren de conexiones de baja potencia de tipo estrella, mientras que otros como los perímetros de seguridad requieren de una mayor área de cobertura por lo que es necesario implementar una red Peer-to-Peer, como se observa en la siguiente figura.

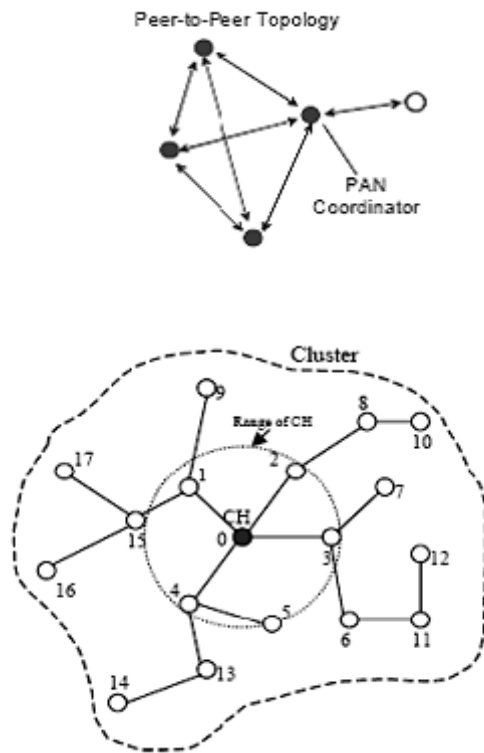


Fig. Nro: 2 Topologías ZigBee: Arbol y Peer-to Peer⁽²⁾

La topología de árbol, como se observa en la Figura Nro: 2, es un caso especial de topología de conexión punto a punto, en la cual muchos dispositivos son FFDs y los RFD pueden conectarse como un nodo único al final de la red. Cualquiera de los FFDs restantes pueden actuar como coordinadores y proveer servicios de sincronización hacia otros dispositivos o coordinadores.



Fig. Nro: 3 Topología Mesh⁽³⁾

La Figura Nro: 3, muestra la topología Mesh, donde hay conectividad total de todos los FFDs que conforman la red. El FFD actúa como coordinador PAN. Los RFDs pueden también participar en la red pero hay solamente conectividad con los FFD y no

puede participar en enrutamiento. Las ventajas de esta topología es que son confiables y el rendimiento en el proceso de información en la red se debe a las múltiples trayectorias que existen.

FFD (Full Function Device): Es un dispositivo de función completa que se puede usar en cualquier topología. Tiene capacidad de poder ser Coordinador de red y puede hablar con cualquier dispositivo.

RFD (Reduced Function Device): Es un dispositivo de función reducida. Limitado a una topología en estrella. No puede ser un Coordinador de red y solo puede hablar con un Coordinador de red y es muy fácil de implementar.

IEEE 802.15.4, divide la capa de enlace de Datos, en dos subcapas, la subcapa de Control de Acceso al Medio (MAC), y la subcapa de Control de Enlace Lógico (LLC). El LLC es común en todos los estándares 802, mientras que la subcapa MAC depende del hardware y varía respecto a la implementación de la capa física.

En la siguiente figura se muestra la relación del estándar 802.15.4 y el modelo de referencia OSI.

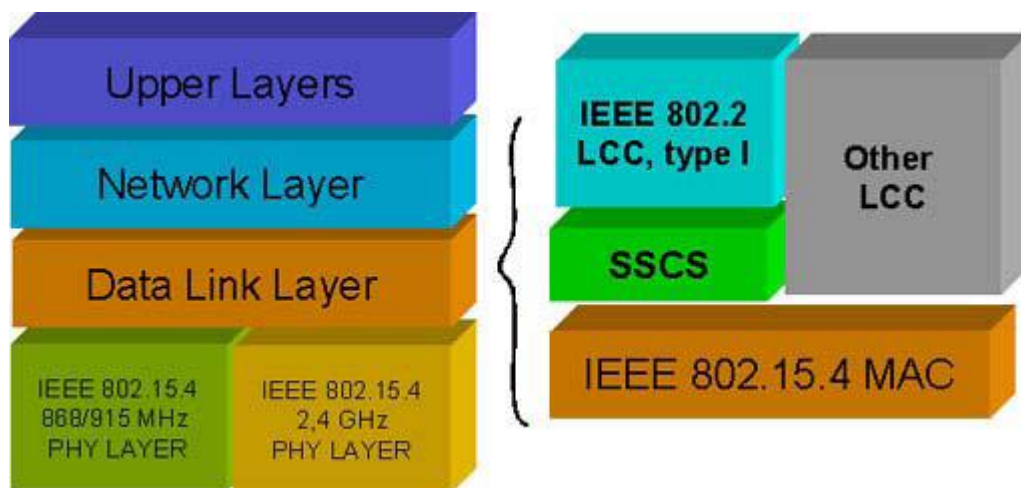


Fig. Nro: 4 Relación del estándar 802.15.4 y el modelo OSI ⁽⁴⁾

Las características de la subcapa MAC 803.15.4 son: asociación/disociación, reconocimientos de entrega de trama (AKC), mecanismos de acceso al canal, validación de trama, control de garantía de ranuras de tiempo (Slot Time), control de guías (Beacon) y barrido de canal. La subcapa proporciona dos tipos de servicios hacia las capas superiores que se acceden a través de dos Puntos de acceso a Servicios (SAPs). A los servicios de datos MAC se accede por medio de la parte común de la subcapa (MCPS-SAP), y el manejo del servicio MAC se accede por medio de la capa MAC de manejo de identidades (MLME-SAP). Estos dos servicios proporcionan una interfaz entre las subcapas de convergencia de servicios específicos (SSCS) y otro LLC y las capas físicas.

La función importante de la subcapa MAC es la confirmación de recepciones exitosas de tramas de algún dispositivo. Las recepciones exitosas y las validaciones de datos o comandos MAC se confirman por medio de tramas ACK. Si por algún motivo el

dispositivo de recepción no es capaz de recibir la información en ese momento, el receptor no manda ningún ACK.

En las redes sin Beacon (control de guías), se utiliza el estándar CSMA-CA. Estas redes trabajan de la siguiente forma, cuando algún dispositivo desea transmitir en una red que no permite señales guía, la red revisa primero si el otro dispositivo se encuentra transmitiendo en el mismo canal, si esto ocurre, el intento de acceso al canal será en una ocasión posterior, o caso contrario después de varios intentos fallidos indicara una falla de conexión.

La capa física (PHY) del estándar, ofrece dos opciones, que combinadas con la subcapa MAC, permiten un amplio rango de aplicaciones. Ambas capas físicas utilizan como método de transmisión la Secuencia Directa de Espectro Extendido (DSSS), que resulta de bajo costo, y comparten la misma estructura básica de paquetes low-duty-cycle con operaciones de bajo consumo de energía. La principal diferencia es la banda de frecuencias, la de 2,4 Ghz, utilizada en la banda Industrial, médica y científica (ISM), disponible en todo el mundo, y la de frecuencia de 868 Mhz, utilizada en Europa y la de 915 Mhz utilizada en la banda de ISM en EE.UU.

La segunda opción es el rango de transmisión. La frecuencia de 2.4 Ghz, permite una transmisión de datos de 250 kb/s y la de 868/915 Mhz, entre 20 y 40 kb/s respectivamente.

En función de los objetivos a cubrir, se puede usar la banda de 868/915 Mhz, para aplicaciones de baja densidad de datos y áreas de cobertura grande, con lo que se reduce el numero de nodos requeridos para cubrir una cierta área geográfica, mientras que la de 2.4 Ghz, para comunicaciones de datos de baja latencia.

4.2.1.3 BLUETOOTH (IEEE 802.15.1)

Bluetooth, es una tecnología diseñada para la comunicación inalámbrica principalmente entre computadoras, periféricos y teléfonos celulares, en aplicaciones donde las conexiones inalámbricas representan una gran ventaja.

En el ambiente industrial, los requerimientos son diferentes: mensajes cortos, seguros, robustos y de rápida transferencia. No obstante salvados estos requerimientos, la aplicación de **Bluetooth**, es ventajosa y esta empezando a ser tenida en cuenta para las aplicaciones industriales.

Las plantas industriales incluyen una multitud de dispositivos interconectados de diferentes maneras: simple recolección de unidades de datos sin inteligencia alguna, dispositivos como sensores con cierta inteligencia incorporada, controladores de simple-lazo o controladores programables y sistemas de supervisión, donde la tecnología inalámbrica **Bluetooth** es potencialmente útil.

Las áreas potenciales donde se podría aplicar serian las siguientes:

- Como reemplazo de comunicaciones seriales RS- 322 / 422 o 485, como se observa en la Figura Nro: 5.
- Como "Access Point", para acceso a redes cableadas vía Internet. (Figura Nro: 6).

- En sensores y actuadores inalámbricos, que controlan maquinas herramientas, como la observada en la Figura Nro: 7.

Los cables seriales RS-232/422/485, son utilizados normalmente para la conexión de las computadoras portátiles a equipos de control, con el objeto de efectuar configuraciones y/o monitorización de los mismos o de la red.

El uso de **Bluetooth** resulta ideal para suprimir la incomodidad que representa la conexión física, por ejemplo si el PLC no contara con una interfaz adecuada, se le colocaría un adaptador para conectarlo a la computadora portátil con el soft adecuado. Una opción más avanzada podría ser la conexión con dispositivos que posean TCP/IP con un Web Server incorporado.

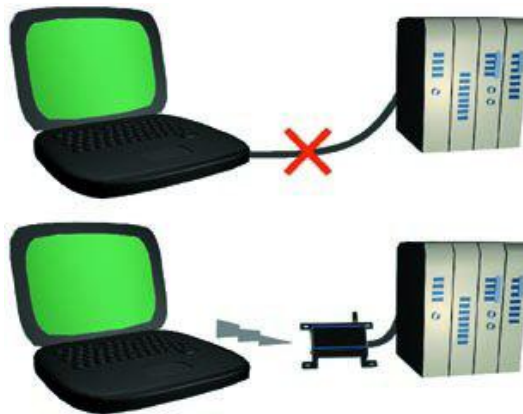


Fig. Nro: 5 Reemplazo de conexiones seriales ⁽⁵⁾

Otra opción sería la conexión de un celular con WAP incorporado utilizado como HMI (interfaz hombre maquina), la especificación WAP con **Bluetooth** incluye la función de routing. Para ello es necesario que los dispositivos de campo posean Web Server incorporado corriendo sobre Bluetooth, o bien que se disponga de puntos de acceso específicos ubicados en varios puntos en la red cableada.

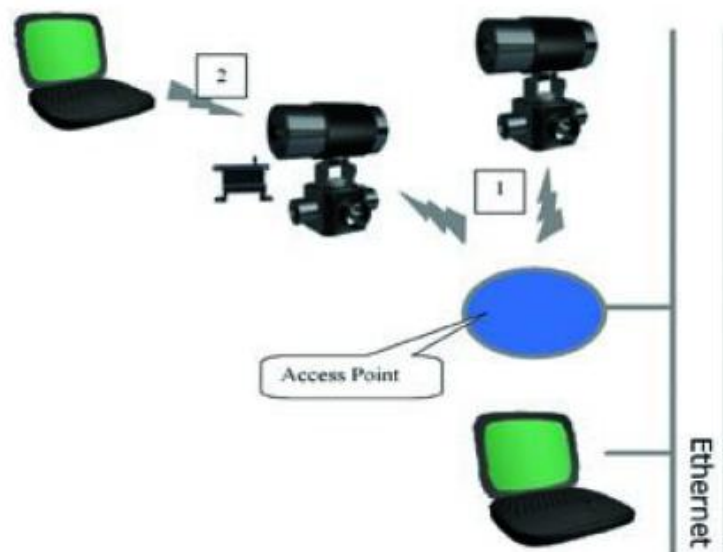


Fig. Nro: 6 Punto de acceso en una red cableada ⁽⁶⁾

Una utilización ideal de **Bluetooth**, sería su utilización en maquinas-herramientas o vehículos, donde las distancias son cortas y la utilización de cableado sería muy dificultosa. Para ello se requiere que los sensores utilizados posean cierta inteligencia y el espacio físico suficiente para poder contener a la electrónica necesaria para su funcionamiento. Además es conveniente que los mismos cuenten con una cierta independencia funcional como para poder seguir conectados aun ante los cortes en la comunicación.



Fig. Nro: 7 Conexión en maquinas-herramientas ⁽⁷⁾

Gracias a este protocolo, los dispositivos que lo implementan pueden comunicarse entre ellos cuando se encuentran dentro de su alcance. Las comunicaciones se realizan utilizando RF, de forma tal que los dispositivos no tienen que estar alineados y pueden incluso estar en ambientes separados si la potencia de transmisión lo permite. Se clasifican como Clase 1, Clase 2 o Clase 3, en referencia a su potencia de transmisión, siendo completamente compatibles entre ellas.

Clase	Pot. Max. Permitida (mW)	Pot. Max. Permitida (dBm)	Rango (aproximado)
1	100	20	100
2	2,5	4	10
3	1	0	1

Tabla Nro: 2 Clasificación del protocolo

También se pueden clasificar en función de su ancho de banda:

Versión	Ancho de banda
1.2	1 Mbit/s
2.0 + EDR	3 Mbit/s
UWB (propuesto)	53 – 480 Mbit/s

Tabla Nro: 3 Ancho de banda de Bluetooth

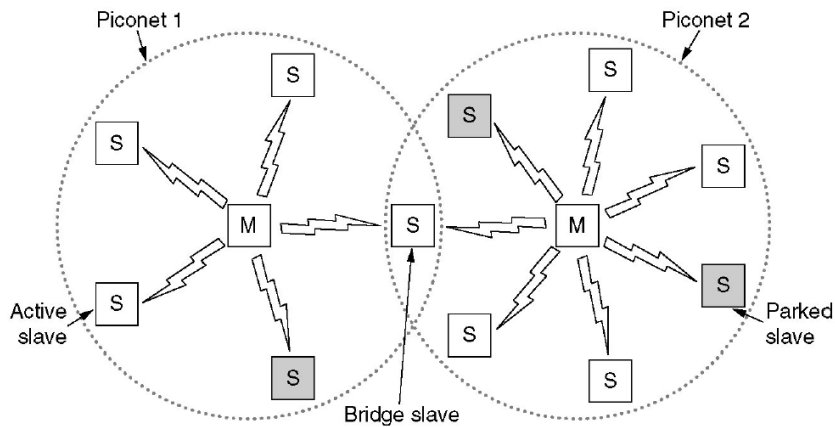


Fig. Nro: 8 Arquitectura Red Bluetooth ⁽⁸⁾

Como se observa en la Figura los dispositivos Bluetooth se relacionan formando piconets y scatternets.

Las piconets (o picoredes) son las topologías de red utilizada por Bluetooth, en todo enlace Bluetooth existe una de estas redes, que unen dos o más dispositivos por medio de un canal físico compartido con un reloj y una secuencia de saltos única. Distintos canales (combinación de un maestro y su reloj) pueden coexistir. Si bien un maestro puede serlo de una única piconet, un dispositivo cualquiera puede pertenecer a varias piconet al mismo tiempo. Este solapamiento se denomina scatternet (red dispersa), aunque no se define capacidades de ruteo por defecto entre ellas.

Los dispositivos que forman parte de una piconet comparten el canal físico y disponen de un canal físico y otro lógico entre ellos. Los modos por defecto pueden ajustarse y se pueden añadir enlaces lógicos adicionales. Un dispositivo puede pasar a operar en modo de mantenimiento (hold mode), un estado transitorio que limita la actividad en el enlace físico, también se puede establecer un modo de rastreo (sniff) que define periodos de presencia y ausencia en la piconet, que pueden tener efectos en la recepción de información por broadcast no fiable. Los esclavos pueden dejarse en un estado aparcado controlado por el maestro. Además, dos dispositivos concretos de una piconet pueden intercambiar sus papeles, lo que les afectara solo a ellos, y no al resto de esclavos del maestro inicial.

Otras características técnicas importantes:

- Rango de frecuencia de trabajo: 2,4 a 2,48 Ghz.
- Full Duplex.
- Salto de frecuencia. Máximo 1600 saltos.
- Tecnología CMOS
- Etc.

La integración de UWB con **Bluetooth**, crea una versión de gran ancho de banda, que permitirá alcanzar requisitos de sincronización y transferencia de grandes cantidades de datos como así también contenidos de alta definición para dispositivos portátiles, muy apropiado para futuras aplicaciones industriales.

4.2.2 REDES WLAN (Wireless Local Area Network)

Son redes a nivel de Área Local (LAN), que abarca desde la zona de proceso llegando al nivel de gestión. El estándar utilizado **IEEE 802.11.x**, define los niveles de capa física y de enlace incluido el control de acceso al medio (MAC). Habitualmente se denominan redes **Ethernet Inalámbricas**, donde los dispositivos que la conforman son fácilmente integrables a una red Ethernet cableada a través de un punto de acceso, que permite la unión de ambas redes, como se observa en la Figura Nro: 9.

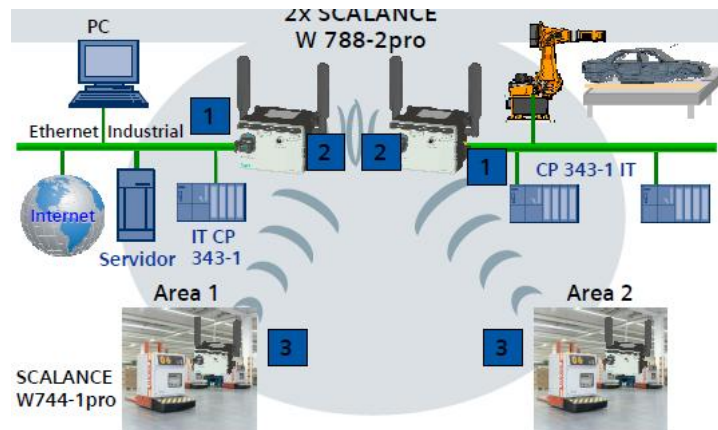


Fig. Nro: 9 Red WLAN integrada con Industrial Ethernet ⁽⁹⁾

Las redes inalámbricas (Wireless Local Área Networks, WLAN), ofrecen las siguientes ventajas, con respecto a las redes cableadas:

- **Movilidad:** Los sistemas WLAN ofrecen a sus usuarios acceso a la información en tiempo real en cualquier lugar de su organización.
- **Velocidad y sencillez de instalación,** evitando la necesidad de tender cables a través de paredes y techos.
- **Flexibilidad de instalación,** permitiendo llegar a lugares de difícil acceso para una red cableada.
- **Reducción de gastos** de instalación durante el tiempo útil de la red, aunque la inversión inicial puede ser mayor. Esto es primordial para entornos dinámicos que requieren mudanzas y cambios frecuentes.
- **Escalabilidad:** Los sistemas WLAN se pueden configurar con diversos tipos de topologías para satisfacer las necesidades de aplicaciones e instalaciones específicas. Las configuraciones se cambian con facilidad y varían desde redes igual a igual asta infraestructuras para redes de muchos usuarios.

También hay que tener en cuenta las siguientes desventajas:

- **Velocidad de transmisión:** En términos generales la velocidad de transmisión siempre Será inferior a la de una red cableada e incluso sus prestaciones se degradaran más rápidamente cuando se introduzcan nuevos nodos.

- **Interferencias:** La red estará sometida a interferencias, debidas al entorno radioeléctrico e incluso podría causar interferencias a dispositivos cercanos a su entorno.
 - **Privacidad:** Las transmisiones se propagan por el espacio sin límites definidos por lo que podrían ser captadas por terceros y espiadas si no se habilitan los sistemas adecuados para mantener su privacidad.
- En la siguiente tabla se muestran algunos de los protocolos utilizados en las redes inalámbricas.

	802.11b	802.11g	802.11a/h	802.11a/h	802.11a/h	802.11a/h
Frequency band	2.4 GHz	2.4 GHz	5.15-5.25 GHz	5.25-5.35 GHz	5.4-5.7 GHz	5.7-5.8 GHz
Data rate	11 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps
Non-overlapping channels	3	3	4	4	10/11	4/5
Transmit power	100 mW EIRP (ETSI), 1 W (FCC)	100 mW EIRP (ETSI), 1 W (FCC)	200 mW EIRP (ETSI) 50 mW (FCC)	200 mW EIRP (ETSI) 250 mW (FCC)	1 W EIRP (ETSI)	1 W (FCC)
Data rate Mbps ²						
1 m	11 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps
10 m	11 Mbps	1	1	1	1	36 Mbps
100 m	1 Mbps	1	1	1	1	6 Mbps
Modulation	DSSS	OFDM	OFDM	OFDM	OFDM	OFDM
Penetration of walls	Medium	Medium	Poor	Poor	Poor	Poor
Reflections, for example from metallic objects	Robust	¹	Robust	Robust	Robust	Robust
Risk of interference by other radio applications	Medium	Medium	Low	Low	Very low	Very low

Tabla Nro: 4 Protocolos WLAN

4.2.2.1 IEEE 802.11.b

Posee una velocidad máxima de transmisión de 11 Mbit/s y utiliza el método de acceso al medio CSMA/CA. Funciona en la banda de 2,4 Ghz. Debido al espacio ocupado por la codificación del proceso CSMA/CA, en la práctica la velocidad máxima de transmisión es de 5,9 Mbit/s sobre TCP y de 7,1 Mbit/s sobre UDP.

Aunque utiliza la técnica de ensanchado de espectro basada en DSSS, también introduce CCK (Complementary code Keying) para poder llegar a la velocidad de 5,5 y 11 Mbps (tasa física de bit). El estándar también admite el uso de PBCC (Packet Binary Convolutional Coding) como opción. Además los dispositivos **802.11b** deben mantener la compatibilidad con el equipamiento anterior DSSS especificado en la norma original con velocidades que rondan los 1 y 2 Mbps.

4.2.2.2 IEEE 802.11 g

Es la evolución del estándar **802.11 b**. Utiliza la banda de 2,4 Ghz, al igual que el, pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar al estándar 802.11 a. Es compatible con **802.11 b** y utiliza las mismas frecuencias. Actualmente los dispositivos que trabajan con este estándar, pueden comunicarse con una potencia de salida de medio vatio, y con la inclusión de la tecnología i-MOX el alcance pueden llegar a varios kilómetros, muy apropiado para ciertas aplicaciones industriales.

4.2.2.3 IEEE 802.11 a

Este estándar opera en la banda de 5 Ghz y utiliza 52 subportadoras, con una velocidad máxima de 108 Mbit/s, lo que lo hace práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de los datos se pueden reducir en función de la aplicación a: 48, 36, 24, 18, 12, 9 o 6 Mbit/s. Tiene 12 canales no solapados, 8 para redes inalámbricas y 4 para conexiones punto a punto.

Dado que la banda de 2,4 Ghz tiene gran uso, el utilizar 5 Ghz representa una gran ventaja para el estándar, dado que presenta menos interferencias, pero también tiene sus desventajas, ya que se restringe su uso a conexiones punto a punto en línea de vista, con lo que se hace necesario la instalación de un número mayor de puntos de acceso. Esto significa también que las señales no pueden llegar tan lejos como el estándar **802.11 b** ya son fácilmente absorbidas por el medio.

4.2.2.4 IEEE 802.11 h

La especificación **IEEE 802.11 h** es una modificación sobre el estándar 802.11 para WLAN, que intenta resolver los problemas derivados de la coexistencia de las redes 802.11 con sistemas de radares y satélites. Esta especificación proporciona la capacidad de gestionar dinámicamente tanto la frecuencia como la potencia de transmisión, para ello utiliza DFS y TPC, para poderlo llevarlo a cabo.

- **DFS** (Selección Dinámica de Frecuencia), es una funcionalidad requerida por las WLAN que operan en la banda de 5 Ghz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.
- **TPC** (Transmitter Power Control), es una funcionalidad requerida por la WLAN que operan en la banda de 5 Ghz, para asegurar que se respeten las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

4.2.2.5 CAPA FISICA

Las redes inalámbricas se diferencian del resto, principalmente por la capa Física y la capa de Enlace de Datos, según el modelo OSI, ya que sustituyen al cable típico por una señal de radiofrecuencia (RF), o luz infrarroja (IR).

La capa física puede utilizar tanto enlaces de radiofrecuencia FHSS (Espectro Disperso con Salto de Frecuencia) o DSSS (Espectro Disperso de Secuencia Directa), en la banda de 2,4 / 5 Ghz, que son los más usados habitualmente o enlaces infrarrojos, modulando la señal con la técnica PPM (modulación por posición de pulso), en la banda de 300 a 428 Ghz.

Los sistemas infrarrojos pueden clasificarse, a su vez en sistemas de **corta apertura**, también llamados **de línea de vista** (LOS – Line Of Sight) o **de rayo dirigido** y en sistemas de **gran apertura** pudiendo estos últimos ser reflejados o difusos.

Las bandas de frecuencias utilizadas son tres: 902 a 828 MHz, 2483,5 MHz y 5725 a 5850 MHz, denominadas bandas ICM (Industrial, Científico y Medico), limitadas a uso industrial, científicos y médicos, sin embargo en la actualidad algunas de estas frecuencias están siendo utilizadas por numerosos dispositivos, como ser: teléfonos inalámbricos, puertas de garaje automáticos, sensores remotos, etc. Por esto las redes inalámbricas que operan en estas frecuencias deben ser diseñadas para trabajar bajo interferencias considerables. Por lo tanto utilizan, generalmente, una tecnología desarrollada en los años 40 para proteger las comunicaciones militares: la técnica de **espectro disperso**.

La técnica trabaja de la siguiente forma: toma una señal de banda convencional y distribuye su energía en un dominio más amplio de frecuencias, así la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía por debajo del nivel de ruido ambiental de tal forma que la señal no fuese detectable, en cambio su aplicación en redes inalámbricas permite que la señal sea transmitida y recibida con un mínimo de interferencia.

La Tecnología de Espectro Disperso presenta dos técnicas de modulación:

- **Salto de Frecuencia** (FHSS, Frequency – Hopping Spread Spectrum). Los dispositivos saltan de una frecuencia a otra de manera sincrona según un patrón predeterminado. Solo aquellos dispositivos sincronizados pueden acceder a la información.

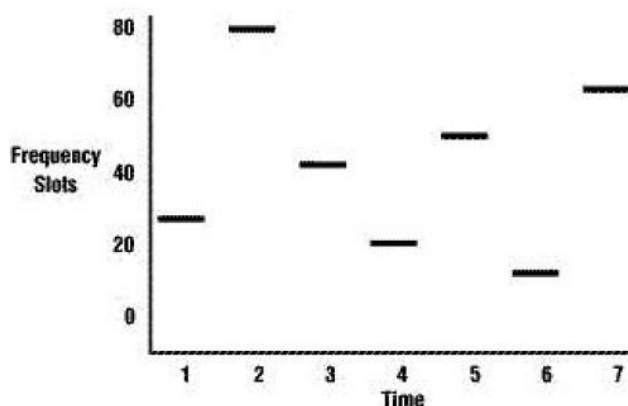


Fig. Nro: 10 Técnica de saltos de FHSS ⁽¹⁰⁾

- **Secuencia directa** (DSSS, Direct- Sequence Spread Spectrum). La información a transmitir se mezcla con un patrón pseudoaleatorio de bits para extender los

datos antes de que se transmitan. Cada BIT transmitido se modula por medio de la secuencia de bits del patrón de referencia, extendiendo su ancho de banda. Solo el receptor que tenga el mismo código de extensión será capaz de regenerar la información original, mientras que para cualquier otro receptor es ruido de baja potencia que resulta ignorado. Esta técnica permite corregir algunos de los errores que se pueden producir en la transmisión y requiere un procesador digital de señales (DSP) para correlacionar la señal de entrada.

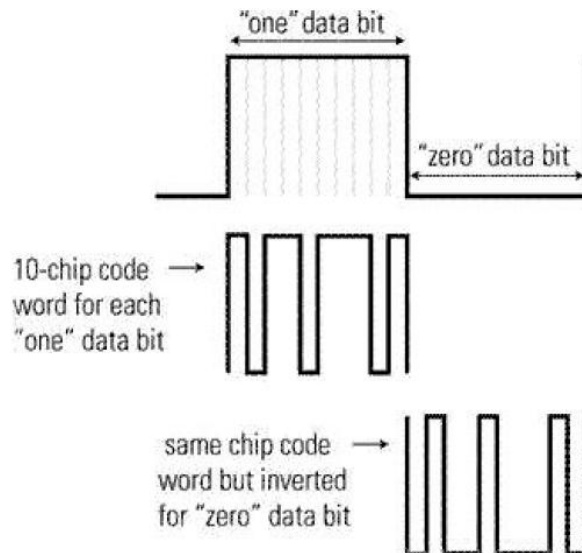


Fig. Nro: 11 Codificación de la información mediante la secuencia de Barker ⁽¹¹⁾

4.2.2.6 CAPA DE ENLACE

La capa de enlace incluye el mecanismo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), donde un nodo se asegura de que el canal está libre antes de transmitir. El mecanismo de detección de colisiones usado en CSMA/CD no puede utilizarse en este caso debido a que un nodo no puede transmitir y escuchar el canal para detectar si otra estación lo hace al mismo tiempo. El mecanismo CSMA/CA no elimina las colisiones completamente, solo minimiza su probabilidad. Como se observa en la Figura Nro: 12, el algoritmo funciona de la siguiente manera:

- Antes que una estación transmita la información, se debe testear el medio o canal, para verificar su estado (libre/ocupado).
- Si el medio no está ocupado por ninguna otra trama la estación ejecuta una espera adicional llamado “**espaciado entre tramas**” (IFS).
- Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
- Una vez finalizada esta espera debido a la ocupación del medio, la estación ejecuta el algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado “**ventana de contienda**” (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de

colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

- Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS, esta espera va avanzando temporalmente hasta que la estación consume todas las ranuras temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo queda suspendido hasta que se cumpla esta condición. Cada retransmisión provocara que el valor de CW, que se encontrara entre CW_{min} y CW_{max} se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es de 20 seg.

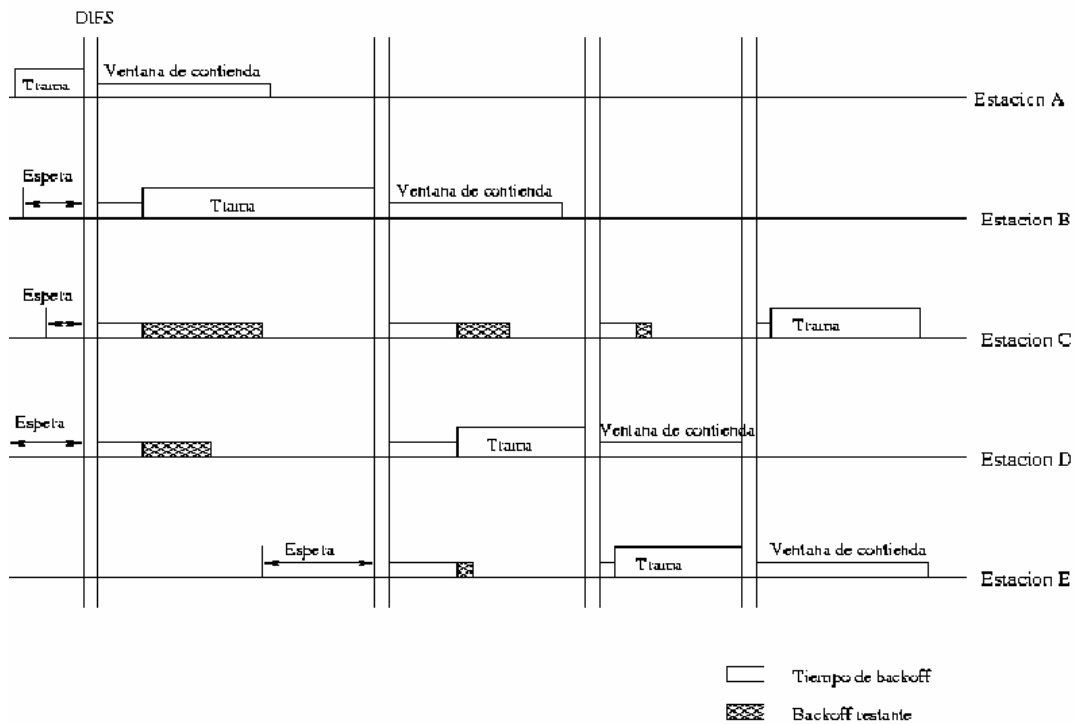


Fig. Nro: 12 Funcionamiento del acceso CSMA/CA ⁽¹²⁾

Sin embargo, CSMA/CA en un entorno inalámbrico presenta una serie de problemas que son:

- **Nodos ocultos.** Una estación cree que el canal esta libre, pero en realidad esta ocupado por otro nodo que no se oye.
- **Nodos expuestos.** Una estación cree que el canal esta ocupado, pero en realidad esta libre, pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución propuesta es a través del protocolo **MACA** (Multi Access Collision Avoidance), que funciona de la siguiente forma:

- Antes de transmitir el emisor envía una trama RTS (Request to Send). Indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama

CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS.
- Al escuchar un CTS, hay que espera según la longitud.

La solución final de 802.11 es utilizar el protocolo MACA con CSMA/CA para enviar los RTS y CTS.

4.2.2.7 CONFIGURACIONES WLAN

El grado de complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que quisiéramos implementar, podemos utilizar diversas configuraciones de red.

a) Redes Ad-Hoc

La configuración más básica es la llamada **de igual a igual o ad-hoc** y consiste en una red de terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. En la figura se muestra un ejemplo. Para que la comunicación entre las estaciones sea posible hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra. Las redes de tipo **ad-hoc** son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa.

Las redes ad-hoc, como se observa en la figura siguiente, normalmente están compuestas de dos o más dispositivos que son similares entre ellos, por ejemplo computadoras, sensores, etc. Con tarjetas 802.11x integradas. Una red ad-hoc se la conoce como un conjunto de servicios básicos independientes IBSS (Independent Basic Service Set), donde independiente se refiere a que no existen puntos de acceso.



Fig. Nro: 13 Redes Ad Hoc⁽¹³⁾

b) Redes de Infraestructura

Estas configuraciones utilizan el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, que para aumentar el alcance, hace falta la instalación de un **punto de acceso**. Con este nuevo elemento doblamos el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso). En la Figura se muestra un ejemplo. Además, los puntos de acceso se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos. Para dar cobertura en una zona determinada habrá que instalar varios puntos de acceso de tal manera que podamos cubrir la superficie necesaria con las celdas de cobertura que proporciona cada punto de acceso y ligeramente solapadas para permitir el paso de una celda a otra sin perder la comunicación.

Los **Puntos de acceso** son colocados normalmente espaciados, pero es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan. Un único punto de acceso puede soportar un pequeño grupo de dispositivos y puede funcionar en un rango de al menos treinta metros, a cientos de metros.

La técnica de **Punto de acceso** es capaz de dotar a una red inalámbrica de muchas más posibilidades. Además del evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como **roaming**, es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas. En la siguiente figura, se observa una red de infraestructura, integrada por varios puntos de acceso industrial y dispositivos inalámbricos.

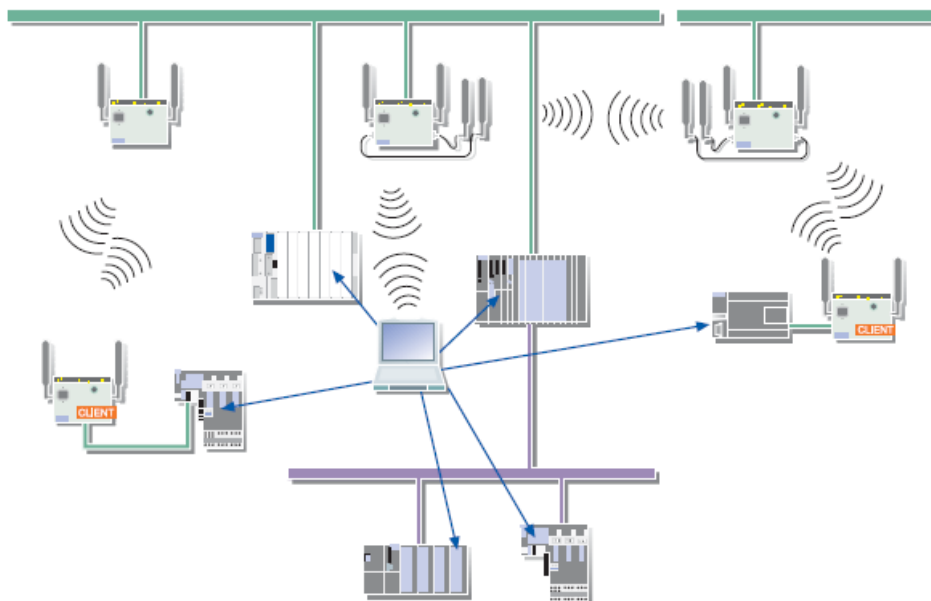


Fig. Nro: 14 Red de Infraestructura ⁽¹⁴⁾

4.2.2.8 DISPOSITIVOS PARA COMUNICACIONES INDUSTRIALES

Las redes inalámbricas 802.11 x, se configuran habitualmente entorno a un dispositivo denominado punto de acceso. Este dispone normalmente de una conexión para una red Ethernet cableada, permitiendo la integración con los dispositivos inalámbricos.

El punto de acceso soporta entre 20 y 50 dispositivos inalámbricos que estén dentro de su radio de acción, que dependiendo de las condiciones del edificio pueden alcanzar hasta los 100 metros. Si hay que extender el alcance se puede unir más puntos de accesos a la red cableada, lo cual permite conectar a los dispositivos móviles inalámbricos, según su situación con el punto de acceso más próximo. También existen elementos para extender el alcance de la red, utilizando un punto de acceso con una antena direccional, lo cual permite propagar la señal a zonas más lejanas.

En la Figura Nro: 15, se puede observar los diferentes dispositivos, sensores, actuadores, instrumental de proceso, etc., que forman parte de una red inalámbrica industrial.

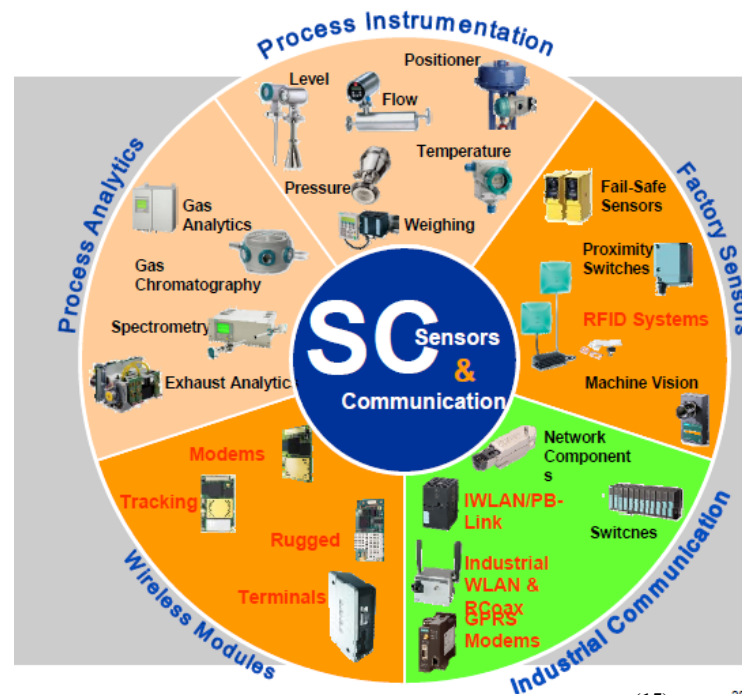


Fig. Nro: 15 Dispositivos para Redes WLAN ⁽¹⁵⁾

4.2.2.9 SEGURIDAD DE LA RED INALAMBRICA

Para mantener la seguridad de las transmisiones se ha desarrollado un algoritmo de codificación denominado WEP (Wired Equivalent Privacy), basado en el algoritmo RC4, el cual presenta claves simétricas de 64 y 128 bits, reforzándolo con el cambio de las claves de los puntos de acceso y computadoras de la red en forma periódica.

Otro método para aumentar la seguridad, es limitar el acceso a los dispositivos que tengan direcciones de red conocidas, como así también utilizar el sistema Radius

(Remote Authentication Dial – In User Service), para la autenticación de los usuarios que acceden a la red o la alternativa WPA (Wi – FI Protected Access).

4.2.2.10 OTRAS CARACTERISTICAS DE LA NORMA IEEE 802.11

Otras características de la norma son las siguientes:

- Permite la conexión en red de dispositivos portátiles (notebook, PDAs, Tablet PCs, teléfonos por VoIP, sensores, actuadores, etc.).
- Facilita la instalación de nuevas redes, en zonas que no cuentan con la infraestructura adecuada.
- Utilización de la Norma ISA SP 100.11a, la cual provee de mecanismos de encriptación para garantizar la seguridad contra intrusiones, interceptaciones y/o sabotaje.

4.2.3 REDES-(WI-FI MAN)

Estas redes dependen de la infraestructura y requerimiento de las empresas, la más conocida son las redes **WI-MAX IEEE 802.16**. Se aplican en redes metropolitanas de acceso inalámbrico no móviles, como se observa en la Figura Nro: 16. Lo que el proveedor del servicio denomina “la última milla”, cubriendo frecuencias de 10 a 66 Ghz.

El IEEE 802.16 ha sido diseñado específicamente para topologías punto a multipunto en ambientes abiertos que con un mismo control de acceso al medio (MAC) que puede acomodar diferentes capas físicas (PHY) en el rango de frecuencia de 2 a 66 GHz. IEEE aprobó el estándar inicial de IEEE 802.16 para las redes MAN inalámbricas en el rango de frecuencias 11-66 GHz en diciembre de 2001. La extensión 802.16a para frecuencias inferiores a 11 GHz fue aprobada en enero de 2003.

El estándar 802.16-2004 fue ratificado por el IEEE en junio de 2004. El estándar 802.16e fue ratificado por IEEE en diciembre de 2005. El propósito del 802.16e es agregar soporte a la movilidad al estándar 802.16d anterior, que se diseñó específicamente para operación fija.

En términos simples, aunque la técnica de modulación cambia dependiendo de la frecuencia de la operación, el formato del paquete de datos, el acceso al medio o las técnicas de control de errores son independientes de la frecuencia de operación. La “electrónica” utilizada en la capa MAC (ISO, capa 2, enlace) del IEEE 802.16 MAC es independiente de la frecuencia de operación.

IEEE 802.16 no solo apunta a satisfacer los WISP y los requerimientos de la industria en todos los posibles escenarios sino que aspira a volverse el estándar “de facto” para acceso inalámbrico. Esto no necesariamente quiere decir que otras tecnologías se volverán automáticamente obsoletas. En muchos casos la discusión es sobre la eficiencia espectral, aspectos regulatorios, acceso a la tecnología o costos de inversión.

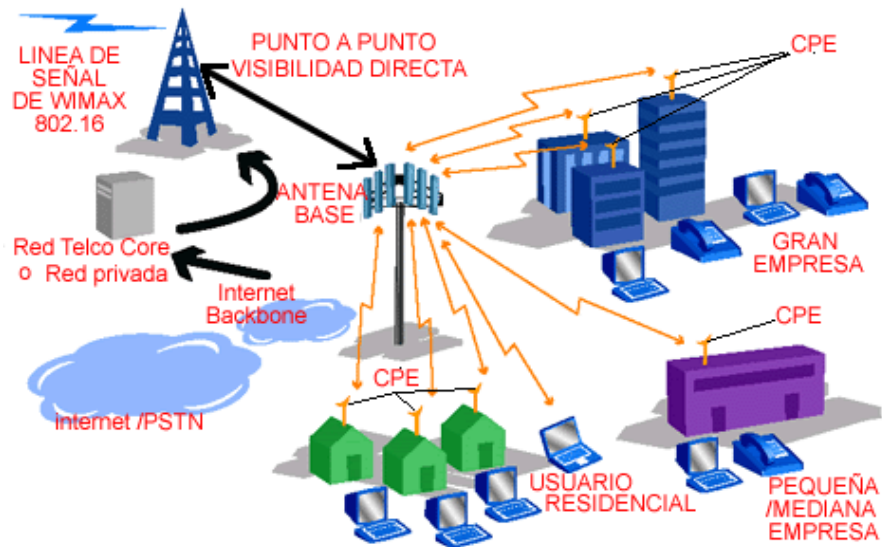


Fig. Nro: 16 Componentes de un sistema WiMAX ⁽¹⁶⁾

4.2.4 REDES WWAN (WI-FI Wide Area Network)

Como puede observarse en la Figura Nro: 17, las redes inalámbricas que integran este bloque, pueden emplearse como apoyo a las redes de comunicaciones industriales:

- **GSM** (Groupe Special Mobile).
- **EDGE** (Enhanced Data rates for GSM of Evolution (Tasas de datos mejoradas para la evolución de GSM)).
- **HSCSD** (High-Speed Circuit-Switched Data).
- **UMTS** (Universal Mobile Telecommunications System), Sistema Universal de Telecomunicaciones Móviles.
- **GPRS** (General Packer Radio Service).

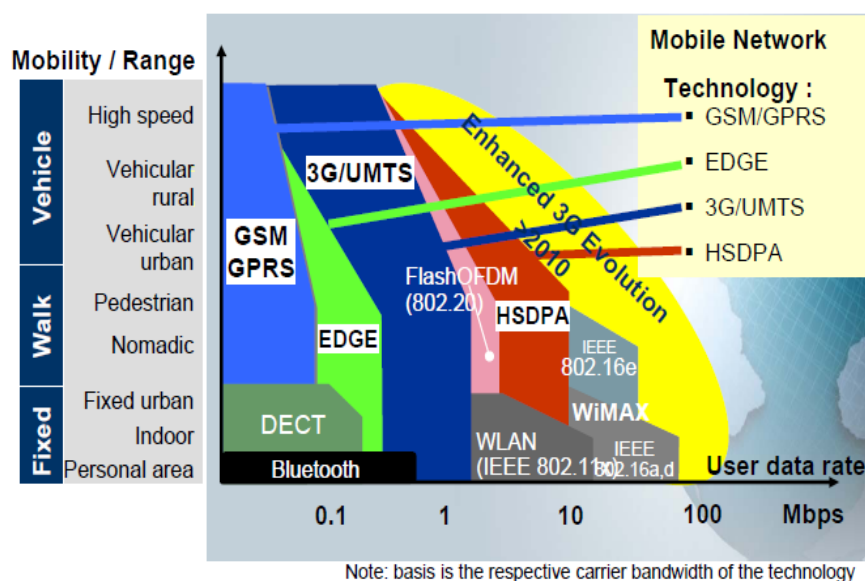


Fig. Nro: 17 Redes WWAN ⁽¹⁷⁾

4.2.4.1 RED GSM

Es un sistema estándar. Completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital. Por ser digital cualquier cliente GSM puede conectarse a través de su teléfono con una computadora, y puede enviar o recibir mensajes vía e-mail, faxes, navegar por Internet, tener acceso seguro a la red informática de una empresa (LAN/Intranet), como puede observarse en la Figura Nro: 18, así como utilizar otras funciones digitales de transmisión de datos, incluyendo el Servicio de Mensajes Cortos (SMS) o mensajes de texto.

GSM se considera por su velocidad de transmisión y otras características, un estándar de segunda generación (2G). Su extensión a 3G se denomina UMTS, que posee mayor velocidad de transmisión, una arquitectura de red distinta y sobre todo utiliza el protocolo de radio W-CDMA.

Su utilización en el entorno industrial, esta especialmente orientada a la información de alarmas, que se produzcan en un proceso, a los encargados del sistema de supervisión y control.

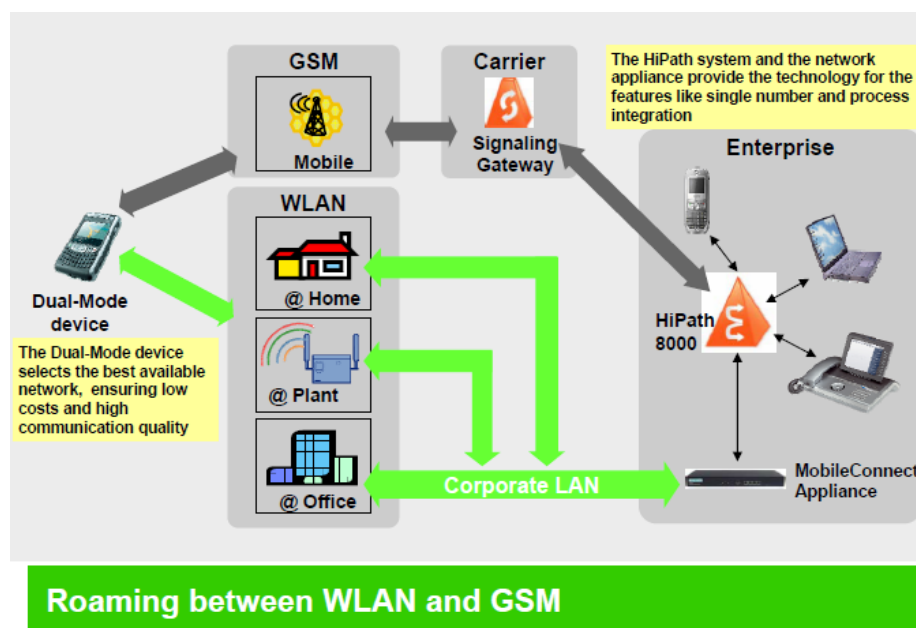


Fig.Nro: 18 Integración WLAN con GSM ⁽¹⁸⁾

4.2.4.2 REDES EDGE

Es una tecnología Mobil celular también conocida como EGPRS (Enhanced GPRS), actúa como puente entre las redes 2G y 3G, se considera una evolución de GPRS. Esta tecnología funciona con cualquier red GSM que tenga implementado GPRS, puede ser usado en cualquier transferencia de datos basada en conmutación por paquetes (Pack Switched), como la utilizada en Internet.

Su utilización en el entorno industrial, como muestra la Figura Nro: 19, es igual que GSM.

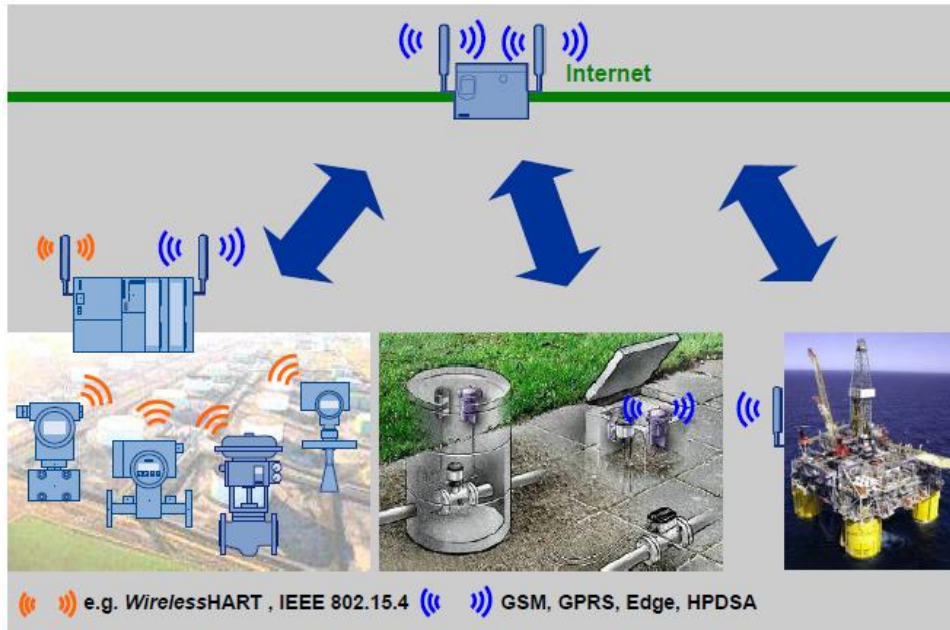


Fig. Nro: 19 Integración de Internet con: EDGE, GSM, GPRS, etc. ⁽¹⁹⁾

4.2.4.3 REDES HSCSD

Es una mejora a de la tecnología CSD, que hace al mecanismo de transferencia de datos de los dispositivos GSM cuatro veces más rápido, con velocidades de hasta 38,4 Kbps. La diferencia es la habilidad para usar diferentes métodos de codificación y/o múltiples puertos para incrementar la transferencia de datos.

Una diferencia importante es que admite diferentes métodos de corrección de errores para la transferencia de datos, que pueden ser usados de acuerdo a la calidad del enlace. Otra innovación es la habilidad de usar varios puertos a la vez, con un máximo de cuatro puertos, incrementando la velocidad máxima de transferencia de datos a 57,6 Kbps, mejorando su rendimiento en lugares de malas condiciones de recepción de señales.

Su aplicación en el entorno industrial, es igual que GSM.

4.2.4.4 REDES UMTS

Sistema Universal de Telecomunicaciones Móviles (por sus siglas en inglés UMTS) es una tecnología inalámbrica de voz y datos de alta velocidad que integra la familia de normas inalámbricas de tercera generación (3G) IMT-2000 de la Unión Internacional de Telecomunicaciones (UIT). La tecnología radial utilizada en UMTS es la WCDMA, o CDMA en banda amplia.

UMTS es una tecnología basada en Protocolo de Internet (IP) que da soporte a voz y datos, con velocidades de hasta 2 Mbps y velocidades promedio de 220 a 320 Kbps cuando el usuario se encuentra caminando o conduciendo.

UMTS está diseñada para conectar servicios ávidos de ancho de banda tales como, streaming multimedia, transferencias de archivos pesados y video-conferencia a una gran variedad de dispositivos, entre ellos teléfonos celulares, PDAs y computadoras portátiles. **UMTS** utiliza una combinación de las tecnologías Acceso Múltiple por División de Código (**CDMA**) y Acceso Múltiple por División de Tiempo (**TDMA**) para hacer un uso altamente eficiente del espectro.

Los servicios 3G combinan el acceso móvil de alta velocidad con los servicios basados en el protocolo IP. Pero esto no sólo conlleva una conexión rápida con la World Wide Web, sino que implica además nuevas formas de comunicarse, de acceder a la información, de hacer negocios y de aprender, dejando a un lado las conexiones lentas, los grandes terminales y los puntos de acceso fijos. Con la 3G se pueden realizar múltiples conexiones simultáneamente desde un mismo terminal móvil. Así, por ejemplo, un usuario podría conectarse a una base de datos remota para obtener información sin necesidad de interrumpir una sesión de videoconferencia.

4.2.4.5 REDES GPRS

GPRS (General Packet Radio Service), el criterio seguido en estas redes para su desarrollo, es ofrecer comunicación IP sobre la red de distribución actual de GSM. De esta forma se reduce el costo de las inversiones y se introduce un paso previo, a la llegada de la telefonía 3G o UMTS. La implantación de esta técnica supone una importante revolución para las comunicaciones móviles industriales. Las aplicaciones M2M (Machine to Machine) y H2M (Human to Machine) pueden aprovechar las ventajas de esta tecnología.

Fundamentalmente existen las siguientes ventajas sobre la tecnología **GPRS**:

- Incremento de la velocidad

Ya hay en el mercado dispositivos industriales capaces de soportar 85.6 Kbps de "bajada" y 21.4Kbps de "subida". Estas tasas de transferencia suponen un incremento importante respecto a la velocidad disponible en GSM. Naturalmente esta velocidad no es comparable a la que puede ofrecer UMTS, pero supone un paso más hacia la capacidad de transferir volúmenes considerables de información y cubre las necesidades del mercado industrial.

“Always On”

Desde el momento en que el equipo remoto (terminal, datalogger, etc.) se registra en la red **GPRS** éste no necesita ser reconectado. Aún en el caso de perder la "cobertura" **GPRS**, cuando ésta vuelve a estar disponible, las unidades remotas siguen trabajando en ese entorno. Las características de funcionamiento son similares a las de TCP/IP y esto debe garantizar que la información siempre llega a su destino.

En definitiva el gran avance que introduce **GPRS** para las comunicaciones industriales viene determinado por la posibilidad de dotar a cualquier dispositivo, en cualquier sitio, con soporte a Internet sin necesidad de cables. Para acceder a esta funcionalidad tan solo se necesita conectar el módem a un ordenador tipo PC o que la electrónica asociada soporte TCP/IP.

Servicios ofrecidos:

La tecnología **GPRS** mejora y actualiza a GSM con los servicios siguientes:

- Servicio de mensajes multimedia (MMS)
- Mensajería instantánea
- Aplicaciones en red para dispositivos a través del protocolo WAP
- Servicios P2P utilizando el protocolo IP
- Servicio de mensajes cortos (SMS)
- Posibilidad de utilizar el dispositivo como módem USB

La tecnología **GPRS** se puede utilizar para servicios como el acceso mediante el Protocolo de Aplicaciones Inalámbrico (WAP), el servicio de mensajes cortos (SMS) y multimedia (MMS), acceso a Internet y correo electrónico.

En la siguiente figura, se observa el enlace entre dos redes Lan industriales de una empresa, a través de un router GPRS.

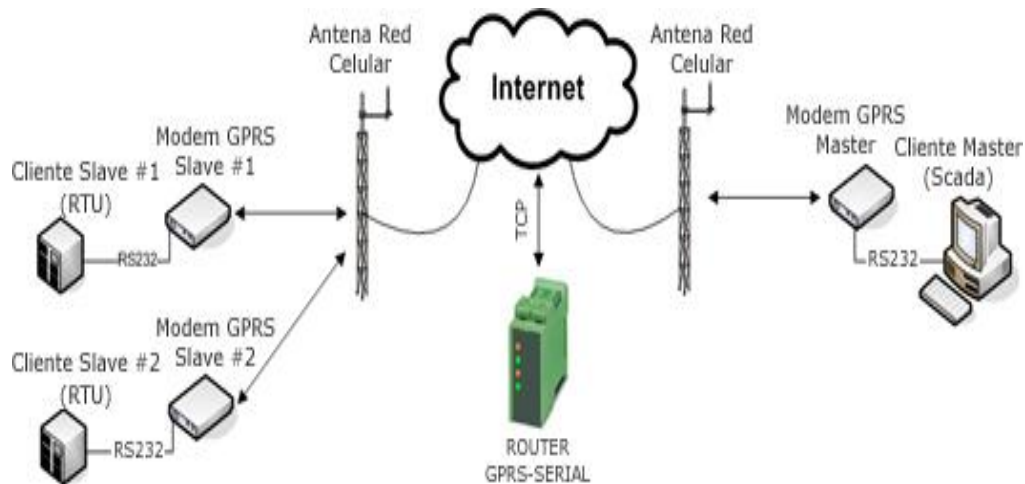


Fig. Nro: 20 Conexión Red GPRS a una Red Industrial ⁽²⁰⁾

4.3 REDES IWLAN (Industrial Wireless)

Después de haber hecho una descripción de los diferentes sistemas de enlaces inalámbricos existentes en la actualidad, su utilización en las comunicaciones de los diferentes procesos industriales, y teniendo presente la capacidad gráfica que tienen los dispositivos móviles, aplicados a la consulta del estado y control del proceso, mediante diferentes pantallas creadas ex profeso, tienden a eliminar en un futuro no muy lejano el alambrado físico entre los dispositivos de campo, ya que todas las señales de medición y diagnóstico, se enviarán en forma inalámbrica.

Las redes locales inalámbricas industriales (**IWLAN**) no solo proveen comunicación de acuerdo al estándar IEEE 802.11 x, sino que además están preparadas para salvar los problemas que se les presentan con los enlaces inalámbricos convencionales que son los siguientes:

- Pérdida de potencia de la señal con la distancia.

- Overheads en la capa física, preámbulos de las tramas más largos para facilitar la sincronización en un canal ruidoso.
- Errores en el canal, debido a reflexiones o desvanecimientos de la señal, lo que causa: Interferencias entre símbolos y desvanecimiento por múltiples trayectorias.
- Errores en el canal debido a ruidos, interferencias con otros canales u otras transmisiones, ruidos inducidos en el transceptor por causa de un ambiente adverso.
- Problema de estación oculta y problema de estación expuesta.

Por lo tanto las redes **IWLAN** cuentan con muchas funcionalidades adicionales, imprescindibles para la industria.

En estas redes, la confiabilidad del canal se convierte en un factor muy importante a tener en cuenta. A diferencia del entorno ofimática o de uso masivo, en la industria la pérdida de comunicación de un equipo significa costos importantes. Para atender esta situación, las prestaciones industriales cuentan con los siguientes recursos:

4.3.1 MONITOREO DEL CANAL INALÁMBRICO

En el estándar IEEE 802.11 se requiere monitorear la calidad del enlace inalámbrico, este factor tiene un efecto considerable en la confiabilidad. Si un equipo móvil se utiliza para el diagnóstico o monitoreo de una maquina, es muy importante permitirle al administrador u operador conocer su estado de conexión.

Por ejemplo, si en un proceso industrial, la PDA inalámbrica pierde su conexión radial, es necesario que el administrador este informado de este evento y tome el control de la función que este dispositivo estaba realizando en el proceso. Esta situación se puede dar cuando el canal inalámbrico esta muy degradado o cuando simplemente el dispositivo se desplaza hasta quedar fuera de la célula (por ejemplo, la ubicación B de la figura) y se queda sin conexión inalámbrica.

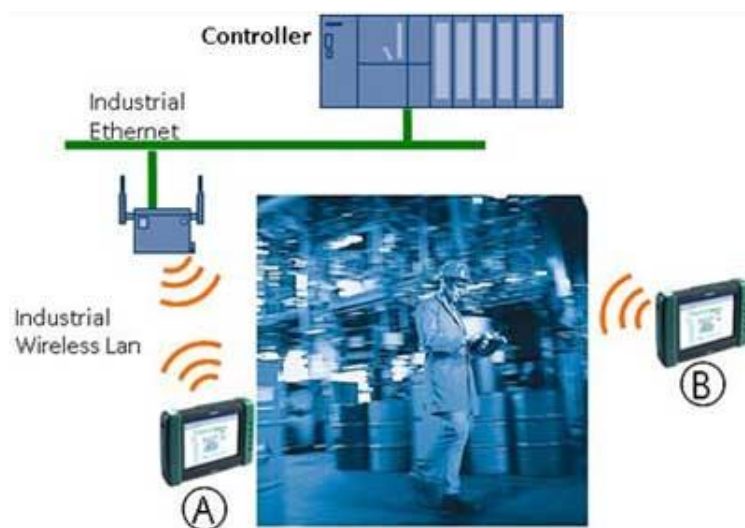


Fig. Nro: 21 Monitoreo del canal inalámbrico ⁽²¹⁾

Al ocurrir este evento el Access Point debería enviar un mensaje utilizando el protocolo SNMP (Protocolo TCP/IP para administrar redes) o un e-mail, utilizando el protocolo SMTP (Protocolo de correo simple) al administrador de la red, avisándole del acontecimiento. También esta la opción, de que en forma cíclica se interroge el estado de los dispositivos, y ante cualquier evento, ejecute un aviso o alguna alarma especial.

En IWLAN existen dos métodos para chequear el estado de un enlace:

a) “Link Check”

Este método trabaja de la siguiente forma: cuando no hay comunicación, (como se observa en la Figura Nro: 22, se están enviando tramas a un determinado nodo a intervalos cíclicos seleccionables para verificar su presencia en la red inalámbrica, aunque el método reduce un poco el desempeño del sistema, provee un alto grado de confiabilidad operativa.

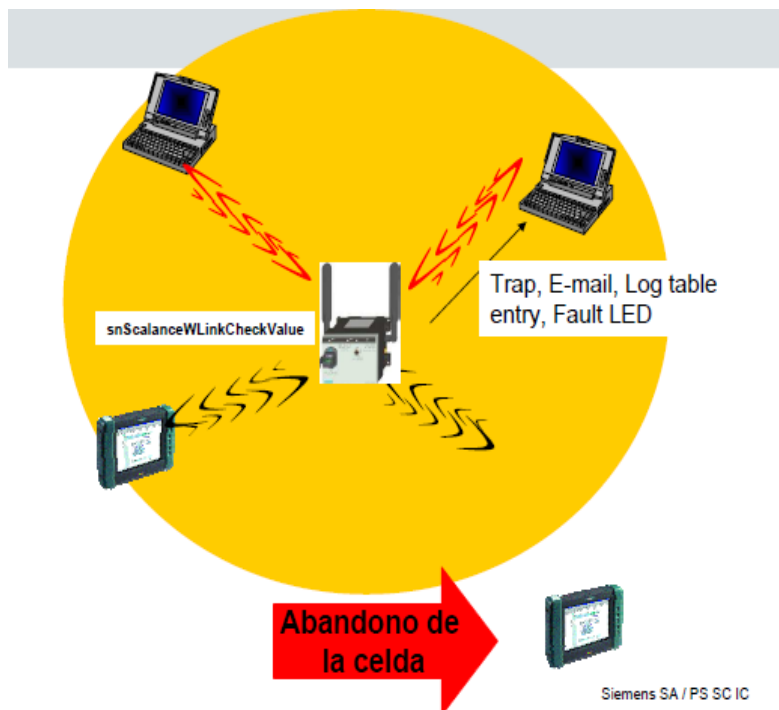


Fig. Nro: 22 Vigilancia de la conexión (Link Check) ⁽²²⁾

b) “IP-Alive ”

Este procedimiento monitorea conexiones con comunicación cíclica, que son muy comunes en las aplicaciones de automatización. En las direcciones IP seleccionadas, la función de monitoreo revisa si los paquetes realmente se intercambian en los tiempos prescritos para cada ciclo. Si se pierden paquetes, se pueden reportar errores de la misma manera que el mecanismo de “Link Check”, el usuario puede definir la forma más apropiada de dar la alarma (encendido de un led de error, archivo de errores, email, SNMP Trap, etc.).

4.3.2 **DETERMINISMO Y TIEMPO REAL**

Las **WLAN** implementadas de acuerdo a la norma IEEE 802.11, proveen una conexión inalámbrica muy potente que por si solas satisfacen las necesidades hogareñas y de oficina.

Sin embargo, su especificación básica no contempla aplicaciones en tiempo real o de requerimientos determinísticos. **WLAN**, según IEEE 802.11, establece un medio en el cual todas las estaciones deben compartir el acceso al mismo. Aunque el acceso es controlado, no es totalmente predecible.

Con el método de determinismo y tiempo real, **IWLAN**, provee la opción de garantizar, tanto una tasa de transferencia mínima como una tasa de “peor caso”, para clientes seleccionados (mediante Calidad de Servicio – Quality Of Service – QoS). Estos parámetros son negociados previamente al establecer la comunicación.

A continuación se muestran dos ejemplos:

Ejemplo 1: Trafico Cíclico de Datos

En la configuración antes descrita, el operador desea estar seguro de que un nodo es capaz de enviar paquetes de longitud de 64 bytes cada 50 ms. desde el enlace **WLAN** al controlador central. Por lo tanto se deben considerar los siguientes parámetros:

a) Tiempo de Transmisión (tiempo de respuesta).

El requisito de 50 ms. es el tiempo durante el cual los datos no se deben apilar en el nodo. Luego de 50 ms., el último BIT del paquete previo debe haber sido transmitido antes de transmitir el siguiente paquete de 64 BIT.

b) Tasa de Transferencia (ancho de banda).

Si se van a transmitir 64 bytes en 50 ms., se requerirá al menos una tasa de transferencia de: $(64 \text{ BIT} \times 8 \text{ bits/BIT}) / (50\text{s}/1000) = 10,24 \text{ Kbps}$. Este seteo asegura que no se produzcan cuellos de botella en el sistema y que el tráfico cíclico de datos pueda ser transmitido al controlador central sin complicaciones.

Ejemplo 2: Transferencia de Archivos

Si el nodo tiene un archivo de 1 Mbit de tamaño, se puede lograr una transferencia de duración predecible con los siguientes ajustes:

a) Tiempo de Transmisión (tiempo de respuesta).

Dado que se puede esperar un tiempo del orden de los segundos, la latencia del canal inalámbrico no es un factor muy importante. Se puede elegir un tiempo de 500 ms.

b) Tasa de Transferencia (ancho de banda)

Si se ajusta una tasa de transferencia de 500 Kbps, todo el archivo se podrá transmitir en: $(1 \text{ Mbit} \times 8 \text{ bits/BIT}) \times 106/500 \text{ Kbps} = 16 \text{ segundos}$, el hecho de que los paquetes individuales teóricamente puedan tener una latencia de 50 ms. no juega aquí ningún rol especial.

Al reservar la tasa de transferencia se deben tener en cuenta las siguientes restricciones:

- 1- La tasa neta de transferencia de la red se toma en base a la de la conexión Ethernet. La sobrecarga del protocolo dado por la transmisión inalámbrica no es necesario tenerla en cuenta.
- 2- Cuando una estación inalámbrica se pasa a otra célula, toma cierto tiempo para quedar configurada como “cliente crítico” con el nuevo Access Point (AP). Esta fase puede tardar hasta varios centenares de milisegundos. Durante este tiempo, no hay tráfico productivo de datos y en ese intervalo, es donde la estación queda desconectada, se debe evaluar la criticidad de esta circunstancia para, eventualmente, emplear mecanismos de comunicación especiales que faciliten el “Rapid Roaming” donde el tiempo de traspaso puede llegar a durar aproximadamente 20 ms.
- 3- Los parámetros entregados a una determinada estación pueden mejorarse según la utilización del ancho de banda, por ejemplo: si a una estación se le otorga 2,4 GHz y 54 Mbps, siendo sus atributos de 100 ms. y 500 Kbps, esto se puede mejorar si en el canal no transmite ninguna otra estación.
- 4- El intercambio de datos es Full Duplex.
- 5- Se provee prioridad a las tramas de datos, por ejemplo que todo el tráfico de voz tenga prioridad sobre otros tipos de datos.

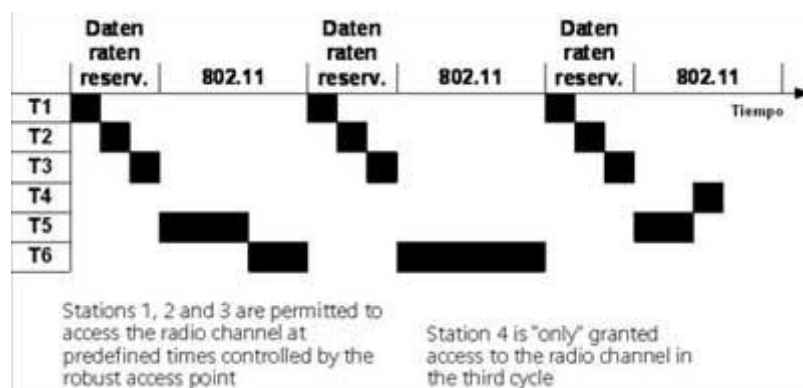


Fig. Nro: 23 Mecanismo de conexión ⁽²³⁾

En la Figura Nro: 23, se muestra que 6 estaciones (clientes 1 al 6) están conectadas a un Access Point. Si una aplicación requiere que los clientes 1, 2 y 3 (por ejemplo, controladores móviles) se comuniquen con el resto de la planta utilizando un enlace **WLAN**, se debe garantizar que estos controladores puedan mandar mensajes de estado en determinados ciclos fijos.

Esto es posible solo si esta disponible un mecanismo adicional que asigne el derecho de transmisión. Reservando tasa de transmisión, los clientes 1 y 3 tienen la oportunidad de acceder al Access Point en la primera fase, a pesar de que los clientes 4 y 5 tengan largos archivos para transmitir pendientes. Esto se continúa con un periodo durante el cual el resto de las estaciones transmiten cuando le corresponde, de acuerdo a las reglas normales, en la figura se muestra, primero el cliente 5 y luego el 6. A continuación se sucede de nuevo la transmisión de las estaciones con tasa de datos reservada que requieren acceder al Access Point con prioridad. Se aprecia que el cliente 4 es “víctima” del método de acceso de IEEE 802.11. Dado que no es un cliente con prestación previamente configurada y asegurada (que sería asignarle QoS), debe esperar hasta que los clientes 5 y 6 hayan transmitido sus datos completamente.

En el ejemplo de la figura se deja claro que en **WLAN** transmiten estaciones que pueden ser tanto compatibles con el estándar de tráfico **WLAN** como también con tráfico de datos con prioridad.

4.3.3 ROAMING FORZADO

La norma IEEE 802.11 no especifica que un Access Point deba estar conectado a la red cableada de Ethernet. Aun más, ni siquiera especifica que deba estar disponible una red cableada. Esto significa que una estación de la célula no necesariamente pueda reconocer que en su interfase se asigne o agregue una conexión cableada, lo que puede implicar consecuencias inestimables, por ejemplo, si la estación es un controlador móvil que envía datos importantes del proceso a la sala de control.

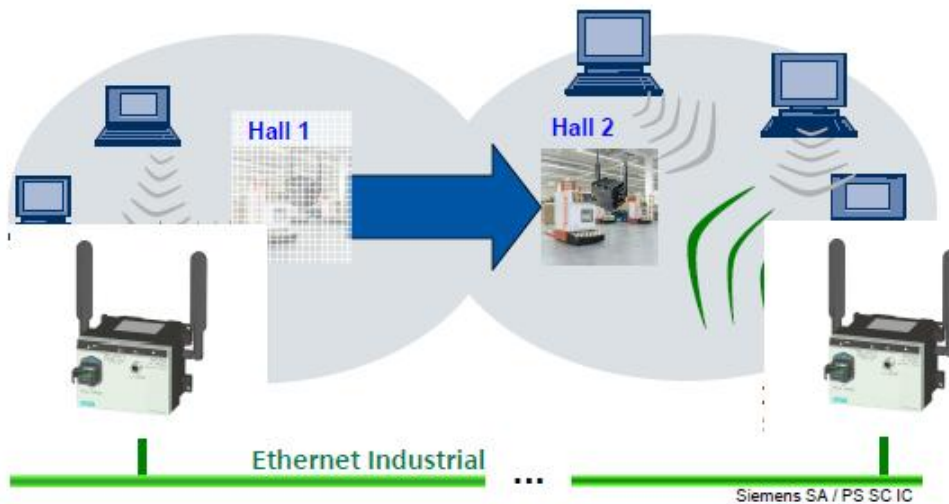


Fig. Nro: 24 Comunicación iWLAN Rapid Roaming (RR) ⁽²⁴⁾

La Figura Nro: 24, muestra cuando la conmutación entre los dos puntos de acceso, se produce sin interrupción de la comunicación.

La tecnología de **Rapid Roaming (RR)** es una extensión de **IWLAN**, es un protocolo alternativo denominado iPCF (Industrial Point Coordinated Function) y cuyo procedimiento se basa en que un Access Point, mediante ciclos de polling muy cortos, asigna “ventanas” temporales de comunicación a sus clientes, logrando tiempo de respuestas estables, predecibles y donde el uso del ancho de banda es sumamente más

eficiente que si se viese obligado a realizar el polling por diferentes canales, el precio es perder algunos servicios de comunicación que no son requeridos para estas aplicaciones.

Así se puede proveer al sistema comunicación inalámbrica real-time critica cuando se requieren tiempo de transmisión del orden de 10 a 100 ms. Mediante chips de comunicación especiales (ERTEC, Enhanced Real Time Ethernet Controller) se logra garantizar además comunicación determinística, y esta tecnología permite en forma apropiada transmitir sobre enlaces inalámbricos, señales críticas, como marcha y parada de maquinas, posicionamiento y sincronización de ejes.

Es importante tener en cuenta que los estándares comerciales 802.11 no cuentan con esta función específica, para ello existen Access Point duales que permiten por un lado, transmitir **IWLAN** estándar y por otra vía **IWLAN RR**, en una configuración denominada “**shadow cell**”.

IWLAN RR, aparte de lo explicado en la figura anterior, se orienta a la solución de sistemas que se desplazan a altas velocidades y que se deben automatizar y controlar en forma remota. Esto sucede habitualmente en los sistemas robotizados y de traslado de mineral sin conductores a bordo y cuando estos deben atravesar regiones extensas cubierta por varios Access Point, debiendo conmutar de uno a otro en forma dinámica, como se observa en la Figura Nro: 25.

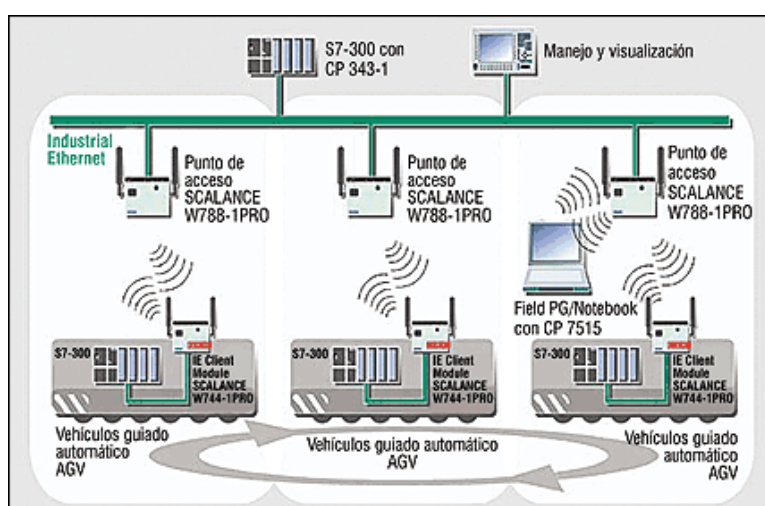


Fig. Nro: 25 Rapid Roaming con estaciones móviles (25)

El determinismo con que la tecnología **IWLAN RR** maneja las tramas críticas de transmisión de señales permite que se reserve ancho de banda para la transmisión de otras tramas que si bien requieren sincronismo y determinismo no son tan críticas, como lo es el protocolo de voz sobre IP (VoIP), asignando apropiada y automáticamente la calidad de servicios que cada uno de éstos exige.

4.3.4 MODOS DE CONEXIÓN Y OPERACIÓN

4.3.4.1 SISTEMA DISTRIBUIDO INALÁMBRICO

Si se necesita actualizar una red **IWLAN** de una planta, a veces no es suficiente con conectar un Access Point (AP) sobre Ethernet para establecer la comunicación más

allá de los límites de la célula. Sino que hay que salvar previamente las siguientes dificultades: el equipo adicional no esta disponible; no hay canales disponibles y la instalación es dificultosa, (por ejemplo, en áreas inhóspitas).

En tales circunstancias, los Access Points se pueden utilizar en modo de Wireless Distribution System (WDS) sin necesidad de cablearlos.

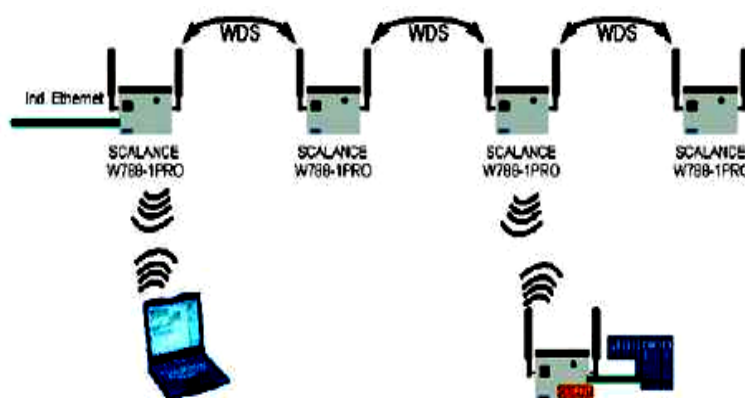


Fig. Nro: 26 Sistema WDS ⁽²⁶⁾

En el modo WDS, es importante que un AP pueda ver a sus vecinos (de otra manera la cadena se interrumpiría). Esto puede requerir la utilización de antenas especiales distantes en reemplazo de las antenas normales integradas.

En la Figura Nro: 26, las estaciones son capaces, perfectamente, de tomar parte de las operaciones en este modo. Surge una propiedad importante de esta configuración que es que las estaciones y los Access Points deben compartir la totalidad de la tasa de transferencia disponible. Esta situación se puede tornar aun más crítica porque en el modo WDS, todos los AP y las estaciones operan en el mismo canal inalámbrico (por ejemplo 802.11g y canal 1, en 2.4 GHz y 54Mbps). Esta restricción puede tener consecuencias para la aplicación.

De esta forma, deberían evitarse aquellas aplicaciones donde se requiera una alta tasa de transferencia para una gran cantidad de estaciones (por ejemplo un Hot Spot en un local comercial o público). Por el contrario, en aplicaciones donde la red inalámbrica es accedida por controladores PLCs (que transmiten en el orden de 100Kbps) o equipos HMI (que puedan llegar a los Mbps) y donde el manejo de archivos es poco usual, no es de esperarse cuellos de botella significativos.

La configuración WDS del esquema anterior se puede mejorar si se utilizan Access Points del tipo dual.

De esta manera, una tarjeta inalámbrica se puede utilizar para establecer una infraestructura inalámbrica central (o Backbone) y la otra tarjeta provee conectividad a la célula de la estación local para que tenga acceso a la infraestructura inalámbrica.

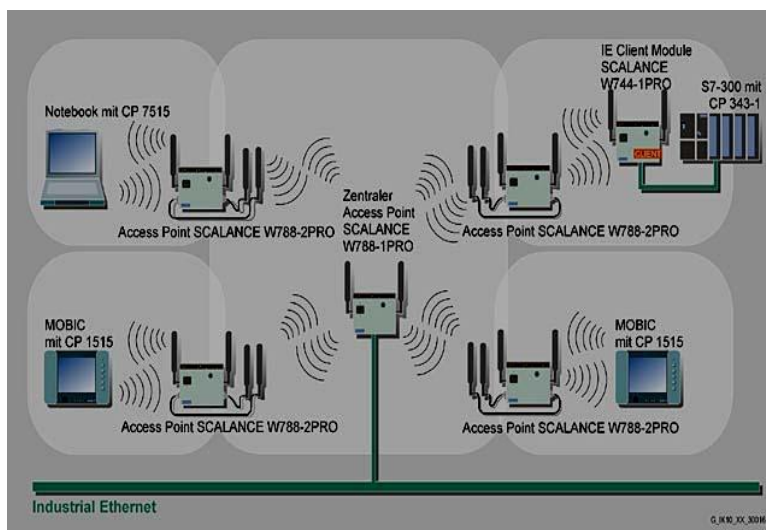


Fig. Nro: 27 Enlace con Access Point central ⁽²⁷⁾

Una WDS se puede dejar implementada con un Access Point central y una tarjeta de conexión inalámbrica en cada uno de los cuatro enlaces disponibles para la red cableada. Como se mostró en la figura anterior, el Access Point dual implementa una red inalámbrica “local” en el lugar donde esta instalado, que le sirve de interfase inalámbrica al resto de las estaciones. WDS provee de nuevo el Backbone de la infraestructura inalámbrica.

4.3.4.2 UTILIZACIÓN DE CABLES DE RADIACIÓN COAXIAL (RCOAX)

Existen condiciones donde el rango de transmisión/recepción de las antenas convencionales de los Access Point no se puede cubrir una cierta área, por ejemplo en determinadas plantas industriales, túneles o vehículos que se desplazan sobre rieles.

En estas situaciones se aprovecha el hecho de que los cables pueden emitir radiaciones electromagnéticas, si estos poseen un diseño apropiado.

En estas situaciones la tecnología de los cables RCoax, permiten extender, concentrar y dirigir la radiación electromagnética de un Access Point, de manera que su campo de iluminación se extienda geométricamente dentro de una zona de interés para la planta que se desea comunicar.

En los casos donde se desplazan vehículos móviles, como se observa en la Figura Nro: 28, el cable se extiende paralelo a la trayectoria de dichos vehículos, evitando así la dispersión de la radiación en direcciones que no son de provecho, y en los túneles, donde se necesita la transmisión inalámbrica para agentes de mantenimiento, servicios técnicos y alarmas, el cable RCoax permite que la radiación se emita longitudinalmente y en forma paralela al desplazamiento del vehículo, focalizando la transmisión al interior.

Esta tecnología en conjunto con **IWLAN**, permite reemplazar la comunicación por cables o por los mismos rieles, haciéndola más eficiente y segura.

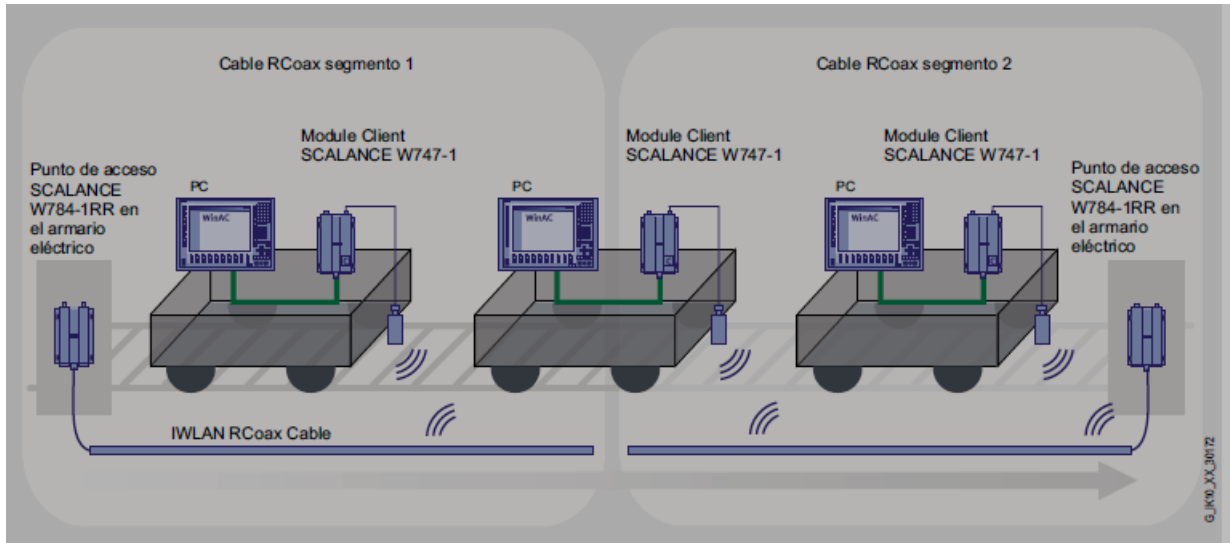


Fig. Nro: 28 Aplicación RCoax. Comunicación de carros móviles. (28)

4.3.4.3 OPERACIÓN EN MODO PUENTE (BRIDGE)

En los ambientes industriales, es frecuente el caso en que una parte descentralizada de la planta se comunica a la red principal a través de un enlace punto a punto. Para esta situación, se utiliza el modo puente (Bridge), un caso especial de sistema distribuido inalámbrico. Para esto, normalmente se utilizan antenas direccionadas de manera que la propagación de ondas se efectúe optimizada para el enlace punto a punto.

Para vincular la parte aislada de la planta, se tiene disponible todo el ancho de banda de la **WLAN**, si se utiliza solamente el enlace inalámbrico direccionado.

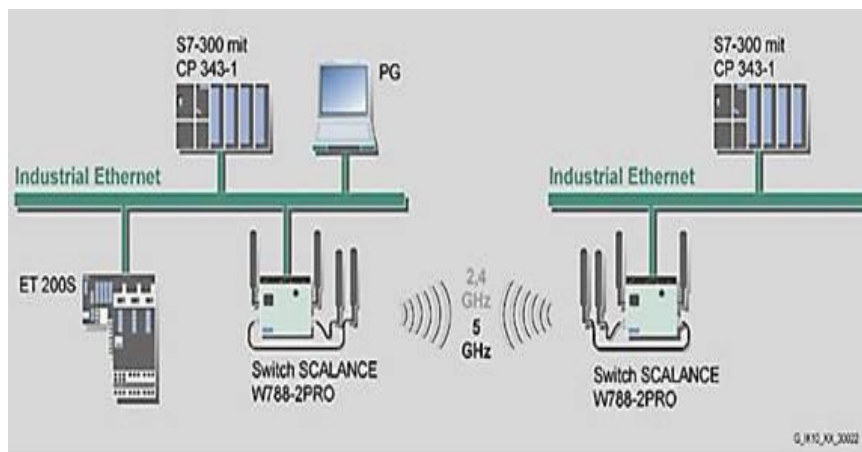


Fig. Nro: 29 Operación en modo puente (Bridge) (29)

En la figura anterior, se muestran dos redes conectadas, (se supone que cada red implica una gran extensión con muchos usuarios adheridos). En el enlace inalámbrico direccionado no pueden incluirse células dedicadas.

4.3.4.4 OPERACIÓN EN MODO REDUNDANTE

En la figura anterior, el enlace inalámbrico conecta dos partes importantes de la planta, lo que implica que por este enlace se transporta información vital y que, en consecuencia, la interferencia de este enlace tiene serias consecuencias para la planta entera. Las propiedades industriales del equipo implican aquí que los datos no solo se pasen a través de un enlace inalámbrico, sino también a través de un segundo enlace que maneja el mismo flujo de datos. Para esto se requiere un Access Point dual.

La confiabilidad de la transmisión reside en el hecho de que una tarjeta opera en la banda de 2.4GHz y la otra en 5GHz. Sin embargo, no es totalmente necesario cambiar a una banda de frecuencia diferente. Aun utilizando el canal 1 y el canal 11 a 2.4GHz, significa que las tramas de datos están alejadas unas de otras que difícilmente una perturbación afecte a los dos canales simultáneamente.

Se debe enfatizar el hecho que esta técnica es totalmente transparente para la aplicación y que los Access Points se encargan de determinar que tarjeta inalámbrica esta activa y cual en modo de respaldo “Hot Standby”. Si ocurre un problema, se pueden lograr tiempos de conmutación de entre 20 ms y 25 ms.

4.3.4.5 INFRAESTRUCTURA INALAMBRICA REDUNDANTE – SPANNING TREE (ST)

Para proveer protección contra la falla de la infraestructura inalámbrica y para mejorar aun más la confiabilidad de la red, se puede utilizar una topología de anillo en vez de estrella. Una estructura así también se puede utilizar para respaldar un enlace cableado, mediante un enlace inalámbrico en áreas riesgosas.

4.3.4.6 FUNCION HOPPING (IHOP)

La función **industrial Hopping (iHOP)**, ofrece una ventaja adicional para crear una red Wireless Local Area Network (WLAN). Hasta ahora, en la banda de frecuencia de 2,4 GHz, sólo se podían crear en paralelo un máximo de 3 celdas de emisión sin que hubiese interferencias, mientras que ahora con ayuda de la función iHop se puede implementar una cuarta aplicación dentro de las 3 celdas de emisión. Este concepto tiene la ventaja de que se puede reaccionar más fácilmente a las interferencias, ya que la selección de 3 canales **WLAN** admite canales de desvío. Si el cliente tiene la necesidad de que su aplicación funcione en cualquier instante independientemente de las influencias externas, la función iHOP puede utilizarse de forma ideal en este caso. Si no se dispone de ancho de banda suficiente para otras aplicaciones en el rango de frecuencia de 2,4 Ghz, la función iHOP tiene la capacidad de saltar al rango de frecuencia de 5 Ghz y mantener la comunicación con estos canales.

Condiciones para utilizar iHOP:

Ventajas:

- Adecuada sobre todo para celdas de emisión móviles (los clientes se asignan de forma fija al AP)

-
- Cuanto más ancho de banda se disponga en el campo de emisión, sumando todos los canales utilizados, se puede obtener un mayor flujo de datos
 - Si se utilizan „canales con restricción“, se puede limitar el número de canales utilizados por el iHOP
 - Disponible tanto en el rango de 2,4 GHz como en el rango de 5 GHz. Además, iHOP puede cambiar entre 2,4 y 5 GHz.

Desventajas:

- iHOP sólo se puede utilizar en el modo WLAN estándar (sin iPCF)
- La utilización del iHOP no es adecuado para el servicio en paralelo con instalaciones que implementen iPCF, ya que se podría perturbar una red WLAN que funcione con iPCF
- iHOP no es adecuado actualmente para la comunicación PN IO. Para realizar la comunicación PN IO, se recomienda la función iPCF.
- iHOP no es adecuado para aplicaciones críticas en el tiempo. En este caso, también se recomienda la utilización del iPCF.
- Si se utiliza el iHOP, no se pueden garantizar los tiempos de Roaming.
- Con cada iHOP AP, se pueden conectar un máximo de 8 clientes iHOP.

4.3.4.7 FUNCION HiPath WIRELESS CONTROLLER

HiPath Wireless Controller, se usa para configurar los dispositivos Access Point inalámbricos que funcionan con interfaces Web. Ofrece una gestión central uniendo, administrando y coordinando todos los puntos de acceso y clientes de modo que el entorno WLAN aparezca como varias subredes IP individuales, administradas centralmente. Además administra las conexiones a fin de que las estaciones se puedan mover por toda la red inalámbrica de forma segura y sin problemas.

HiPath Wireless Controller permite dividir una única infraestructura inalámbrica en redes lógicas (Virtual Network Services, VNS). Esto permite la asignación fiable de diversos servicios, requisitos de seguridad y posibilidades de acceso a los usuarios, permitiendo a distintos grupos de usuarios tales como administradores, técnicos de servicio o invitados a compartir la misma red inalámbrica.

De igual manera, también puede haber otras aplicaciones como ser: voz, Internet o PLCs funcionando dentro de la misma infraestructura, lo que permite un aprovechamiento máximo de la red inalámbrica. Para aplicaciones que requieran un alto nivel de fiabilidad, el HiPath Wireless Controller se puede utilizar con un segundo dispositivo redundante.

Cuando se necesite ampliar la red con un enlace inalámbrico, utilizando HiPath Wireless Controller, se utilizara un par Access Point, que utilizan un sistema de distribución inalámbrico WDS (Wireless Distribution System), donde los dos puntos de acceso transmiten datos con total transparencia tanto desde el HiPath como hacia el, tal como muestra la Figura Nro: 30.

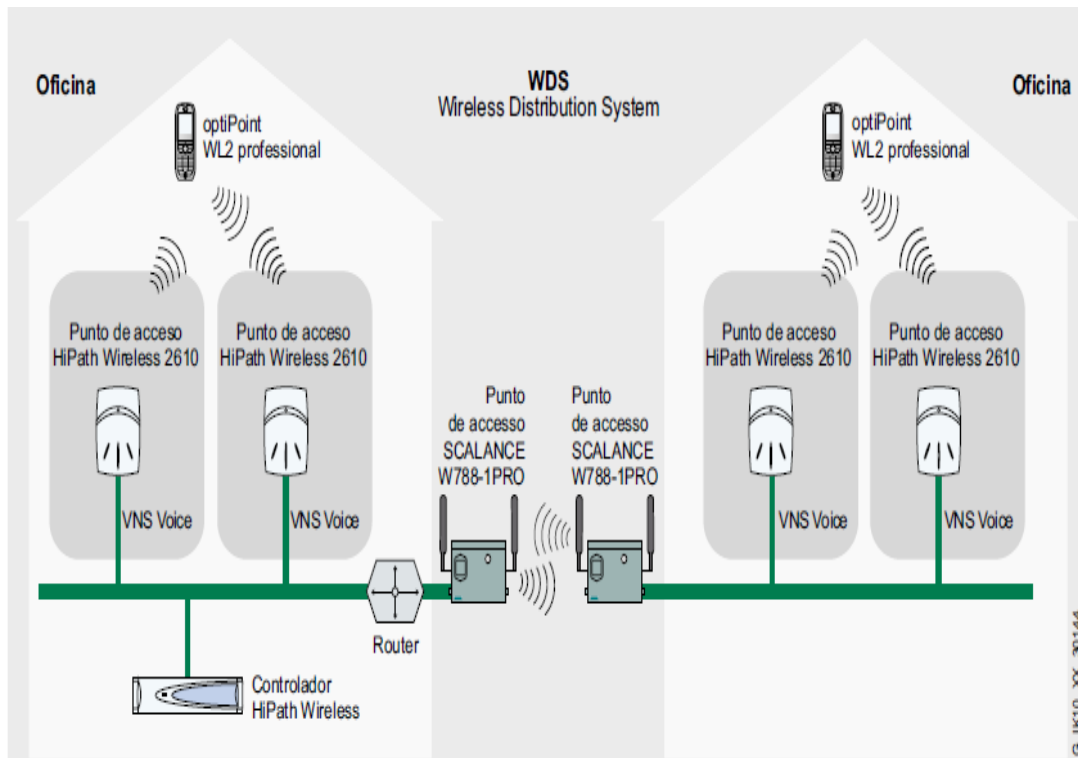


Fig. Nro: 30 Integración de una Red de Oficina Remota en una infraestructura HiPath Wireless Controller ⁽³⁰⁾

4.3.5 SEGURIDAD DE DATOS Y PROTECCIÓN CONTRA ACCESO NO AUTORIZADO

La seguridad de los datos es otra exigencia vital para los usuarios industriales.

En primer lugar está la codificación de los datos transmitidos. Con el proceso WPA (Wireless Fidelity Protected Access – Acceso inalámbrico protegido) se dispone ahora de un estándar para la comunicación inalámbrica móvil segura.

En el modo WPA se modifica en forma automática y periódica el código completo de 128 Bit, de manera que en el flujo de datos no exista ningún tipo de regularidad que ofrezca alguna información relacionada con el código utilizado.

Además de esto, todos los participantes de la red deben identificarse mediante un protocolo de autenticación. En forma alternativa a la seguridad que ofrece WPA, para proteger el tráfico completo de datos útiles entre el aparato final y el Access Point aún puede utilizarse – al igual que con anterioridad – el frecuentemente usado túnel VPN (Virtual Private Network o Red Virtual Privada).

La Figura Nro: 31, muestra la compatibilidad de todos los estándares actuales con **IWLAN**.



Fig. Nro: 31 Estándares de seguridad utilizados en IWLAN ⁽³¹⁾

4.3.6 OTRAS NORMAS IWLAN A UTILIZAR

Aparte de las normas **a**, **b**, **g** y **h**, y debido a su importancia para la aplicación industrial han sido adoptadas las siguientes normas:

- 802.11 e: Seguridad de datos.
- 802.11 i: Priorización de datos.
- 802.11 n: Alta velocidad de transmisión de datos.
- 802.11 s: Malla inalámbrica LAN.

4.3.6.1 NORMA 802.11e

IEEE 802.11 e soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad y Servicio (QoS). El objetivo de este estándar es introducir nuevos mecanismos a nivel de capa MAC, para soportar los servicios que requieran garantías de Calidad de Servicios. Para cumplir con este objetivo introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- EDCA: Enhanced Distributed Channel Access.
- HCCA: Controlled Access.

4.3.6.2 NORMA 802.11i

Este estándar es una enmienda a los mecanismos de seguridad que ofrece 802.11. Las mejoras que propone están referidas al empleo de **TKIP** y **CCMP**, los cuales proporcionan mecanismos más robustos de protección. Se introducen también conceptos de asociación segura a través de mecanismos de “**4-Way Handshake**”, y por

último especifica también el empleo de **802.1x** para autenticación. Como se observa en la Figura Nro: 32, un usuario no autorizado no puede ingresar a la red.

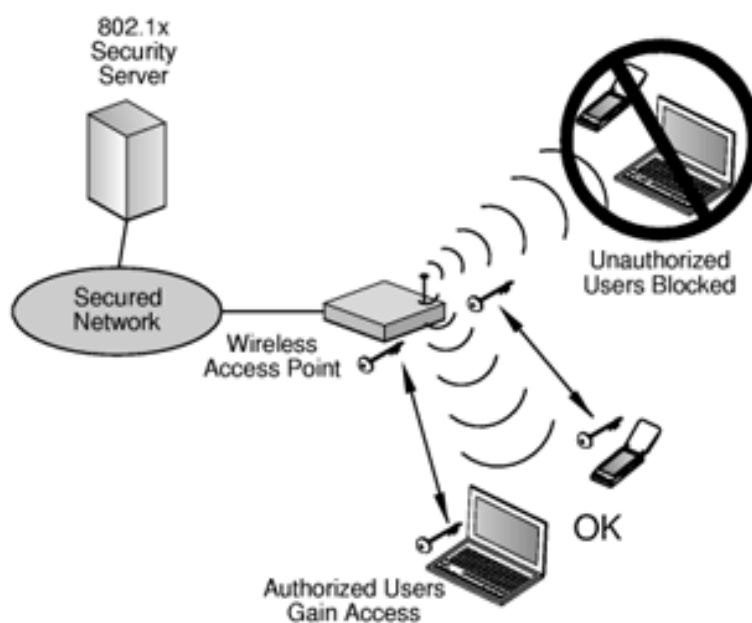


Fig. Nro: 32 Arquitectura 802.11i ⁽³²⁾

4.3.6.3 NORMA 802.11n

La tecnología WI-FI 802.11n es un sistema muy novedoso que se basa en la tecnología MIMO (Múltiple input Múltiple output). Las ondas de RF son "Multi-Señal" y siempre existe una onda primaria y varias secundarias. Hasta ahora, sólo se aprovechaba la onda primaria y las otras eran vistas como "interferencias" o algoritmo MIMO, envía señal a 2 o más antenas y luego las recoge y re-convierte en una. Este estándar a diferencia de las otras versiones, puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a), gracias a ello es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi.

802.11n ofrece grandes ventajas sobre los estándares anteriores, con velocidades hasta cinco veces más rápidas que las LAN's inalámbricas tradicionales (WLAN), un alcance mayor y una fiabilidad mejorada para soportar aplicaciones móviles de altas prestaciones, tales como video HD, imágenes de alta resolución y voz sobre WLAN (VoWLAN).

4.3.6.4 NORMA 802.11s

802.11s define la interoperabilidad de las redes inalámbricas tipo Mesh, que son redes acopladas, o redes de malla inalámbrica de infraestructura, para definir las de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura. Básicamente son redes con topología de infraestructura pero que permiten unir a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del

rango de cobertura de alguna tarjeta de red (TR) que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso (PA).

Permite que las tarjetas de red se comuniquen entre sí, independientemente del punto de acceso. Esto quiere decir que los dispositivos que actúan como tarjeta de red pueden no mandar directamente sus paquetes al punto de acceso sino que pueden pasárselos a otras tarjetas de red para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (Hops en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno. Es resistente a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

4.3.7 APLICACIONES IWLAN.

Las aplicaciones más comunes de estas redes, es donde se requiera movilidad y flexibilidad, esto es el caso de los procesos donde se involucra el movimiento de maquinas, partes o automatismos/robots.

Las siguientes son algunas de las aplicaciones típicas que requieren movilidad y flexibilidad:

- Sistemas de transporte sin conductor.
- Sistemas monorraíl.
- Mesas rotantes.
- Maquinas móviles y rotantes: en reemplazo de cables flexibles, contactos y anillos rozantes.
- Grúas.
- Sistemas de transporte público (metros y tranvías, trenes, autobuses, etc.), uso confiable de los productos en aplicaciones sujetas a requisitos exigentes en cuanto a temperatura y estabilidad mecánica, campo de radiofrecuencia óptimo gracias al control de la potencia de radiación con cable coaxial radiante.
- Equipo de servicio y diagnóstico portátil.
- Equipo de operación y monitoreo portátil.
- Intervinculación rápida de áreas de fabricación y producción, grupos aislados y maquinas durante su puesta en servicio.
- Adquisición de datos en depósitos y logística.
- Enlace inalámbrico de segmentos de comunicación para lograr una puesta en servicio rápido o para ahorrar gastos de interconexión, cuando el tendido de cables supone un gasto considerable (por ejemplo: calles y carreteras, ríos, lagos, líneas de ferrocarril, etc.

También hay muchas aplicaciones en el campo de la automatización en las cuales la comunicación entre estaciones individuales es una ventaja adicional para el usuario.

A continuación se describen algunas de las aplicaciones **IWLAN**.

4.3.7.1 COMUNICACIÓN CON ESTACIONES MÓVILES PARA ADQUIRIR DATOS

El usuario puede adquirir datos de todas las áreas de producción con un equipo móvil como ser notebook o PDAs con navegadores de Internet incorporados, desde un punto central. Los equipos portátiles no se asignan a una maquina o a una función en especial sino a un usuario y de esta manera es posible reducir la cantidad de equipos necesarios para la supervisión de la planta.

Asimismo la conexión online entre el sistema de obtención de datos y la planilla de reporte final permite independizarse de medios escritos como el papel y la lapicera, ahorrando tiempo significativos y eliminando errores, además también permite ahorrar costos, especialmente en el uso de interfaces que permiten traducir datos de un sistema a otro.

4.3.7.2 DIAGNÓSTICO Y SERVICIO MÓVIL

Si ocurre una falla el personal de mantenimiento puede analizarla en el lugar y obtener suficiente información para eliminar el problema rápidamente, relevando los datos desde una PDA o un PAD de Internet portátil, o también desde una notebook con acceso **WLAN**. Al mismo tiempo puede consultar desde el mismo sistema la disponibilidad de repuestos en el depósito y si fuese necesario ordenarlos inmediatamente.

El diagnóstico no sólo se aplica a la detección de fallas, sino también permite al operador informarse sobre el nivel, la velocidad, las horas de operación y otros datos relevantes del sistema productivo automatizado.

La comunicación móvil puede simplificar y acelerar enormemente las fases de puesta en servicio de un equipo o sistema de automatización y a su vez reducir costos en forma significativa. También permite a los encargados de mantenimiento monitorear los ajustes de una maquina desde sus equipos portátiles e intervenir inmediatamente si ocurre algún problema. Para lograr esto no necesitan equipos especiales ya que la tecnología actual de los equipos de computación, vienen con la tecnología inalámbrica incorporada.

4.3.7.3 ADQUISICIÓN DE DATOS EN DEPÓSITOS Y LOGÍSTICA

La tecnología inalámbrica apropiada es la **RFID**, permite el almacenamiento y obtención de datos en forma remota (sin contacto), mediante el uso de dispositivos que permiten el manejo de información de objetos, permitiendo una identificación eficiente de los mismos en forma rápida, definiendo el tipo de información que se desee, dejando los procesos manuales y el tedioso registro directo “uno a uno” como cosa del pasado.

Sin duda la principal ventaja radica en la rápida y automática adquisición de datos, ahorrando tiempo al poder obtener datos del conjunto de materiales en movimiento. La consecuencia directa de esta ventaja es la reducción de costos, por ejemplo, en los inventarios, mejoramiento de la calidad logística o trazabilidad del material.

Esta tecnología también ofrece la posibilidad de generar interacción con el proceso de producción, en forma sincronizada y en tiempo real.

4.3.8 EJEMPLOS DE APLICACIÓN DE UNA RED IWLAN INTEGRADA

4.3.8.1 APLICACIÓN EN UNA PLANTA PROCESADORAS DE HUEVOS

Se describe la utilización de la tecnología inalámbrica (RFID), en la cadena de abastecimiento de una planta productora de huevo líquido pasteurizado, para su utilización en productos lácteos y pastas. La planta en cuestión posee una serie de granjas donde se producen huevos, las que están sujetas a las mismas exigencias logísticas y sanitarias.

El uso de la tecnología inalámbrica RFID comienza en el origen de la producción: los huevos son transportados en carros metálicos, que en su parte superior, llevan un TAG que los identifica en forma única y seriada, registrándose así toda la producción diaria.

Por su parte los camiones de transporte cuentan con una computadora que tiene incorporado Wi-Fi, posicionamiento con GPS y tres antenas RFID ubicadas en el interior del remolque. A este equipamiento, se suma un equipo interno para el registro de la información.

De este modo el camión ya no solo es un medio de transporte, sino que además es un canal de comunicación. A medida que los carros metálicos entran al camión, son leídos por el equipamiento instalado, permitiendo obtener de esta manera diferentes datos, como la cantidad de carros ingresada y si los carros entran o salen.

Una vez que el camión llega a destino, todos los datos que han sido cargados en el origen son descargados, considerando que el vehículo no solo maneja la información de la carga, sino que también posee registros de vital importancia, como ser la temperatura del remolque.

Al aplicar esta tecnología, el beneficio principal fue dar solución a la trazabilidad de los huevos desde las granjas, evitando los errores humanos, actualizando datos automáticamente respecto a las cargas, en estrecha relación con estándares de calidad asociados al transporte de alimentos.

Asimismo al manejar la información sobre el stock que tiene cada granja en tiempo real, se puede planificar la nueva toma de huevos en forma óptima. De igual manera, el saber que se cuenta con un registro claro y seguro del tiempo de transporte y de la fecha de origen del huevo, permite mejorar la calidad del producto final, ya que se puede dar fe de que el producto procesado es fresco.

Los conceptos logísticos utilizados en esta aplicación son similares a los encontrados en otros campos, cambiando solo algunos parámetros centrales como el material, la disposición para el transporte y la cantidad, que son aquellos que definen el comienzo de un proyecto.

4.3.8.2 APLICACIÓN EN PLANTAS DE FABRICACION DE AUTOMÓVILES

La aplicación propuesta, es para la reducción del número de atornilladoras (como se observa en la Figura Nro: 33, es una máquina utilizada para atornillar), en el montaje final del automóvil. Actualmente se usa una atornilladora en cada paso de trabajo y en cada detección de código de barras. Puesto que la solución cableada con anillos deslizantes requiere mucho mantenimiento, se propone una comunicación inalámbrica fiable para aumentar la eficiencia, reducir los tiempos de preparación y que requieran poco mantenimiento.



Fig. Nro: 33 Sistemas de atornilladoras industrial ⁽³³⁾

La solución propuesta es:

- Como se observa en la Figura Nro: 34, para la transferencia de datos inalámbrica se utilizara el cable coaxil radiante **IWLAN (RCoax)**, a lo largo de la barra de codificación. Con esto se obtiene un campo de radiofrecuencia de forma, cónica y fiable y fácil de trasladar.
- Como estación de alimentación del cable coaxil radiante se utiliza **Access Point** con tecnología RR, según norma IEEE 802.11b/g (2,4 GHz) con velocidades de transferencia hasta 54 Mbps.
- Como **estación móvil** se montan módulos inalámbricos con tecnología RR. De este modo se puede utilizar la misma unidad móvil para todas las aplicaciones, y por lo tanto una atornilladora móvil para varios pasos de trabajo, aparte este dispositivo permite conectar hasta 8 terminales.

Con esta propuesta se consigue, reducir costos de inversión, gastos de mantenimiento, disminución de los tiempos improductivos en caso de averías, reducción de las actividades de los operarios (por ejemplo: exploración de códigos), posibilidad de integrar nuevas aplicaciones para mejorar la calidad y por medio del enlace inalámbrico la posibilidad de cargar todos los datos de una atornilladora.

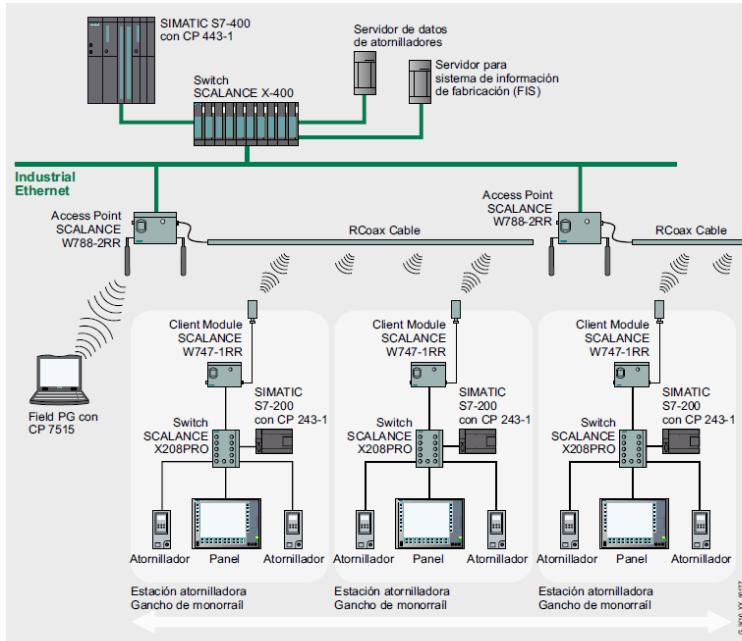


Fig. Nro: 34 Solución para control de atornilladoras con cable coaxil radiante ⁽³⁴⁾

Dispositivos utilizados en la aplicación.



Fig. Nro: 35 Cable RCoax ⁽³⁵⁾



Fig. Nro: 36 Estación móvil ⁽³⁶⁾



Fig. Nro: 37 Punto de Acceso (Access Point) ⁽³⁷⁾

4.3.9 ACTUALIDADY FUTURO DE LAS REDES INALÁMBRICAS

Son muchas las expectativas creadas en torno a Wi-Fi, apoyadas en tres variables: la reducción de costos, la movilidad y el apoyo de los fabricantes de equipamiento informático de incrementar esta tecnología, tanto en el ámbito del hogar, la industria manufacturera, y el negocio de las telecomunicaciones. El futuro desarrollo de Wi-Fi deberá contener las características básicas requeridas: movilidad, facilidad de conexión para el usuario, dispositivos económicos y estándares interoperables.

En el ámbito **manufacturero**, el procesamiento de datos, el tele diagnóstico y el tele mantenimiento de las plantas de producción industrial, son un componente imprescindible de la tecnología de automatización moderna. Son más eficientes y económicos que tener a un empleado del servicio técnico in situ.

El tele diagnóstico y el tele mantenimiento permiten recolectar datos, detectar y subsanar las fallas más rápidamente, reducir los tiempos de parada de las maquinas y aumentar su disponibilidad. En el caso de las instalaciones de difícil acceso o muy distribuidas, se necesitan disponer de conexiones de datos fiables, siempre disponibles, seguros y económicos. Para esta tarea se usan cada vez más las tecnologías inalámbricas modernas, combinadas con Internet. También es necesario adoptar las correspondientes medidas de seguridad, para proteger eficazmente la transferencia de datos contra espionaje y manipulación. Los fabricantes de dispositivos IWLAN, para la industria manufacturera tendrán que ir pensando en la utilización de las nuevas propuestas de IEEE, con respecto a los nuevos estándares 802.11x, que permitirán aumentar la velocidad de transmisión e incrementar la seguridad de los datos transmitidos.

Especificación	Tipo	Descripción	Fecha aproximada
802.11 ac	Velocidad	Busca incrementar sobre 802.11n en factor 2:1. Espectro 5 GHz.	2012
802.11 ad	Velocidad	Busca incrementar sobre 802.11n en factor 10:1. Espectro 60 GHz.	2012
802.11s	Mesh networking	Permitiría a los dispositivos conectarse entre si como nodos mesh.	Septiembre 2010
802.11u	Seguridad	Conocido como "internetworking with external networks". Basaría su seguridad en la red externa que utiliza.	Marzo 2010
802.11z	Networking Ad-hoc	Llamado "direct link setup" permitirá a dos laptops con Wi-Fi conectarse de forma segura en modo P2P usando credenciales del AP de la red más grande.	Enero 2010

Tabla Nro: 5 Estándares futuros IEEE 802.11

Nuevos estándares están apareciendo, WiMax, ZigBee, Z-Wave, GPRS, telefonía celular, etc., que sirven de apoyo a las redes Wi-Fi locales, que la industria manufacturera moderna lo va adoptando, para obtener comunicaciones seguras, un control óptimo de la producción, diagnóstico efectivo de fallas y mantenimiento adecuado de los procesos industriales.

4.4 CONCLUSIONES

La finalidad del trabajo integrador, es demostrar como las comunicaciones industriales se han convertido en un medio fundamental para mejorar el rendimiento y la eficacia de las funciones operacionales en una empresa industrial moderna. La obtención de datos en el momento y punto de origen, al integrarse al ciclo de procesamiento y control de las operaciones y al actualizar las bases de datos en forma automática, permite la toma de decisiones operacionales, tácticas y estratégicas más eficaces cualesquiera que sea la naturaleza de la empresa.

Estas estrategias básicas de las comunicaciones en los procesos industriales tienen como objetivo:

- Aumentar la eficacia de las operaciones y procesos industriales a través de la aplicación de las modernas tecnologías de la electrónica, la informática y las modernas redes de comunicaciones ethernet, cableadas e inalámbricas.
- Incrementar la productividad de los recursos humanos mediante, la automatización de las actividades manuales y repetitivas, la dotación de procedimientos, equipos y sistemas que permitan disponer de la información en forma oportuna y confiable en el sitio y momento deseado, como así también disminuir costos y aumentar la disponibilidad de la planta física, mediante mantenimiento centrado en la confiabilidad.

Durante el desarrollo del trabajo se puede observar como las comunicaciones desempeñan una función de primordial importancia en la implantación de los modernos sistemas de Automatización Industrial. Esta función es vital para aquellas empresas cuyas operaciones se encuentran dispersas geográficamente, como es el caso de los sistemas de distribución de energía eléctrica, la supervisión y control de instalaciones petroleras, patios de tanques, poliductos, refinerías, etc.

Para poder cumplir con los siguientes objetivos:

- Recolección, procesamiento y transmisión de datos.
- Supervisión de alarmas, de procesos continuos, verificación de instalaciones y seguimiento de las condiciones de operación de estaciones remotas.

Se debe contar con una estructura jerárquica de comunicación bidireccional bien definida y bajo premisas de nacionalización, conectividad, calidad y confiabilidad.

Como fue desarrollado, las grandes empresas industriales utilizan un modelo de sistema integrado con computadora (pirámide CIM), que la podemos reducir en tres niveles primordiales, que engloban a los ya expresados.

NIVEL OPERACIONAL:

Donde se llevan a cabo todas las actividades y procesos básicos que constituyen el objetivo de la empresa, donde la velocidad de transferencia de información es variable, pudiendo extenderse desde 300 bps a 20 Mbps.

NIVEL TÁCTICO:

Donde se llevan a cabo actividades de planificación de operaciones y mantenimiento, labores de ingeniería, control de inventarios, etc. En este nivel la velocidad de transferencia de la información es alta, sobre los 20 Mbps.

NIVEL ESTRATÉGICO:

Donde se manejan todas las directrices de producción y mercadeo, las políticas de la empresa, la gestión, la administración, etc. En este nivel la velocidad de transferencia de información es generalmente muy alta del orden de los 100 Mbps o más.

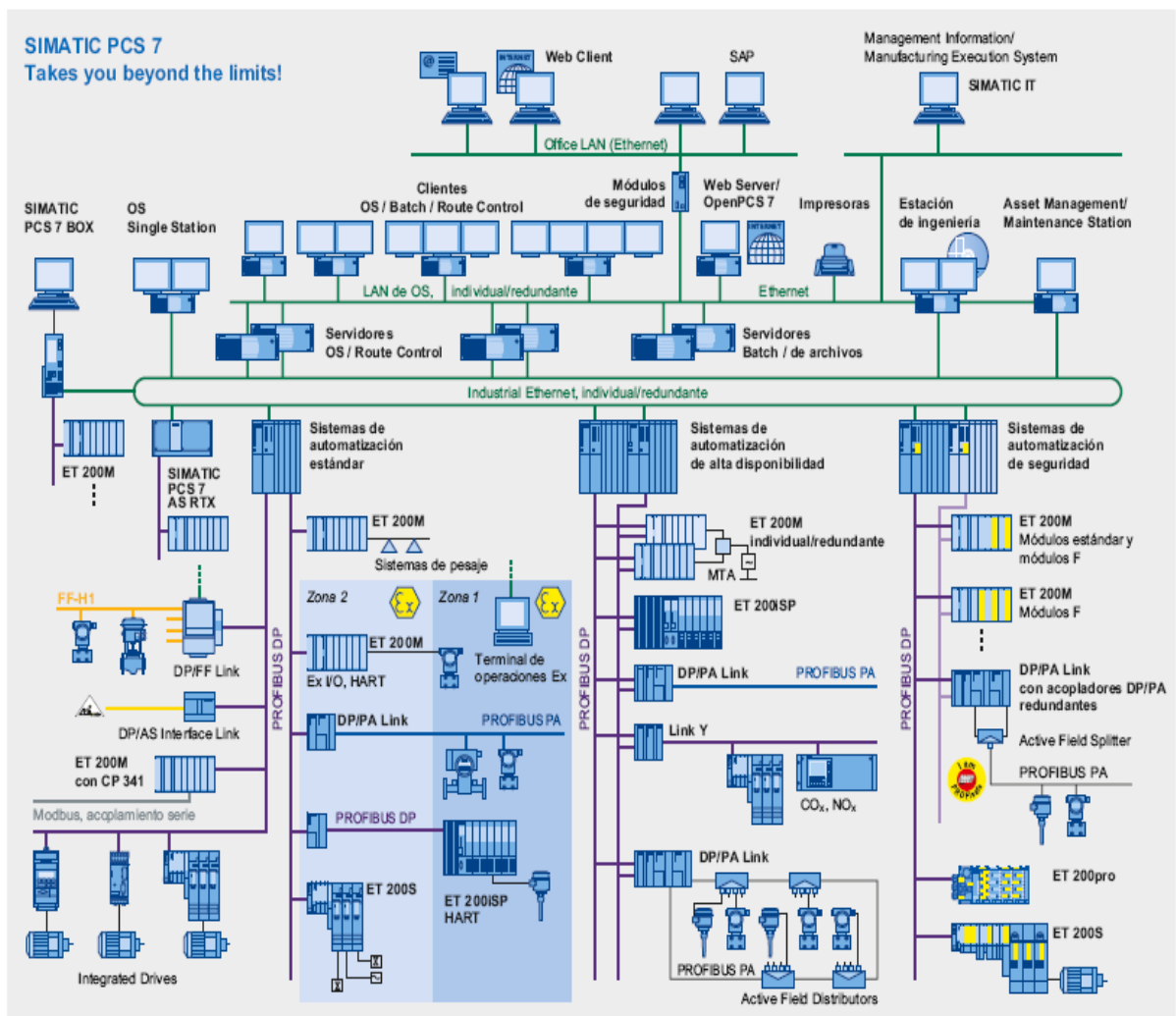


Fig. Nro: 38 Red de comunicación Industrial Siemens (38)

En la Figura Nro: 38, se puede observar una red de comunicación industrial de Siemens, donde se integran redes de buses y Ethernet industrial, utilizada para procesar datos, desde el nivel de proceso, (sensores y actuadores), pasando por las diferentes capas del modelo CIM, hasta llegar al nivel de gestión, donde se pueden observar, los diferentes servicios de esta capa: servidores Web, Sap, etc.

Para poder lograr la integración de la información en los tres niveles, hay que crear un sistema distribuido con una alta conectividad e interoperabilidad. Como se explico en el trabajo, se requiere, una infraestructura sólida de comunicaciones que comprenda:

- Redes orientadas al control local.
- Redes orientadas al control supervisor.
- Redes orientadas al soporte de la planificación, ingeniería, gerencia y administración.
- Interconexión con redes Externas de la Empresa.

Estas redes permitirán, mantener una visión integrada de los sistemas, tanto desde el punto de vista del modelo del flujo de datos como desde el punto de vista de la integración de los procesos.

La gran red corporativa, simplemente es una red MAN o WAN de media o alta velocidad, con diferentes tipos de servicios. La red de Procesos generalmente es una Red de Área Local (LAN), que puede ser cableada o inalámbrica (WLAN o IWLAN) y dentro del área de Operaciones y Procesos Físicos se encuentran las Redes de campo (buses).

En el nivel de campo (niveles inferiores), los buses representan el eslabón final entre los dispositivos de campo (sensores y actuadores), y los esquemas de control y de gestión de un sistema de fabricación integrado.

Dentro de los buses utilizados en las comunicaciones industriales, se pueden dividir en grupos, en función de los diversos campos de aplicación y las topologías utilizadas: buses de alta velocidad y baja funcionalidad (ASI, CAN, etc.), buses de alta velocidad y funcionalidad media (DeviceNet, LONWorks, DIN, etc.), buses de altas prestaciones (Profibus, FIP, etc.), y buses para áreas de seguridad intrínseca (Hart, Profibus PA, etc.).

Pero los buses tienen sus limitaciones, cuando la información, debe llegar para su procesamiento y supervisión en las capas superiores del modelo CIM, por lo tanto la utilización de Ethernet Industrial, similar a Ethernet convencional (de oficina), pero rediseñada para ser aplicada en la industria, le permite a los ingenieros de proceso y producto tomar datos **en tiempo real** y realizar tareas de logística, diagnóstico y monitorización remota de los procesos de fabricación.

Un punto importante a tener en cuenta, es contar con un mecanismo para evitar conflictos en el envío de paquetes de datos y proteger su integridad, para eso se utilizan varios protocolos de **acceso al medio** que evitan la pérdida de los mismos.

En la actualidad hay diferentes protocolos, aplicados a los procesos industriales, y su elección se encuentra ligado al estándar adoptado para las capas de los dispositivos de control, que a continuación se detallan: Ethercat, Profinet, Ethernet Power Link, Ethernet/IP, Modbus TCP/IP, Sercos III, y CC-LinK IE. Estos protocolos obtienen datos en tiempo real y se diferencian entre ellos, en los medios (Fibra Óptica, UTP, cable bifilar, etc.) utilizados para conectarse al sistema, rendimiento, compatibilidad con los buses de campo, forma de procesar los datos, la transferencia de información (datos de proceso, alarmas, telegramas, etc.) entre los maestros y los esclavos, topologías soportadas, escalabilidad, etc.

Ethernet Industrial es un estándar basado en una red optimizada para satisfacer las necesidades de las comunicaciones en la industria moderna. Con los nuevos protocolos, se esta usando ampliamente en el nivel de campo y en aplicaciones de tiempo criticas, su integración en la conmutación en los dispositivos de campo, hace que este sustituyendo a los buses industriales.

En la actualidad las redes cableadas se han transformado en un obstáculo para ciertas aplicaciones, por lo tanto se esta usando: IWLAN (redes ethernet inalámbricas), que ofrecen ventajas como la movilidad, flexibilidad , la reducción de cableado y permiten que los datos de producción y servicios estén disponible prácticamente en toda la fabrica para poder ser accedidos cuando se desee por los ingenieros, para poder observar desde sus puestos de trabajo, e influenciar con sus acciones el proceso de toda la planta.

Para poder utilizar el estándar IEEE 802.x en los procesos de la industria, de deben adicionar prestaciones especiales “Industriales”, al estándar WLAN, manteniendo la compatibilidad, de manera que los equipos comerciales se puedan integrar a la red industrial.

En función de las diversas aplicaciones en el sistema y la distancia a cubrir (Redes PAN, LAN o WAN), hay varias tecnologías inalámbricas disponibles, estas son: RFID, Bluetooth, ZigBee, WiMAX, GSM, EDGE, etc.

Estas tecnologías aplicadas a diferentes tipos de redes y topologías, permiten movilidad del sistema, velocidad en la comunicación, flexibilidad en la instalación, escalabilidad, etc. En función de lo expuesto tiene múltiples aplicaciones como ser:

- Sistemas de transporte sin conductor.
- Grúas.
- Sistemas monorriel.
- Monitoreo y diagnostico portátil.
- Etc.

En la Figura Nro: 39, se puede observar ,una integración inalámbrica (IWLAN), entre redes de oficina y redes industriales de proceso y control, separadas por router industriales.

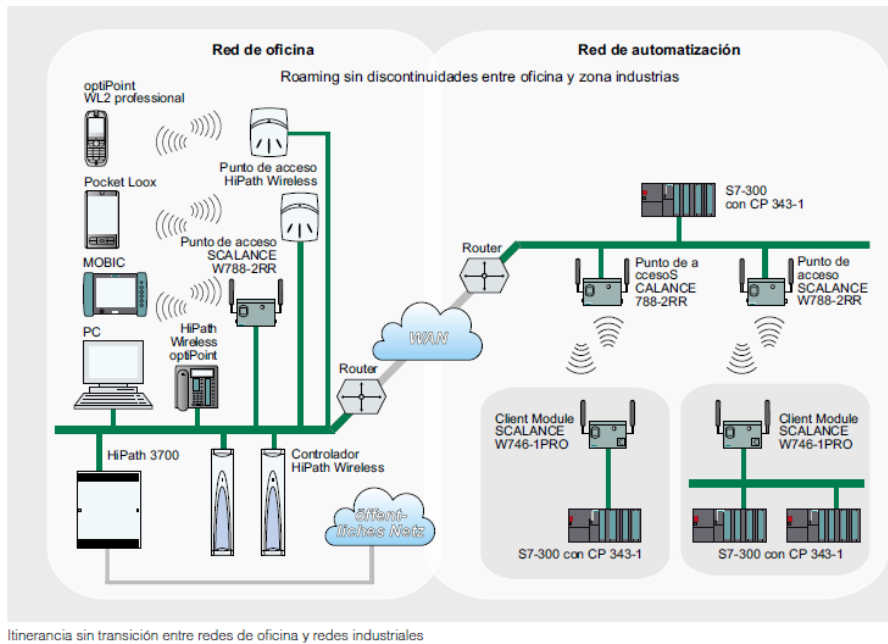


Fig. Nro. 39 Integración entre redes de oficina y redes industriales ⁽³⁹⁾

El trabajo trato de exponer, como fue evolucionando las comunicaciones y el control de procesos en la industria, hasta su total integración, en todos los niveles (Pirámide CIM), combinando varias tecnologías (buses y redes), desde el nivel de proceso, utilizando los buses industriales, redes Ethernet cableadas (WLAN) o inalámbricas (IWLAN), en los niveles de campo, célula, área y fabrica, hasta el nivel de gestión – red de oficina, y su enlace con el exterior utilizando las nuevas tecnologías como ser: WI-Max, GPRS, telefonía móvil, etc.

Este es el futuro que ya esta en marcha, con lo cual se podrán obtener mejores productos, con procesos controlados, seguros y eficientes.

REFERENCIAS BIBLIOGRAFICAS:

- **Andrew S. Tanenbaum.** “Redes de Computadoras”. Editorial Pearson. (4ta edición -2003).
- **Neil Reid y Ron Seide.**”802.11 (Wi-Fi). Manual de Redes Inalámbricas”. Editorial MC Graw Hill. (2005).
- **William Stallings.** “Comunicaciones y Redes de Computadoras”. Editorial Pearson. (7ma edición – 2007).
- **Huidobro Mayo José Manuel.** Comunicaciones móviles. Editorial Paraninfo. (2002).
- **Ing. Diego M. Romero.** Aadeca. Seminario Introducción a Ethernet Industrial. (2007).
- **Ing. Mariano López Figuerola.** Trabajo Integrador: “Tecnologías de Telecomunicaciones aplicadas a transmisión de Datos de Procesos Industriales. (2006).
- **Siemens.** Simatic Net. Basics of Industrial Wireless LAN. Manual C79000-G8976-C168-02. Revision 05/2004.

- **Siemens.** Comunicación Industrial. Automation and drives. Referencia 6BZ 5530-1AED4-OBAS (2005).
- **Siemens.** Simatic Net White Paper V1.3. Industrial Wireless LAN. I-Features, Applications, Examples. (2004).
- **Siemens.** Simatic Net White Paper V 1.0. Industrial Wireless LAN – Industrial Features and Current Standards, (2006).
- **Grupo de comunicaciones móviles y Banda amplia.** Protocolo CSMA/CA. (2008).
- **Siemens.** Seminario de actualización docente sobre redes IWLAN y sistemas de automatización industriales. (Julio 2009).
- **[http:// www.zigbee.org/](http://www.zigbee.org/).** Apuntes tecnología zigbee. (2008)
- **Empresa Silica An Avent División.** Publicación protocolo 802.15.4. (2008)
- **www.oviedo.edu.es.** Protocolo 802.15.1. (2008).
- **www.observatorio.cnice.mec.es.** Protocolo Wi-Max. (2008).
- **www.proser.com.ar.** Red GPRS. (2008).
- **www.electroindustria.** Revista Electroindustria. Artículo sobre Rapid Roaming en la industria.
- **www.airtightnetworks.com/..802.11i.html.** Arquitectura 802.11i.
- **www.fein.de/feindownload/es/FEIN.ACCUTEK.es.pdf.** Artículo sobre atornilladoras automáticas.
- **<http://ethernetindustrial-networking.com>.** Industrial Wireless Book. Artículos sobre IWLAN. (2009).
- **www.cnc.gov.ar/pdf/ns_wi-fi.pdf.** Artículos del Gobierno Nacional sobre implementación Wi-Fi. (2008).

REFERENCIAS DE FIGURAS:

- (1). www.siemens.com.ar . Siemens S.A. Wireless Fidelity. Tecnología de radio disponible y estándar. Pagina 4. (2008).
- (2) y (3). [http:// www.zigbee.org/](http://www.zigbee.org/). Descripción del estándar de comunicaciones de área personal IEEE 802.15.4. Capítulo 2, Pagina 16. (2008).
- (4). Empresa Silica An Avent División. Estándar 802.15.4. PAGINA 3. (2008).
- (5), (6) y (7). Ing. Mariano López Figuerola. Trabajo integrador. “Tecnología de Telecomunicaciones aplicadas a transmisión de datos de procesos industriales”. Paginas: 53 y 54. ITBA (2006).
- (8). www.oviedo.edu.es. Universidad de Oviedo (España). Tema 9, Redes inalámbricas en la industria. Pagina 13. (2008).
- (9). Siemens S.A. Wireless Fidelity. Aplicaciones IWLAN. Pagina 30. (2008).
- (10) y (11). www.oviedo.edu.es. Universidad de Oviedo (España). Tema 4, Redes locales. Pagina 29. (2008).
- (12). <http://standards.ieee.026/db>. Estándar IEEE 802.11 Wireless Lan. Francisco López Ortiz. Pagina 13. (2008).
- (13) y 14. Siemens. Simatic Net. Basic of Industrial Wireless Lan. Capítulo 2, Paginas 24 y 25.
- (15), (17), (18), y (19). Manual Siemens A & D SC .Sensores y comunicaciones. Siemens AG 2007. Paginas: 3, 5, 9 y 10.
- (16). www.observatorio.cnice.mec.es. Que es Wi-Max. (2008).
- (20). www.proser.com.ar. Conectividad industrial GPRS. Monitoreo y telesupervision. (2008).

-
- (21). www.siemens.com.ar. Newsletter Nro: 14. Soluciones para aplicaciones de automatización utilizando redes inalámbricas industriales (1ra parte). (2007).
- (22), (23) y (24). Siemens S.A. Wireless Fidelity. Aplicaciones IWLAN. Paginas: 31, 32 y 72. (2008).
- (25). www.electroindustria. Revista Electroindustria. Articulo de Rapid Roaming en la industria. (2009).
- (26), (27), (29) y (30). **Siemens**. Simatic Net. Industrial Ethernet. Industrial Wireless lan. I-Features, Applications y Examples. Paginas: 15, 16 y 17. (2008).
- (28). Siemens AG 2007. Industrial Wireless Communication. Pagina 12.
- (31). Siemens S.A. Wireless Fidelity. Aplicaciones IWLAN. Paginas 77. (2008).
- (32). www.airtightnetworks.com/..802.11i.html. Arquitectura 802.11i.
- (33). www.fein.de/feindowload/es/FEIN.ACCUTEK.es.pdf. Sistemas de atornilladoras FEIN ACCUTEK.
- (34). Siemens S.A. Wireless Fidelity. Aplicaciones IWLAN. Paginas 70. (2008).
- (35), (36) y (37). www.siemens.de/simatic-net. Comunicación Industrial- Automation and drives. Ref. E86060-K6710-A101-B5-7800 (2008).
- (38). Industrial Communication Automatización y comunicación a escala corporativa. Publicación Siemens. Abril 2008. Pág. 2 y 3.
39. www.siemens.de/simatic-net. Simatic Net. Comunicación Industrial Móvil. Productos fiables, robustos y seguros. Ref.6ZBB5530-1AM04-0BA2. (2006).

REFERENCIA DE TABLAS

Tabla Nro: 1. Características De las redes ZigBee. IEEE 802.15.4. Empresa Silica An Avent División. (2008).

Tabla Nro: 2 y 3. www.wikipedia.com.

Tabla Nro: 4. Siemens. Introducción a IWLAN, Protocolos. Manual C79000-G8976-C168-02.

Tabla Nro 5. Revista NEX IT Nro: 52. Articulo de Redes Wi-Fi, presente y futuro. (Julio 2009).

GLOSARIO

- **2G.** Segunda generación de telefonía móvil. La telefonía móvil 2G no es un estándar o un protocolo sino que es una forma de marcar el cambio de protocolos de telefonía móvil analógica a digital.
- **3G.** Telefonía móvil de tercera generación. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de email, y mensajería instantánea).
- **ACCESS POINT.** Punto de acceso inalámbrico, usado en las redes de infraestructura.
- **Ad Hoc Network.** Una red ad hoc es una red inalámbrica descentralizada. La red es ad hoc porque cada nodo está preparado para reenviar datos a los demás y la decisión sobre qué nodos reenvían los datos se toma de forma dinámica en función de la conectividad de la red. Esto contrasta con las redes tradicionales en las que los router llevan a cabo esa función. También difiere de las redes inalámbricas convencionales en las que un nodo especial, llamado punto de acceso, gestiona las comunicaciones con el resto de nodos.
- **AES.** Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Se espera que sea usado en el mundo entero y analizado exhaustivamente, como fue el caso de su predecesor, el Data Encryption Standard (DES).
- **ACK.** (Acknowledge, acuse de recibo), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente". Hay tipos más complejos de ACK cuyo significado podría traducirse como "reenvíame la trama 2" o "he recibido tu último mensaje, pero no puedo recibir más hasta que termine de procesar los anteriores".
- **AS-i.** El AS-Interface, o interfaz actuador/sensor, denominado aquí abreviadamente AS-i, es un sistema de conexión para el nivel de procesos más bajo en instalaciones de automatización.
- **B2B.** Es la abreviatura comercial de la expresión anglosajona business to business: (comunicaciones de comercio electrónico) de empresa a empresa, por oposición a las relaciones de comercio entre empresas y consumidores (B2C), o las expresiones menos usadas empresas y gobierno (B2G) o empresas y empleados (B2E).
- **B2C.** Es la abreviatura de la expresión Business-to-Consumer (del negocio al consumidor).
- **BACKOFF (ALGORITMO).** Algoritmo utilizado en el Protocolo CSMA/CA.
- **BLUETOOTH.** Especificación industrial para redes inalámbricas de Área Personal (WPANs), que posibilita la transmisión de datos y voz entre diferentes dispositivos mediante un enlace de radiofrecuencia segura y libre (2,4 GHz).
- **BPDU.** Bridge Protocol Data Units (BPDUs). Son frames que contienen información del protocolo Spanning tree (STP). Los switches mandan BPDUs usando una única dirección MAC de su puerto como Mac de origen y una dirección de multicast como MAC de destino (01:80:C2:00:00:00).
- **BROADCAST.** Transmisión de un paquete que será recibido por todos los dispositivos en una red.

-
- **BSS.** Conjunto de servicio básico (BSS). Grupo de estaciones que se intercomunican entre ellas. Se define dos tipos: Independientes: cuando las estaciones, se intercomunican directamente. Infraestructura: cuando se comunican todas a través de un punto de acceso.
 - **CAD.** El diseño asistido por computador (o computadora u ordenador), abreviado como DAO (Diseño Asistido por Ordenador) pero más conocido por sus siglas inglesas CAD (Computer Aided Design), es el uso de un amplio rango de herramientas computacionales que asisten a ingenieros, arquitectos y a otros profesionales del diseño en sus respectivas actividades. También se llega a encontrar con las siglas CADD, dibujo y diseño asistido por computadora (Computer Aided Drafting and Design). El CAD es también utilizado en el marco de procesos de administración del ciclo de vida de productos (Product Lifecycle Management).
 - **CAE.** Ingeniería asistida por computadora o por ordenador (CAE, del inglés Computer Aided Engineering) es el conjunto de programas informáticos que permiten analizar y simular los diseños de ingeniería realizados con el ordenador, o creados de otro modo e introducidos en el ordenador, para valorar sus características, propiedades, viabilidad y rentabilidad. Su finalidad es optimizar su desarrollo y consecuentes costos de fabricación y reducir al máximo las pruebas para la obtención del producto deseado.
 - **CAM.** La fabricación asistida por computadora (en Hispanoamérica) o fabricación asistida por ordenador (en España), también conocida por las siglas en inglés CAM (Computer Aided Manufacturing), implica el uso de computadores y tecnología de cómputo para ayudar en todas las fases de la manufactura de un producto, incluyendo la planificación del proceso y la producción, mecanizado, calendarización, administración y control de calidad, con una intervención del operario mínima.
 - **CAN.** El protocolo CAN es un protocolo de comunicación serial que describe los servicios de la capa 2 del modelo OSI/ISO. En esta capa, son definidos los diferentes tipos de telegramas (frames), a la forma de detección de errores, validación y arbitraje de mensaje.
 - **CC-LINK IE.** (Protocolo de Control y Comunicación- Ethernet Industrial). Es la primera red Ethernet Industrial de 1 Gbit completamente integrada para la automatización industrial.
 - **CCMP.** Se basa en el modo de MCP de la AES algoritmo de cifrado. CCMP utiliza claves de 128 bits, con una de 48 bits del vector de inicialización (IV) para la detección de reproducción.
 - **CDMA.** La multiplexación por división de código, acceso múltiple por división de código o CDMA (del inglés Code División Multiple Access) es un término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro expandido.
 - **CIM.** John W. Bernard lo define como "la integración de las computadoras digitales en todos los aspectos del proceso de manufactura." Otra definición afirma que se trata de un sistema complejo, de múltiples capas diseñado con el propósito de minimizar los gastos y crear riqueza en todos los aspectos. También se menciona que tiene que ver con proporcionar asistencia computarizada, automatizar, controlar y elevar el nivel de integración en todos los niveles de la manufactura.
 - **CIP.** (Control e Information Protocol, Protocolo de control de información).
 - **CN.** (Control- Node, Nodo de control).

-
- **CRC.** La comprobación de redundancia cíclica (CRC) es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento. Las CRCs son populares porque su implementación en hardware binario es simple, son fáciles de analizar matemáticamente y son particularmente efectivas para detectar errores ocasionados por ruido en los canales de transmisión.
 - **CSMA/CA.** En redes informáticas, Carrier Sense, Múltiple Access, Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones) es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.
 - **CSMA/CD.** (Carrier Sense Multiple Access with Collision Detection, acceso múltiple con detección de portadora y detección de colisiones). Técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación que desee transmitir, comprueba el medio y solo transmite si esta desocupado.
 - **CSMA/DCR.** (Deterministic Collision Resolution).
 - **CSMA/NBA.** (Acceso Múltiple por detección de portadora/Arbitraje de BIT no destructivo).
 - **CTS.** Clear to Send. permiso de ser emitido (en comunicación de datos), señal que permite la difusión al MODEM.
 - **DEVICENET.** Bus de campo utilizado para el control en tiempo real de dispositivos en los primeros niveles de automatización (nivel de proceso).
 - **DFS.** (Dynamic Frequency Selection). Funcionalidad requerida por las WLAN que operan en la banda de 5 GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.
 - **DHCP.** (Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.
 - **DLLM.** (Direct Data Link Mapped).
 - **DMA.** El acceso directo a memoria (Direct Memory Access) permite a cierto tipo de componentes de ordenador acceder a la memoria del sistema para leer o escribir independientemente de la CPU principal. Muchos sistemas hardware utilizan DMA, incluyendo controladores de unidades de disco, tarjetas gráficas y

-
- tarjetas de sonido. DMA es una característica esencial en todos los ordenadores modernos, ya que permite a dispositivos de diferentes velocidades comunicarse sin someter a la CPU a una carga masiva de interrupciones.
- **DSSS.** Espectro extendido de secuencia directa. Técnica de propagación en la que distintas señales de datos, voz y video, o ambas, se transmiten a través de un conjunto específico de frecuencias de manera secuencial.
 - **E-BUSINESS.** El comercio electrónico, también conocido como e-commerce, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como el Internet y otras redes de ordenadores. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo con el advenimiento de la Internet y la World Wide Web a mediados de los años 90 comenzó a referirse principalmente a la venta de bienes y servicios a través de la Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.
 - **EDGE.** (Enhanced Data rates for GSM of Evolution, tasas de datos mejoradas para la evolución de GSM). Conocida como EGPRS (Enhanced GPRS). Es una tecnología de la telefonía celular móvil, que actúa de puente entre las redes 2G y 3G.
 - **EPL.** Ethernet POWERLINK (conocido también con el acrónimo EPL) es un protocolo de comunicación en tiempo real basado en hardware estándar Ethernet.
 - **ERP.** Los sistemas de planificación de recursos empresariales, o ERP (Enterprise resource planning) son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.
 - **ESTANDAR IEC 870-5-1.** Estandar de seguridad en redes industriales.
 - **ETHERCAT.** Ethernet para el control de tecnología de Automatización. Se trata de un código abierto, de alto rendimiento que utiliza protocolos Ethernet en un entorno industrial.
 - **ETHERNET POWER LINK.** Es un protocolo determinista de tiempo real basado en Ethernet.
 - **ETHERNET/IP.** Es una ampliación industrial de Ethernet TCP/IP, puesto que los mensajes de CIP de la capa de aplicación se empaquetan, mediante encapsulación en las tramas TCP/IP como datos de usuario.
 - **FDL.** (Fieldbus Data Link) .Protocolo utilizado en la capa de enlace del protocolo Profibus.
 - **FHSS.** Espectro extendido de salto en frecuencia. Técnica de transmisión de datos, voz y video que se transmiten a través de un conjunto de frecuencias en un orden pseudoaleatorio, en vez de secuencial.
 - **FIELDBUS FOUNDATION.** Es una asociación de fabricantes que administran, investigan y potencian el uso de este protocolo.
 - **FMMU.** (Campo unidad de gestión de memoria).
 - **FTP.** Protocolo de transferencia de archivos. Se utiliza para transferir archivos entre nodos de una red.
 - **GATEWAY.** Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la

-
- información del protocolo utilizado en una red al protocolo usado en la red de destino.
- **GPRS.** General Packet Radio Service (GPRS) o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes). Existe un servicio similar para los teléfonos móviles que del sistema IS-136. Permite velocidades de transferencia de 56 a 114 kbps.
 - **GPS.** El Global Positioning System (GPS) o Sistema de Posicionamiento Global (más conocido con las siglas GPS, aunque su nombre correcto es NAVSTAR-GPS) es un Sistema Global de Navegación por Satélite (GNSS) que permite determinar en todo el mundo la posición de un objeto, una persona, un vehículo o una nave, con una precisión de centímetros, usando GPS diferencial, aunque lo habitual son unos pocos metros.
 - **GSM.** (Groupe Special Mobile). Sistema global para las comunicaciones móviles, definido para la comunicación mediante teléfonos móviles que incorporan tecnología digital.
 - **GSM-R.** (GSM Railway') es un sistema de comunicaciones inalámbricas desarrollado específicamente para comunicación y aplicaciones ferroviarias. Se garantiza su correcto funcionamiento hasta velocidades de 500 Km/h. Sirve a modo de baliza móvil, enviando continuamente la posición del tren a los centros de tráfico centralizado (CTC). Esta tecnología se usa principalmente en el sistema de señalización ERTMS-ETCS. Gracias a esta tecnología, en el último de sus niveles de implantación sería posible eliminar todo tipo de señales y balizas ya que el sistema enviaría constantemente información al tren.
 - **HART.** El protocolo HART (Highway Addressable Remote Transducer) es uno de los estándares líderes en la comunicación con instrumentación inteligente de campo, y continúa aumentando su popularidad y reconocimiento en la industria como un modelo global para este tipo de tareas, existiendo en la actualidad innumerables instalaciones de HART en el mundo.
 - **HCF.** (Hybrid Coordination Function). Permiten sondear las estaciones durante un periodo libre de contenciones. El sondeo garantiza a una estación un tiempo de inicio específico y una duración máxima de transmisión.
 - **HDLC.** (High-level Data Control, control del enlace de datos de alto nivel. Protocolo de enlace de datos (capa 2 OSI) orientado a BIT.
 - **HMI.** La interfaz de usuario es el medio con que el usuario puede comunicarse con una máquina, un equipo o una computadora, y comprende todos los puntos de contacto entre el usuario y el equipo, normalmente suelen ser fáciles de entender y fáciles de accionar.
 - **HSCSD.** (High-Speed Circuit-Switched Data. Es una mejora de la tecnología CSD, que hace al mecanismo de transferencia de datos de los teléfonos GSM cuatro veces más rápido, con velocidades de hasta 38,4 Kbps.
 - **HTML.** Siglas de HyperText Markup Language (Lenguaje de Marcas de Hipertexto), es el lenguaje de marcado predominante para la construcción de páginas Web.
 - **IBSS.** El modo IBSS, también conocido como modo ad-hoc, se ha diseñado para facilitar las conexiones punto a punto. En realidad existen dos tipos distintos de modos ad-hoc. Uno es el modo IBSS, también conocido como modo ad-hoc o modo ad-hoc del IEEE. Este modo se encuentra especificado en el estándar IEEE 802.11. El segundo tipo se denomina modo ad-hoc de demostración o

modo ad-hoc de Lucent (y algunas veces, también se le llama simplemente modo ad-hoc, lo cual es bastante confuso). Este es el modo de funcionamiento antiguo, anterior al estándar 802.11, del modo ad-hoc debería utilizarse sólo en instalaciones propietarias. No profundizaremos más sobre estos modos de funcionamiento.

- **ISM.** (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (e.g. Wi-Fi) o WPAN (e.g. Bluetooth).
- **IEC 61508.** Norma de seguridad. Es un Sistema diseñado para responder a las condiciones de proceso que pueden ser por si mismas peligrosas o, si no se tomasen medidas, podrían llevar eventualmente a aumentar el peligro, y que genera la salida adecuada para mitigar las consecuencias peligrosas o prevenir el peligro.
- **IEEE 802.11.** Wi-Fi., define el uso de los dos niveles inferiores de la arquitectura OSI (física y enlace de datos), especificando sus normas de funcionamiento en una WLAN.
- **IEEE 802.11a.** Complemento del estándar 802.11, para permitir el uso internacional de redes locales.
- **IEEE 802.11ab.** Estándar de comunicación Wi-Fi.
- **IEEE 802.11b.** Estándar que posee una velocidad máxima de 11 Mbps y utiliza CSMA/CA, definido en el estándar original. Funciona en la banda de 2,4 GHz.
- **IEEE 802.11e.** Introduce nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieran garantías de calidad de servicio.
- **IEEE 802.11g.** evolución del estándar 802.11b. Utiliza la banda de 2,4 GHz, pero opera a 54 Mbps. Compatible con 802.11b.
- **IEEE 802.11h.** Es una modificación del estándar 802.11, que intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de radares y satélites.
- **IEEE 802.11i.** Enfocado en el mejoramiento de MAC 802.11 actual para mejorar la seguridad, autenticación y codificación.
- **IEEE 802.11n.** Norma que especifica un enlace inalámbrico de alta velocidad, hasta un máximo de 600 Mbps. Hace uso simultáneo de las bandas de 2,4 y 5,4 GHz.
- **IEEE 802.11s.** Son redes donde se mezclan las dos topologías de las redes inalámbricas, Ad-hoc y la de infraestructura, denominada redes Mesh.
- **IEEE 802.1d.** Es el estándar de IEEE para Bridges MAC (puentes MAC), que incluye bridging (técnica de reenvío de paquetes que usan los switches), el protocolo Spanning Tree y el funcionamiento de redes 802.11, entre otros.
- **IEEE 802.1Q.** El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.
- **IEEE 802.1w.** Es una evolución del Spanning tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

-
- **IEEE 802.3.** La primera versión fue un intento de estandarizar Ethernet aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).
 - **IFS.** El IFS provee un método unificado para administrar el sistema de archivos que utilizan los routers. Esto incluye los sistemas de archivos de la memoria flash, los sistemas de archivos de red (TFTP y FTP) y la lectura o escritura de datos (de o a la NVRAM, de la configuración en uso, de la ROM). El IFS usa un conjunto común de prefijos para especificar los dispositivos del sistema de archivos.
 - **IGMP.** El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondan periódicamente el estado de la pertenencia.
 - **IHOP.** Modelo de comunicación utilizado por la empresa Siemens en sus Access Point.
 - **IP65.** Índice de protección es un estándar internacional de la Comisión Electrotécnica Internacional 60529 que clasifica el nivel de protección que provee una aplicación eléctrica contra la intrusión de objetos sólidos o polvo, contactos accidentales o agua.
 - **IPSec.** (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.
 - **IRT.** (Tiempo real síncrono).
 - **ISM BAND.** ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. En la actualidad estas bandas han sido popularizadas por su uso en comunicaciones WLAN (e.g. Wi-Fi) o WPAN (e.g. Bluetooth).
 - **OSI.** (Open System Interconnection, Modelo de referencia para la interconexión de sistemas abiertos).
 - **IWLAN.** Redes Ethernet Inalámbricas Industriales.
 - **LLC.** Es la más alta de las dos subcapas de enlace de datos definidas por el IEEE y la responsable del control de enlace lógico. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de la subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión.
 - **LLI.** (Lower Layer Interface, interfase para el nivel inferior).
 - **LONWORKS.** Es una plataforma de control creada por la compañía norteamericana Echelon. Las redes LONWORKS® describen de una manera efectiva una solución completa a los problemas de sistemas de control.
 - **MAC.** Dirección de control de acceso al medio, perteneciente a la capa en enlace de datos del modelo OSI.
 - **MACA.** Un primer protocolo diseñado para redes inalámbricas LANs es MACA (Multiple Access with Collision Avoidance). Se utilizó como base para el

-
- estándar IEEE 802.11 de redes inalámbricas. La idea básica es que el emisor para estimular al receptor le manda una trama corta, así estaciones cercanas pueden detectar esta transmisión y evitarán transmitir a la vez durante el tiempo que tarde la transmisión.
- **MCPS-SAP.** Subcapa de acceso a servicios MAC en redes bajo el estándar IEEE 802.15.4.
 - **MES.** Los MES se basan en definiciones estándares y consistentes (terminologías, modelos y conceptos) creadas por organismos como la ISA (S95), la ISO (15704) y la MESA, organización que define los Sistemas de Ejecución de Manufactura.
 - **MIMO.** Tecnología de Múltiple Input- Multiple Outputs. Permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.
 - **MLME-SAP.** Servicios ofrecidos en la capa de enlace (MAC), en redes bajo el estándar IEEE 802.15.4.
 - **MMS.** Multimedia Messaging System (MMS) o sistema de mensajería multimedia es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos o cualquier otro contenido disponible en el futuro.
 - **MN.** (Managing Node, Nodo administrador).
 - **MODBUS/TCP.** Es una variante o extensión del protocolo Modbus que permite utilizarlo sobre la capa de transporte TCP/IP, por lo cual se lo puede usar en Internet.
 - **MRP.** Los sistemas de planificación de requerimientos de materiales (MRP) integran las actividades de producción y compras. Programan las adquisiciones a proveedores en función de la producción programada. El MRP, es un sistema de planificación de la producción y de gestión de stocks (o inventarios) que responde a las preguntas: ¿qué? ¿cuánto? y ¿cuándo?, se debe fabricar y/o aprovisionar. El objetivo del MRP es brindar un enfoque más efectivo, sensible y disciplinado para determinar los requerimientos de materiales de la empresa.
 - **NORMA IEC61158-2.** Esta subdividida en 6 partes y contempla los aspectos formales relacionados a los niveles 1 y 2 y 7 del modelo de referencia OSI.
 - **NORMA ISO 7498.** Norma internacional que contiene el marco de referencia para la interconexión de sistemas abiertos (modelo OSI).
 - **NRZ.** En telecomunicaciones, se denomina NRZ porque el voltaje no vuelve a cero entre bits consecutivos de valor uno. Mediante la asignación de un nivel de tensión a cada símbolo se simplifica la tarea de codificar un mensaje.
 - **ODVA.** ControlNet es un protocolo de red abierto para aplicaciones de automatismos industriales, también es conocido como bus de campo. ControlNet fue mantenido en un principio por ControlNet Internacional, pero en 2008 el soporte y administración de ControlNet fue transferido a ODVA, que administra actualmente todos los protocolos de la familia Common Industrial Protocol.
 - **OLE/COM.** (Object Linking and Embedding/ Component Object Model).
 - **OPC Server.** El OPC (OLE for Process Control) es un estándar de comunicación en el campo del control y supervisión de procesos. Este estándar permite que diferentes fuentes (Servidores de OPC) envíen datos a un mismo Cliente OPC, al que a su vez podrán conectarse diferentes programas compatibles con dicho estándar. De este modo se elimina la necesidad de que todos los programas cuenten con drivers para dialogar con múltiples fuentes de datos, basta que tengan un driver OPC.

-
- **PAM.** La modulación por amplitud de pulsos (Pulse Amplitud-Modulation) es la más sencilla de las modulaciones digitales. Consiste en cambiar la amplitud de una señal, de frecuencia fija, en función del símbolo a transmitir.
 - **PAN.** IEEE 802.15 es un grupo de trabajo dentro de IEEE 802 especializado en redes inalámbricas de área personal (wireless personal area networks, WPAN). Se divide en cinco subgrupos, del 1 al 5. Los estándares que desarrolla definen redes tipo PAN o HAN, centradas en las cortas distancias. Al igual que Bluetooth o ZigBee, el grupo de estándares 802.15 permite que dispositivos portátiles como PC, PDA's, teléfonos, pagers, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11.x, se definió este estándar para permitir la interoperabilidad de las redes inalámbricas LAN con las redes tipo PAN o HAN.
 - **PBCC.** (Packet Binary Convolution Coding).
 - **PDA.** (Personal Digital Assistant ,Asistente Digital Personal), es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.
 - **PICONET.** Se conoce como piconet a una red de dispositivos informáticos que se conectan utilizando Bluetooth. Una piconet puede constar de dos a ocho dispositivos. En una piconet, habrá siempre un «maestro» y los demás serán esclavos.
 - **PLC.** (Programmable Logic Controller en sus siglas en inglés) son dispositivos electrónicos muy usados en Automatización Industrial. Es un hardware industrial, que se utiliza para la obtención de datos. Una vez obtenidos, los pasa a través de bus (por ejemplo por Ethernet) en un servidor.
 - **PROFIBUS.** Estándar de comunicaciones para bus de campo. Deriva de las palabras PROcess FIEld BUS.
 - **PROFIBUS DP.** (Periferia Distribuida; Decentralized Peripherals), desarrollada en 1993, es la más extendida. Está orientada a control a nivel sensor/actuador.
 - **PROFIBUS FMS.** Diseñada para control a nivel de célula.
 - **PROFIBUS PA.** Es la solución integrada para control a nivel de proceso.
 - **PROFINET.** Estándar Industrial Ethernet para la automatización industrial de Siemens.
 - **PROXY.** El término Proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor Proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
 - **QoS.** Calidad de servicio. Característica de algunos protocolos de red para asegurar los niveles de confiabilidad y latencia de acuerdo con el tipo de tráfico.
 - **RADIUS.** (Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones RC4. Algoritmo de seguridad que usa WEP, considerado un algoritmo inseguro, porque su código fue publicado en Internet.
 - **RCOAX.** Cable coaxil irradiante. Los cables RCoax permiten extender, concentrar y dirigir la radiación electromagnética de un Access Point de manera

-
- que su "campo de iluminación" se extienda geo-métricamente dentro de una zona de interés para la planta que se desea comunicar.
- **RFID.** (Radio Frequency Identification, identificación por radiofrecuencia). Sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tags RFID, que permite transmitir la identidad de un objeto (similar a un número de serie único), mediante ondas de radio.
 - **ROAMING.** La itinerancia (en inglés, y popularmente, roaming) es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. Roaming es una palabra del idioma inglés que significa vagar o rondar. El término más adecuado en castellano es "itinerancia". El concepto de roaming o itinerancia, cuando es utilizado en las redes Wi-Fi, significa que el dispositivo Wi-Fi cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso.
 - **RSTP.** (Rapid Spanning-Tree). Rapid Spanning Tree Protocol (RSTP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. Especificado en IEEE 802.1w, es una evolución del Spanning tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.
 - **SCADA.** Supervisory Control and Data Acquisition (registro de datos y control de supervisión). Es una aplicación de software especialmente diseñada para funcionar sobre ordenadores (computadores) en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos) y controlando el proceso de forma automática desde la pantalla del ordenador. También provee de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros usuarios supervisores dentro de la empresa (supervisión, control calidad, control de producción, almacenamiento de datos, etc.).
 - **SCNM.** (Slot Communication Network Management).
 - **SCTP.** (Screened Twisted Pair, par trenzado apantallado).
 - **SERCOS INTERFACE.** (Serial Real-Time Communication System). Combina los mecanismos en tiempo real establecidos en CERCOS y estandariza el sistema con Ethernet Industrial.
 - **SMS.** El servicio de mensajes cortos o SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (también conocidos como mensajes de texto, o más coloquialmente, textos o mensajitos) entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano. SMS fue diseñado originariamente como parte del estándar de telefonía móvil digital GSM, pero en la actualidad está disponible en una amplia variedad de redes, incluyendo las redes 3G.
 - **SNMP.** Protocolo Simple de Administración de Red. Usado especialmente en las redes TCP/IP, proporciona un medio para supervisar y controlar dispositivos de red, además de manejar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.
 - **SNMP.** El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

-
- **SPANNING-TREE.** (*STP*), es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE_802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.
 - **SSCS.** Subcapa de convergencia específica de servicio. Una de las dos subcapas de cualquier AAL. SSCS, que depende del servicio, brinda una transmisión de datos asegurada. El SSCS también puede ser nulo, en implementaciones IP clásicas sobre ATM o de emulación LAN.
 - **STP.** (Shielded Twisted Pair, Par Trenzado Apantallado). Es similar al cable UTP, con la diferencia que cada par tiene una pantalla protectora, además de tener una lamina externa de aluminio o de cobre trenzado alrededor del conjunto de pares, diseñada para reducir la absorción del ruido eléctrico. Este cable es más costoso y difícil de manipular que el UTP. Se emplea en redes de ordenadores como Ethernet o Token Ring. Su costo en la nueva categoría 6A puede ser el mismo que la versión no apantallada, UTP.
 - **STR.** (Soft real Time). Son sistemas informáticos que se encuentran en multitud de aplicaciones, desde la electrónica de consumo hasta el control de complejos procesos industriales. Están presentes en prácticamente todos los aspectos de nuestra sociedad como, teléfonos móviles, automóviles, control de tráfico, ingenios espaciales, procesos automáticos de fabricación, producción de energía, aeronaves, etc.
 - **TCP.** (Protocolo Control de transmisión). Protocolo de la capa de transporte del modelo OSI orientado a conexión.
 - **TDMA.** Acceso múltiple por división de tiempo. Técnica de división transmisiones en una frecuencia común dentro de periodos, lo que permite que un número más grande de usuarios use una frecuencia determinada.
 - **TFTP.** Protocolo de transferencia de archivo trivial. Versión simplificada FTP, que permite la transferencia de archivos de una computadora a otra a través de la red.
 - **TKIP.** Protocolo temporal de integridad de clave segura, al igual que WEP, esta basado en el cifrado RC4, pero tiene mejoras de generación de nuevas claves de cifrado para cada 10 kbit que se transmiten.
 - **TPC.** (Transmitter Power Control). Funcionalidad requerida por la WLAN que operan en la banda de 5 GHz para asegurar que se respeten las limitaciones de potencia transmitida que puede haber en diferentes canales en una determinada región.
 - **UCMMO.** (Unconnected Message Manager). Mecanismos de afijación que utilizan mensajes del tipo explicit para establecer la conexión, que a seguir será utilizada para el cambio de datos de proceso entre un nudo y otro.
 - **UIT.** La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.
 - **UMTS.** (Universal Mobile Telecommunications System, Sistema universal de Telecomunicaciones móviles. Tecnología utilizada por los móviles de tercera generación 3G, también llamado W-CDMA, sucesora de GSM.
 - **UNICAST.** Es el envío de información desde un único emisor a un único receptor. Se contrapone a multicast (envío a ciertos destinatarios específicos,

-
- más de uno), broadcast (radiado o difusión, donde los destinatarios son todas las estaciones en la red) y anycast (el destinatario es único, uno cualquiera no especificado).
- **USB.** El Universal Serial Bus (bus universal en serie) o Conductor Universal en Serie (CUS), abreviado comúnmente USB, es un puerto que sirve para conectar periféricos a una computadora. Fue creado en 1996 por siete empresas: IBM, Intel, Northern Telecom, Compaq, Microsoft, Digital Equipment Corporation y NEC.
 - **UWB.** Ultra-wideband (también UWB, ultra-wide-band, ultra-wide band, etc.) se usa para referirse a cualquier tecnología de radio que usa un ancho de banda mayor de 500 MHz o del 25% de la frecuencia central, de acuerdo con la FCC (Federal Communications Commission).
 - **VLANs.** Red de área local virtual. Grupo de clientes que están ubicados en lugares distintos pero que se comunican entre si como si pertenecieran al mismo segmento de Lan.
 - **VoWLAN.** Voz sobre redes inalámbricas. VoWLAN (Modo simple) proporciona comunicaciones de datos y de voz móviles a los usuarios que se encuentran dentro de las instalaciones de la empresa.
 - **VPN.** Red Privada Virtual. Es un enlace privado que se efectúa entre dos partes a través de redes públicas.
 - **WAP.** Protocolo de acceso inalámbrico. Lenguaje que se usa para escribir paginas Web que tiene menos sobrecarga en comparación con HTML y XML, usado en accesos inalámbricos de ancho de banda bajo con Internet, para comunicar PDA y teléfonos celulares.
 - **WCDMA.** Wideband Code Division Multiple Access (Acceso múltiple por división de código de banda ancha) cuyo acrónimo es WCDMA es una tecnología móvil inalámbrica de tercera generación que aumenta las tasas de transmisión de datos de los sistemas GSM utilizando la interfaz aérea CDMA en lugar de TDMA (Acceso Múltiple por División de Tiempo) y por ello ofrece velocidades de datos mucho más altas en dispositivos inalámbricos móviles y portátiles que las ofrecidas hasta el momento.
 - **WDS.** Es un sistema de distribución inalámbrico (WDS por sus siglas en inglés) es un sistema que permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11. Permite que una red inalámbrica pueda ser ampliada mediante múltiples puntos de acceso sin la necesidad de un cable troncal que los conecte. La ventaja de WDS sobre otras soluciones es que conserva las direcciones MAC de los paquetes de los clientes a través de los distintos puntos de acceso.
 - **WECA.** Wireless Ethernet Compatibility Alliance, es una empresa creada en 1999 con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse Wi-Fi Alliance.
 - **WEP.** (*Wired Equivalent Privacy* o "Privacidad Equivalente a Cableado"), es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el

-
- sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada
- **WI-FI.** Estándar inalámbrico. Ethernet sin cables.
 - **WI-MAX.** WiMAX son las siglas de Worldwide Interoperability for Microwave Access (interoperabilidad mundial para acceso por microondas). Es una norma de transmisión de datos usando ondas de radio.
 - **WIRELESS LAN.** (Wireless Local Área Network) es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.
 - **WISP.** (Wireless Internet Service Provider). Pueden ser hotspots Wi-Fi o un operador con una infraestructura Wi-Fi. Frecuentemente ofrecen servicios adicionales, como contenido basado en localización, Virtual Private Networking y Voz sobre IP.
 - **WLAN.** Red de área inalámbrica. Una VLAN (acrónimo de Virtual LAN, “red de área local virtual”) es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3).
 - **WPA2.** (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA. WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.
 - **XML.** (Extensible Markup Language (lenguaje de marcas extensible), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML). Por lo tanto XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Algunos de estos lenguajes que usan XML para su definición son XHTML, SVG, MathML.
 - **ZIGBEE.** Es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal área network, WPAN). Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.