

9 capítulo

Redes industriales

Presentación:

- *Necesidades y oferta existente*
- *Tecnologías*
- *Politica de Schneider Electric*



9.1	Introducción	1
9.2	Historia	2
9.3	Requerimientos del mercado y soluciones	3
9.4	Tecnologías de red	4
9.5	Redes recomendadas por Schneider Electric	5
9.6	Ethernet TCP/IP	6
9.7	Servicios web y Transparent Ready	7
9.8	Bus CANopen	8
9.9	La sinergia de Ethernet y CANopen	9
9.10	Bus AS-Interface (AS-I)	10
9.11	Conclusión	11

9. Redes industriales

En esta sección discutiremos las conexiones eléctricas requeridas para el funcionamiento del equipamiento de automatización. Usualmente, esto incluye dos categorías:

- **Conexiones de potencia**, que conectan los componentes de potencia entre la red de alimentación y la carga. No entraremos en este tema, si bien para más información el lector puede dirigirse a otros capítulos.
- **Conexiones de señal**, que conectan todos los componentes de captura, diálogo, tratamiento de datos y control de potencia con la máquina y el proceso.

9.1 Introducción

Tradicionalmente, el cableado de equipos eléctricos se realiza hilo a hilo.

La normativa internacional de máquinas IEC 60 204-1 y las normas específicas de instalaciones (diferentes en cada país) definen con precisión secciones, aislantes y marcado de color. La mayoría de estas conexiones se realizan con unidades de cable flexible con una sección de 1,5-2,5 mm² (AWG 16 y 14), protegidos en sendas extremidades.

Hasta hace una década, estas soluciones cubrían todas las necesidades, tanto para señales digitales como para señales analógicas para servocontrol, requiriendo en éste último caso cables protegidos contra interferencias electromagnéticas.

Influenciadas por las tecnologías de la información y las normas de la industria automovilística, la llegada de la tecnología digital a otras industrias ha tenido un impacto considerable en el diseño y en la construcción de equipamiento eléctrico.

El intercambio de datos digitales impuso conexiones por redes de comunicación que implicaban el uso de conectores y conexiones prefabricadas. Esto simplifica muchísimo la construcción de equipamiento eléctrico dado que los errores de cableado son reducidos y el mantenimiento es más sencillo.

Dado que las tecnologías de conexión convencionales son muy conocidas, nos dedicaremos en esta sección a las redes de comunicación utilizadas en la industria.

9.2 Historia

En 1968, la compañía Modicon inventó el concepto de autómatas programables, un producto único que responde a un amplio rango de necesidades y proporciona una economía de escala. Su gran flexibilidad de uso ofrece numerosas ventajas durante cada etapa de la vida de una instalación industrial. Las redes poco a poco fueron insertándose, inicialmente como enlaces de tipo serie. Los intercambios fueron formalizados por los protocolos, como Modbus (Modicon Bus, 1979), que se ha convertido en un estándar de facto.

Desde hace algunos años, numerosas aplicaciones han adoptado el bus de campo. Esta espina dorsal de la arquitectura del automatismo es una potente herramienta de intercambio, visibilidad y flexibilidad en los dispositivos conectados a él. El bus de campo ha conducido gradualmente a una revisión de la arquitectura:

- supresión del cableado de entradas/salidas;
- supresión o descentralización de los interfaces de entradas/salidas;
- descentralización y distribución de la inteligencia;
- interconexión vía internet.

9. Redes industriales

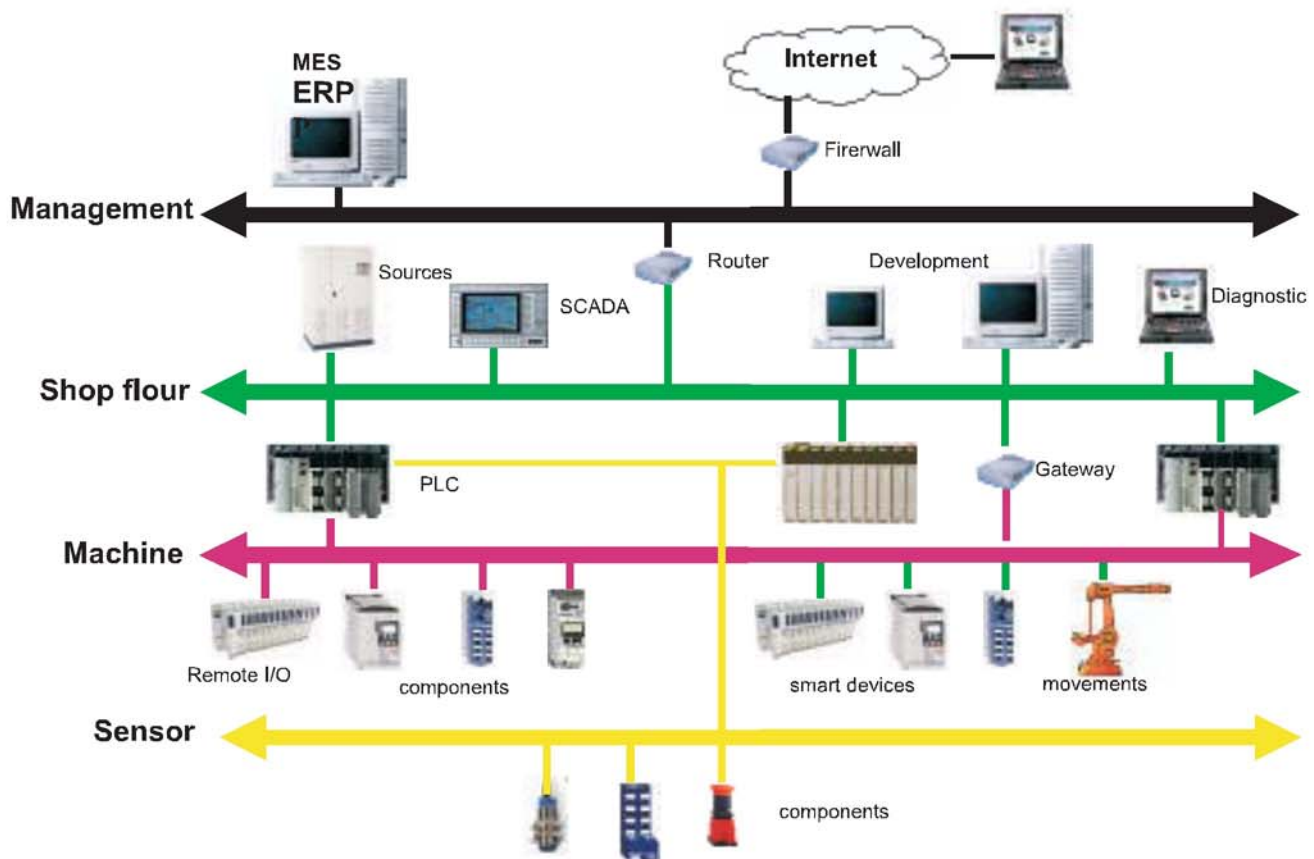
Los años setenta vieron nacer en el Xerox PARC la red Ethernet (de "ether" y "network"), que diez años más tarde se convertiría en un estándar internacional y que se equiparía de forma natural en prácticamente todos los PCs. Sus aplicaciones iniciales fueron la transferencia de archivos y mensajes y la transmisión de páginas web. El desarrollo de las tecnologías de la información en las empresas dio lugar, en los noventa, a la necesidad de la conectividad industrial.

La World Wide Web inventada por la CERN en 1989 fue originalmente desarrollada para permitir a diferentes equipos distribuidos por todo el mundo compartir información. El sistema WWW implica compartir documentos y enlaces mediante HTTP, un sencillo protocolo que utiliza un navegador para acceder a páginas web almacenadas en un servidor. Estas páginas están programadas con lenguajes como HTML o XML. El World Wide Web Consortium (W3C) se creó en 1994 para gestionar el desarrollo técnico de la World Wide Web (ver el sitio <http://www.w3.org>).

En 1996 Schneider Electric promociona la red Ethernet industrial para conectar los niveles "gestión" y "taller" con los autómatas programables, y es entonces cuando desarrolla el concepto de "Transparent Ready". Este concepto se basa en añadir herramientas y protocolos industriales, incluyendo Modbus, a elementos estándar existentes en Ethernet.

9.3 Requerimientos del mercado y soluciones

Con los efectos combinados de los requerimientos de las tecnologías, del usuario y de las normas, las arquitecturas están actualmente estructuradas en cuatro niveles diferenciados, interconectados por redes (⇒ Fig. 1).



↑ Fig. 1 Ejemplo de niveles de arquitectura

9. Redes industriales

Antes de analizar las tecnologías de las redes de comunicación, es necesario presentar una síntesis de las principales necesidades a las cuales estos niveles proporcionan una respuesta pertinente. Las características del cuadro de la *figura 2* se detallarán en los siguientes apartados.

Nivel	Requerimientos	Volumen datos a transmitir	Tiempo de respuesta	Distancia	Topología de la red	Número de direcciones	Medio
Gestión	Intercambio de datos. Seguridad informática. Estándar entre packs de software.	Archivos Mbits	1 min	Mundial	Bus, estrella	Ilimitado	Eléctrico, óptico, radio
Taller	Sincronización de autómatas en una misma célula de intercambio datos en modo cliente/servidor con las herramientas de control (interfaces hombre-máquina, supervisión). En tiempo real.	Datos Kbits	50-500 ms	2-40 Km	Bus, estrella	10-100	Eléctrico, óptico, radio
Máquina	Arquitectura distribuida. Integración funcional y transparencia de intercambios. Costes topología y conexión.	Datos Kbits	50-100 ms (ciclo de autómata)	10 m a 1 Km	Bus, estrella	10-100	Eléctrico, óptico, radio
Sensor	Simplificación del cableado de distribución para alimentar sensores y actuadores. Costes cableado optimizados.	Datos bits		1-100 m	No existe restricción	10-50	Eléctrico, radio

Fig. 2 Requerimientos y restricciones de la comunicación

Una aproximación inicial pasa por adoptar los dos enfoques principales de este cuadro de requerimientos:

- la cantidad de información a transmitir;
- el tiempo de respuesta necesario.

Esto permite posicionar las principales redes del mercado (⇒ Fig.3).

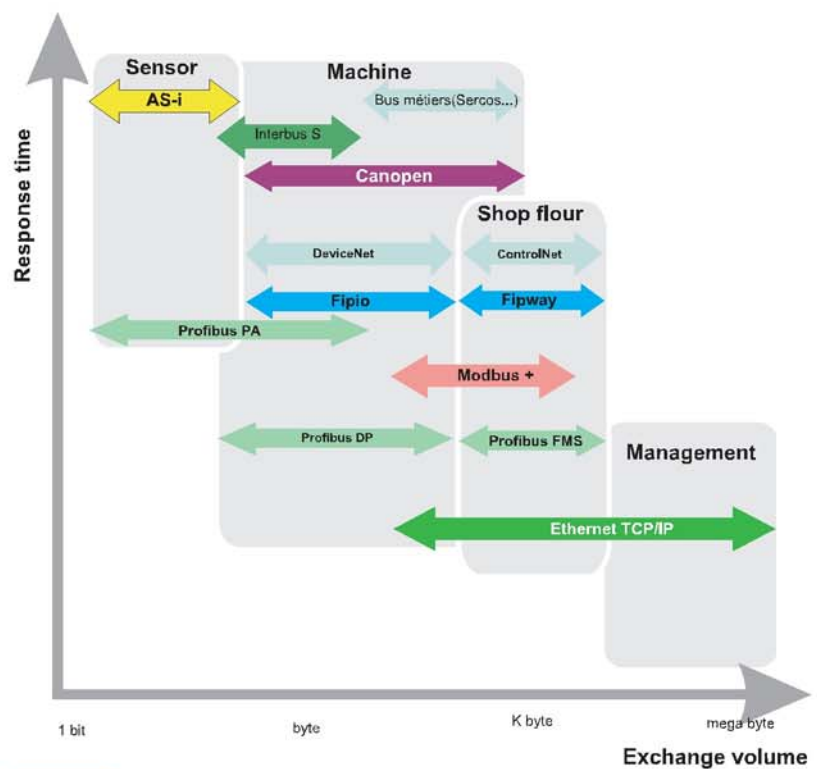
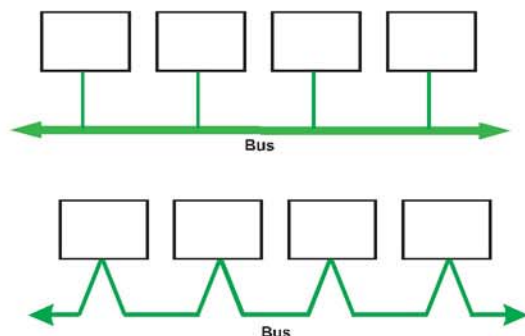


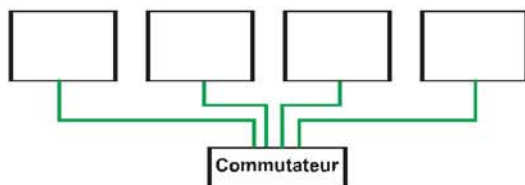
Fig. 3 Principales redes industriales

9. Redes industriales

9.4 Tecnologías de red



↑ Fig. 4 Topología de red bus



↑ Fig. 5 Topología de red estrella

Estos conceptos se describirán de forma breve; para más información, consultar cualquiera de las diversas obras referidas a esta temática.

■ Topología de la red

Una red industrial está compuesta de autómatas, interfaces hombre-máquina, PCs y dispositivos de E/S conectados de forma conjunta por enlaces de comunicación como cables eléctricos, fibras ópticas, enlaces por radio y elementos de interface como tarjetas de red y pasarelas. La distribución física de una red es la topología de hardware o la arquitectura de red.

Para la circulación de información el término utilizado es **topología de software**.

Las topologías normalmente se dividen de la siguiente manera:

- bus,
- estrella,
- árbol,
- anillo,
- malla.

• Topología de bus

Esta es una de las distribuciones más simples; todos los elementos están cableados conjuntamente con la misma línea de transmisión. La palabra "bus" se refiere a la línea física. Esta topología se implementa fácilmente y el fallo de un nudo o elemento no provoca la avería de la red.

Las redes de nivel "máquina" y "sensor", conocidos como buses de campo, usan este sistema.

La topología de bus se implementa conectando los dispositivos conjuntamente en una cadena o al cable principal por una caja de conexiones (TAP) (⇒ Fig. 4).

• Topología de estrella

Esta es la topología de Ethernet, el más común en los niveles "gestión" y "taller" (⇒ Fig. 5). Tiene la ventaja de ser muy flexible en su funcionamiento y reparación. Las estaciones finales están conectadas todas ellas a través de un dispositivo intermedio (repetidor, conmutador). El fallo de un nudo no provoca la avería de la red, si bien los dispositivos intermedios que conectan todos los nudos representan un punto débil.

• Otras topologías (⇒ Fig. 6)

- **Topología de anillo:** utiliza la misma distribución de hardware que la topología de estrella pero asegura una mayor disponibilidad de la red.
- **Topología de malla:** no se utiliza mucho en la industria y presenta el inconveniente de tener un gran número de enlaces.

Anillo	Malla
La topología de anillo usa la misma distribución de hardware que la estrella y asegura mayor disponibilidad.	La topología de malla no se utiliza mucho en la industria y presenta el inconveniente de tener muchos enlaces.

↑ Fig. 6 Otras topologías de red

9. Redes industriales

■ Protocolo

Un protocolo de comunicación establece un conjunto de reglas para un tipo de comunicación particular. Inicialmente, "protocolo" fue la palabra usada para designar lo que se utilizaba para comunicar dos dispositivos diferentes en la misma capa de abstracción. Ahora este término se extiende a las reglas de comunicación entre dos capas de un mismo dispositivo.

El modelo OSI (Open System Interconnection) fue creado por la ISO (International Standards Organisation) que publicó la norma ISO 7498 para proporcionar una base común para la descripción de todas las redes informáticas. Dentro de este modelo, el conjunto de protocolos de una red se divide en 7 partes conocidas como capas OSI, numeradas del 1 al 7. Las capas OSI trabajan según los principios que siguen:

- cada capa soporta un protocolo independientemente de las otras capas;
- cada capa proporciona servicios a la capa inmediatamente por encima de ella;
- cada capa requiere los servicios de la capa inmediatamente por debajo de ella;
- la capa 1 describe el soporte de comunicación;
- la capa 7 proporciona servicios al usuario o a una aplicación.

En la comunicación, el usuario de red utiliza los servicios de la capa 7 a través de un programa. Esta capa formatea y enriquece la información que recibe del programa de acuerdo con su protocolo, y la envía a la capa por debajo de ella cuando se requiere un servicio. Cada capa formatea la información y la adiciona de acuerdo con los protocolos usados. Finalmente, se envía al soporte de comunicación y es recibido por otro nodo de red. Vuelve a través de todas las capas de este nodo y finaliza en el programa correspondiente, sin ninguna adición relacionada con los protocolos.

El modelo OSI de 7 capas ($\Rightarrow$ Fig.7) ha sido implementado por varios fabricantes, pero nunca ha sido un éxito comercial, ya que el mercado siempre se ha decantado por el modelo TCP/IP de 4 capas que tiene un funcionamiento mucho más sencillo y para el cual ya existían implementaciones. Sin embargo, el modelo OSI tiene cierta ventaja teórica, aunque las fronteras de las 4 capas TCP/IP no tienen un equivalente exacto en OSI. Estas capas serán descritas en el apartado dedicado a Ethernet.

Nº	Capa OSI	Función de la capa	Ejemplos
7	Aplicación	Es el interface con el usuario; hace llegar las peticiones a la capa de presentación	HTTP, SMTP, POP3, FTP, Modbus.
6	Presentación	Define como se representará la información, de tal manera que cualquier sistema la interprete.	HTML, XML.
5	Sesión	Garantiza las correctas comunicaciones y conexiones entre los sistemas. Define la apertura de las sesiones sobre los equipamientos de la red.	ISO8327, RPC, Netbios.
4	Transporte	Permite establecer una comunicación de un extremo a otro, segmentar y montar datos, controlar el flujo, detectar errores y repararlos.	TCP, UDP, RTP, SPX, ATP.
3	Red	Se ocupa del transporte de paquetes (datagramas) a través de la red.	IP, ICMP, IPX, WDS.
2	Conexión	Permite establecer, a través de un soporte físico, una conexión libre de errores.	ARCnet, PPP, Ethernet, Token ring.
1	Física	Define los protocolos para el intercambio de bits y los aspectos eléctricos, mecánicos y funcionales del acceso a la red.	CSMA, RS-232, 10 Base-T, ADSL.

† Fig. 7 Capas OSI

9. Redes industriales

■ Trama

Una trama ($\Rightarrow$ Fig.8) es un conjunto de datos enviados a través de una red en un único bloque. También se conoce como paquete. Cada trama tiene la misma disposición básica y contiene información de control como caracteres de sincronización, direcciones de estación, un valor de control de errores, así como una cantidad variable de información.

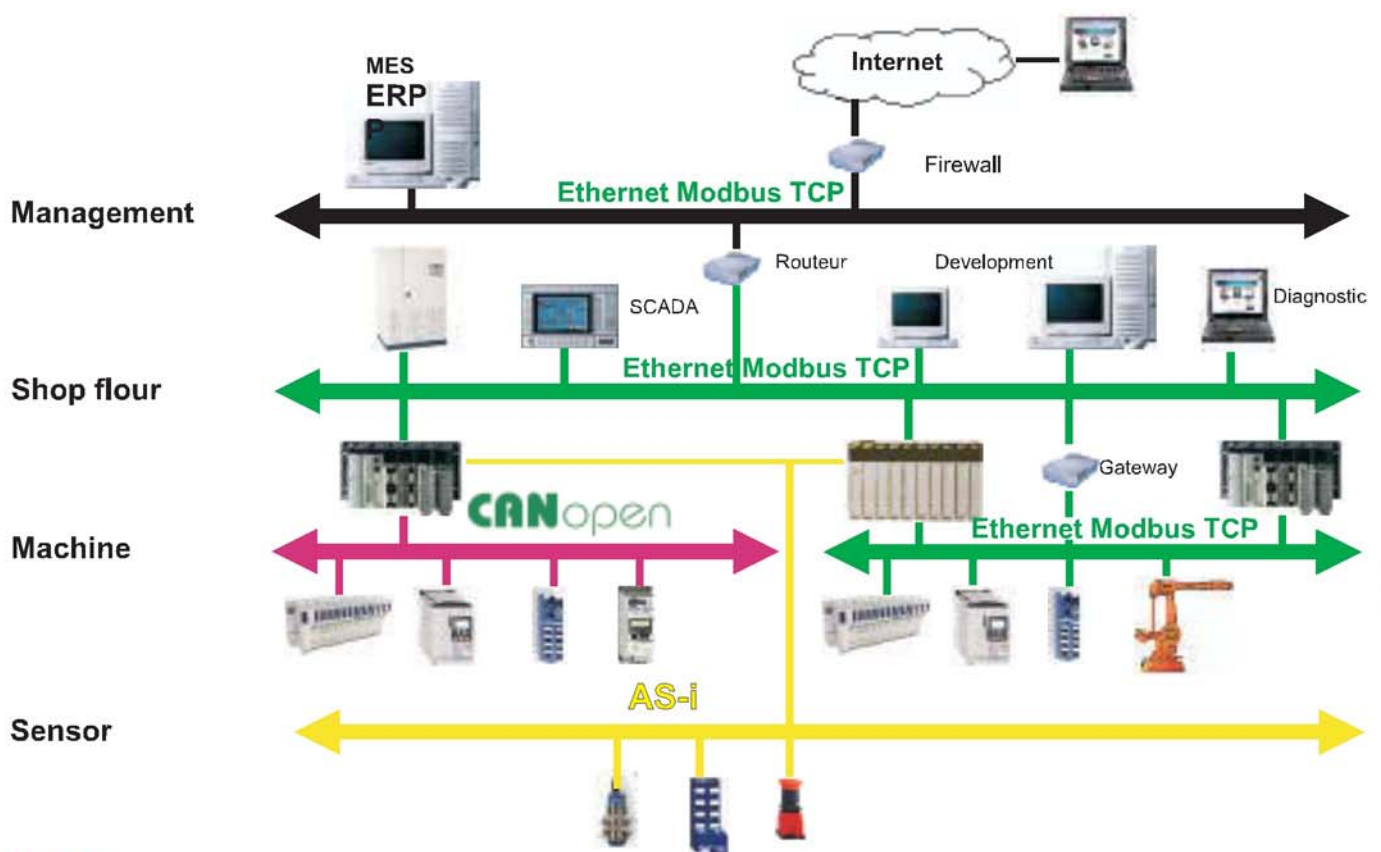
Header	Frame delimiter	Target address	Source address	Data size	Data	Frame sequence control
--------	-----------------	----------------	----------------	-----------	------	------------------------

↑ Fig. 8

Formato de una trama

9.5 Redes recomendadas por Schneider Electric

Para responder a todos los requerimientos con una oferta racional, Schneider Electric ha seleccionado tres redes de comunicación ($\Rightarrow$ Fig.9) para realizar los sistemas descritos en la introducción de este documento.



↑ Fig. 9

Niveles de comunicación elegidos por Schneider Electric

■ Ethernet Modbus TCP

La generalización en el uso de Ethernet en el mundo de los negocios y en Internet ha hecho inevitablemente de él un estándar de comunicación. Ayuda a reducir los costes de conexión y a potenciar las prestaciones, la fiabilidad y la funcionalidad. Su velocidad no frena las aplicaciones y su arquitectura permite una modernización fácil. Los productos y el software son compatibles, por lo que los sistemas se caracterizan por su durabilidad. El protocolo "Modbus", de uso estándar en la industria, proporciona una capa de aplicación simple y barata.

9. Redes industriales

■ CANopen

CANopen es la versión industrial del bus CAN desarrollado para aplicaciones en el campo de la automoción. Esta red tiene una flexibilidad y una fiabilidad probadas por más de 10 años en un amplio rango de aplicaciones como equipamiento médico, trenes y ascensores, así como diversas máquinas e instalaciones industriales. La gran difusión de CANopen avaló la apuesta de Schneider Electric.

■ AS-Interface

Las máquinas modernas tienen un gran número de actuadores y sensores, y a menudo también muchas restricciones. AS-Interface es la red a nivel sensor que cumple con los requerimientos de la automatización industrial. Tiene la ventaja de sus rápidas conexiones y de un único cable que transmite datos y potencia.

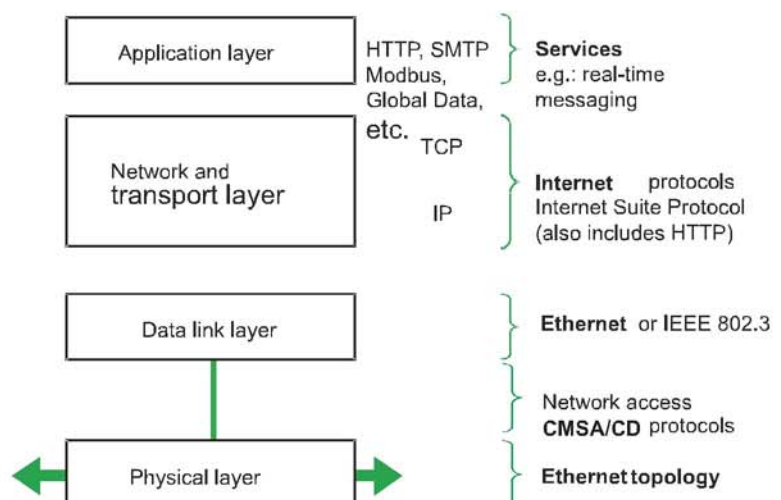
9.6 Ethernet TCP/IP

■ Descripción general

Ethernet funciona bajo el principio de acceso a los medios controlado por un mecanismo de detección de colisiones. Cada estación está identificada por una clave única o dirección MAC, que asegura que cada PC en una red Ethernet tiene una dirección diferente. Esta tecnología, conocida como "Carrier Sense Multiple Access with Collision Detection" (CSMA/CD) asegura que sólo una estación puede transmitir un mensaje en el medio a la vez.

Las mejoras sucesivas de Ethernet han dado lugar a la norma IEEE 802.3 ([ver la página web www.ieee.org](http://www.ieee.org)) que sólo define las características de las capas físicas; la manera como la información accede a la red y la trama de datos debe ser definida por las capas complementarias. La *figura 10* muestra estas capas y los protocolos mencionados se explicarán en los siguientes párrafos, para evitar la normal confusión entre todos estos conceptos.

Durante muchos años, Ethernet estuvo presente en la industria pero fue poco exitosa. Tanto los fabricantes como los clientes la percibían como no-determinista. Su necesidad de control en tiempo real hizo que prefirieran redes propietarias. Fue la combinación de los protocolos industriales y de Internet lo que cambió su parecer.



↑ Fig. 10 Topología de Ethernet

9. Redes industriales

■ Capa física

La capa física describe las características físicas de la comunicación como la convención acerca de la naturaleza del medio usado (cables eléctricos, fibra óptica o enlace por radio) y todos los detalles relacionados como conectores, tipos de codificación y modulación, niveles de señal, longitudes de onda, sincronización y distancias máximas.

■ Capa conexión

La capa conexión especifica el control de acceso al medio y cómo los paquetes de datos son transportados sobre la capa física, en particular la estructura de la trama (esto es, secuencias específicas de bits al principio y al final de los paquetes). Por ejemplo, los encabezados de las tramas de Ethernet contienen campos que indican a qué máquina de la red se destina un paquete.

■ Capa red

En su definición original, la capa red soluciona el problema de transporte de paquetes a través de una única red. Con la llegada del concepto de interconexión de redes, se añadieron algunas funciones adicionales a esta capa, como el transporte de datos desde una red fuente hasta una red destinatario. Esto significa que los paquetes son transportados a través de una red de redes (Internet).

Dentro de los protocolos de Internet, IP transmite paquetes de una fuente a un destinatario en cualquier lugar del mundo. El transporte por IP se hace posible definiendo una dirección IP para asegurar y reforzar la unicidad de cada una de estas direcciones. Cada estación es identificada por su propia dirección IP. El protocolo IP incluye además otros protocolos, como el ICMP usado para transferir mensajes de error de transmisión IP, y el IGMP que gestiona datos multicast. Los protocolos ICMP y IGMP se sitúan por encima de IP pero participan en las funciones de la capa red, ilustrando la incompatibilidad de Internet y OSI.

La capa red IP puede transferir datos para protocolos de más alto nivel.

■ Capa transporte

Los protocolos de la capa transporte pueden solucionar problemas como la fiabilidad del intercambio de datos ("¿han llegado los datos al receptor?"), la adaptación automática a la capacidad de las redes utilizadas, y el control de flujo. Además asegura que los datos llegan en el orden correcto. Por tanto en TCP/IP, estos protocolos determinan a qué aplicación debe entregarse cada paquete.

El TCP es un protocolo de transporte, orientado a la conexión. Proporciona un flujo de bytes fiable que garantiza la llegada de datos sin alteración y en orden, con retransmisión en caso de pérdida y eliminación de datos duplicados. Gestiona también los datos "urgentes" para ser procesados en orden aleatorio (aunque, técnicamente, no se emiten fuera de la banda). El TCP intenta expedir todos los datos correctamente y en orden: es su objetivo y su principal ventaja sobre el UDP, aunque en aplicaciones de transferencia instantánea esto puede ser una desventaja con elevadas tasas de pérdida en la capa red. El UDP es un protocolo simple, sin conexión y "no-fiable". Ello no significa que sea poco fiable, el problema es que no comprueba que los paquetes lleguen a destino y en orden. Si una aplicación necesita estas garantías, o se las asegura por sí misma, o bien usa el TCP. El UDP es normalmente usado para aplicaciones de difusión, tales como el Global Data o las aplicaciones multimedia (audio, video, etc.), donde el tiempo requerido por el TCP para gestionar la retransmisión y la ordenación de paquetes no están disponibles, o para aplicaciones basadas en mecanismos simples de pregunta/respuesta como las peticiones SNMP, donde el coste más elevado de establecer una conexión es desproporcionado a las necesidades.

El TCP y el UDP se utilizan para muchas aplicaciones. La diferencia entre las que usan servicios TCP o UDP radica en su número de puerto. El Modbus TCP usa servicios TCP. El UDP se puede usar en Factorycast.

■ Capa aplicación

La mayoría de funciones de las aplicaciones de red se sitúan en esta capa.

Ello incluye el HTTP (World Wide Web), el FTP (transferencia de ficheros), el SMTP (servicio de mensajería), el SSH (conexión remota securizada), el DNS (búsqueda de correspondencia entre nombres y direcciones IP) y muchos otros.

Las aplicaciones funcionan generalmente bajo TCP o UDP y están normalmente asociadas a un puerto bien conocido. Ejemplos:

- HTTP puerto TCP 80 u 8080;
- Modbus puerto 502;
- SMTP puerto 25;
- FTP puerto 20/21.

Estos puertos fueron asignados por el Internet Assigned Numbers Authority.

□ El protocolo HTTP ("HyperText Transfer Protocol")

Se usa para transferir páginas web entre un servidor y un navegador. El HTTP se ha usado en la web desde 1990.

Los servidores web integrados en los dispositivos de automatización Transparent Ready proporcionan un acceso fácil a los productos en cualquier parte del mundo a través de un navegador, como Internet Explorer, Netscape Navigator u otros.

□ BOOTP/DHCP

Proporciona de forma automática los parámetros de las direcciones IP de los productos. Esto evita tener que encontrar la dirección individual de cada dispositivo prorrogando esta gestión en un servidor de direcciones IP dedicado.

El protocolo DHCP ("Dynamic Host Configuration Protocol") asigna de forma automática los parámetros de configuración de los dispositivos. El DHCP es una extensión del BOOTP. El protocolo BOOTP/DHCP tiene dos componentes:

- el servidor que proporciona la dirección de red IP;
- el cliente que pide la dirección IP.

Los dispositivos de Schneider Electric pueden ser:

- Clientes BOOTP/DHCP que automáticamente recuperan la dirección IP procedente de un servidor;
- Servidores BOOTP/DHCP que permiten al producto distribuir las direcciones IP a las estaciones de red.

Los protocolos estándar BOOTP/DHCP se usan para proporcionar el servicio de sustitución de dispositivos defectuosos ("Faulty Device Replacement", FDR).

□ FTP ("File Transfer Protocol")

Proporciona los elementos básicos para la transferencia de archivos. Este protocolo es utilizado por multitud de sistemas para intercambiar ficheros entre productos.

□ TFTP ("Trivial File Transfer Protocol")

Es un protocolo que simplifica la transferencia de archivos, y que permite descargar códigos de productos. Por ejemplo, se puede usar para transferir el código de arranque (boot code) en una estación de trabajo sin unidad de disco o para conectarse y descargar actualizaciones de software. Los productos Transparent Ready aplican el FTP y el TFTP para transferir información entre ellos.

9. Redes industriales

□ NTP ("Network Time Protocol")

Se utiliza para sincronizar la hora en dispositivos (cliente o servidor) a través del servidor de un proveedor. Dependiendo de la red usada proporciona, a partir de la hora universal (UTC), una precisión de algunos milisegundos en una red local (LAN) o de algunas decenas de milisegundos en una red ancha (WAN).

□ SMTP ("Simple Mail Transfer Protocol")

Proporciona un servicio de transmisión de correos electrónicos, enviándolos entre un emisor y un destinatario a través de un servidor SMTP.

□ SNMP ("Simple Network Management Protocol")

La comunidad de Internet desarrolló este estándar para gestionar los diferentes componentes de una red a través de un único sistema. El sistema de gestión de la red puede intercambiar datos con los productos agentes SNMP. Esta función permite al gestor visualizar el estado de la red y de los dispositivos, modificar su configuración y rearmar las alarmas en caso de fallo. Los dispositivos Transparent Ready son compatibles con SNMP y pueden integrarse de forma natural en una red SNMP.

□ COM/DCOM ("Distributed Component Object Model") u OLE ("Object Linking and Embedding")

Es el nombre de la tecnología que compone los objetos de Windows utilizados para una comunicación transparente entre aplicaciones de Windows. Estas tecnologías se utilizan en software de servidor de datos OFS ("OLE for Process Control Factory Server").

9.7 Servicios web y Transparent Ready

Como ya se ha explicado, dado que los servicios universales no se ajustan a los usos industriales, los fabricantes de componentes han completado la oferta de servicios universales de Internet con funciones específicas de automatización.

Schneider Electric ha desarrollado una gama de comunicación "transparente" entre la web y los niveles descritos anteriormente, definiéndola como tecnología web integrada en productos y servicios. Esta gama de comunicación tiene dos pilares básicos:

- La red Ethernet industrial;
- Los componentes WEB.

El objetivo es ofrecer "**servicios**" con funciones que permitan al cliente desarrollar tareas específicas como enviar datos de un autómatas programable a otro o hacer saltar una alarma.

La "tecnología web" significa lo mismo que la "tecnología Internet" y comprende: protocolos de Internet, lenguajes de programación como Java, HTML, CML, etc. y las herramientas que han revolucionado la manera de compartir la información.

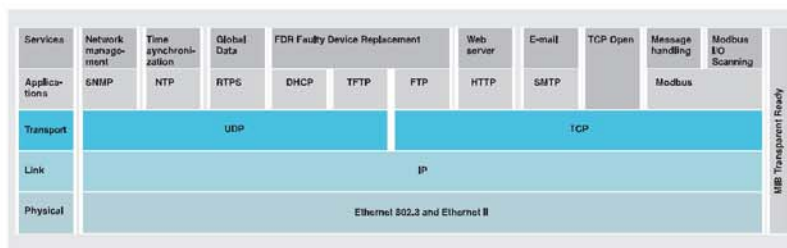
9. Redes industriales

■ Servicios Ethernet industriales

Además de los servicios Ethernet universales (HTTP, BOOTP/DHCP, FTP, etc.), se pueden proporcionar ocho tipos diferentes de servicios de comunicación Ethernet con:

- Servicio de mensajería Modbus TCP;
- Servicio de intercambio de E/S remotas: I/O Scanning;
- Servicio de sustitución de equipamiento defectuoso: FDR;
- Servicio de administración de red: SNMP;
- Servicio de administración de datos global;
- Servicio de gestión de la banda de transmisión;
- Servicio de sincronización de la hora: NTP;
- Servicio de notificación de eventos: SMTP (correo electrónico).

La **tabla 11** muestra la posición de estos servicios en relación con las capas de la red.

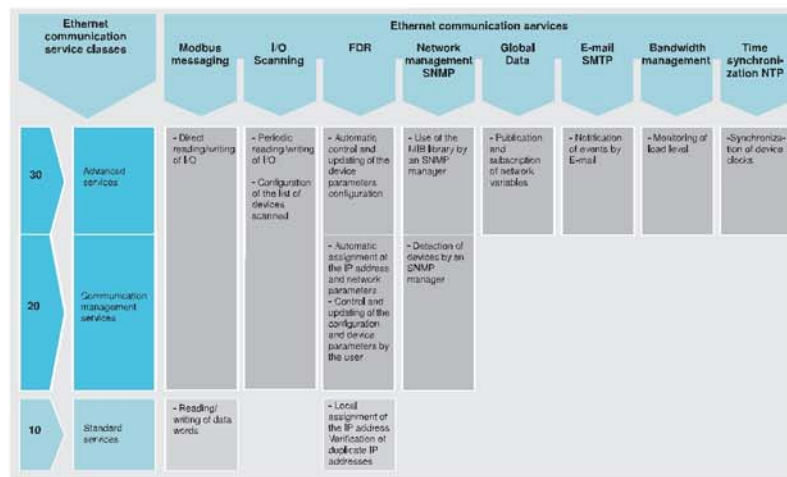


↑ **Fig. 11** Posición de los servicios de comunicación Ethernet

Estos servicios de comunicación se dividen en tres clases:

- Clase 10: servicios básicos de comunicación Ethernet;
- Clase 20: servicios de gestión de la comunicación Ethernet (nivel red y nivel producto);
- Clase 30: servicios avanzados de comunicación Ethernet.

La **tabla 12** da una breve descripción de los servicios.



↑ **Fig. 12** Breve descripción de los servicios Ethernet

■ Servicio de mensajería: Ethernet Modbus TCP

Modbus, el estándar de comunicación industrial desde 1979, fue aplicado a Ethernet TCP/IP para crear Ethernet Modbus TCP, un protocolo Ethernet completamente abierto. El desarrollo de una conexión Ethernet Modbus TCP no requiere ningún componente propietario o licencia de compra. El protocolo se puede aplicar a cualquier dispositivo que soporte un estándar de comunicación TCP/IP. Las especificaciones se pueden encontrar de forma gratuita en la página web www.modbus-ida.org.

9. Redes industriales

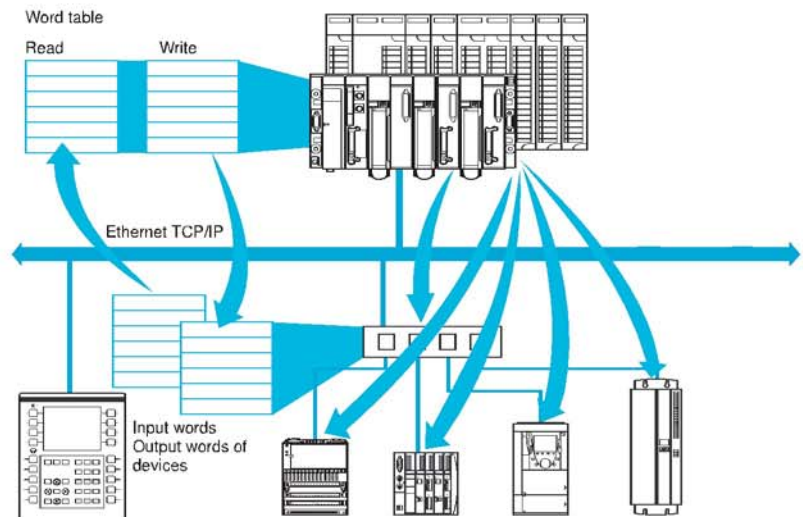
Su simplicidad permite que cualquier dispositivo de campo, como un módulo de E/S, se comuniquen vía Ethernet sin necesidad de un potente microprocesador o de mucha memoria interna. El Ethernet Modbus TCP tiene un protocolo muy sencillo y una salida a 100 Mbps que garantizan sus excelentes prestaciones permitiendo que este tipo de red sea usada en aplicaciones en tiempo real.

Dado que el protocolo de aplicación es idéntico que en un Modbus conexión serie, Modbus Plus y Ethernet Modbus TCP, los mensajes se pueden direccionar de una red a otra sin tener que cambiar protocolos. Modbus se implementa sobre la capa TCP/IP, por lo que los usuarios se benefician también del direccionamiento IP que permite a los dispositivos en cualquier lugar del mundo comunicarse sin importar la distancia que los separa.

La IANA ("Internet Assigned Numbers Authority") ha asignado al Ethernet Modbus TCP con el puerto fijo TCP 502, haciendo de Modbus un estándar de Internet. El tamaño máximo de los datos es de 125 palabras o registros en modo escritura y 100 palabras o registros en modo lectura.

■ Servicio de intercambio de E/S remotas: "I/O Scanning"

Este servicio se utiliza para gestionar el intercambio de estados entre E/S remotas a través de la red Ethernet. Después de una simple configuración y sin necesidad de programación específica, las E/S se escanean "transparentemente" con ayuda de peticiones de lectura/escritura según el protocolo cliente/servidor Ethernet Modbus TCP. Este principio de escaneo permite comunicar, mediante un protocolo normal, con cualquier producto que soporte Ethernet Modbus TCP. Este servicio permite definir dos zonas de palabras (lectura entradas, escritura salidas) (⇒ Fig. 13). Los periodos de refresco son independientes del ciclo del autómatas.



↑ Fig. 13 Servicio de intercambio de E/S remotas: "I/O Scanning"

Durante el funcionamiento, el módulo asegura:

- la gestión de las conexiones TCP/IP con cada uno de los dispositivos remotos;
- el escaneo de productos y E/S copiándolos en la zona configurada de palabras;
- el "feedback" de las palabras de estado para controlar el buen funcionamiento del servicio desde la aplicación del autómatas;
- el uso de valores preconfigurados por defecto en caso de problemas de comunicación.

Una gama de hardware y software para implementar el protocolo I/O Scanning en cualquier dispositivo que pueda ser conectado a Ethernet Modbus TCP se puede encontrar en la web de Modbus-IDA (www.modbus-ida.org).

■ Servicio "Faulty Device Replacement" (FDR)

El servicio de sustitución de un producto defectuoso utiliza la tecnología de gestión de direcciones estándar (BOOTP, DHCP) y el servicio de gestión de ficheros FTP o TFTP ("Trivial File Transfer Protocol"). Esto facilita el mantenimiento de los dispositivos conectados a Ethernet Modbus TCP.

Sustituye un dispositivo que falla por uno nuevo y asegura que el sistema lo detecta, lo reconfigura y lo reinicia automáticamente. Los pasos principales de esta sustitución son:

- un dispositivo que utiliza el servicio FDR tiene un fallo;
- se coge un producto similar de un stock de mantenimiento, preconfigurado con el nombre del dispositivo que falla y reinstalado en la red. Dependiendo del dispositivo, se puede direccionar con selectores rotativos (por ejemplo, E/S distribuidas Advantys STB, o Advantys OTB) o con el teclado integrado del dispositivo (por ejemplo, el variador de velocidad Altivar 71);
- el servidor FDR detecta el nuevo dispositivo, le asigna una dirección IP y le transfiere los parámetros de configuración;
- el dispositivo de sustitución comprueba que todos los parámetros son compatibles con sus propias características y cambia a modo operativo.

■ Servicio de administración de redes: SNMP

El protocolo SNMP ("Simple Network Management Protocol") supervisa y controla todos los componentes de la arquitectura Ethernet desde una estación gestora de red, para permitir un rápido diagnóstico de problemas que puedan surgir. Se usa para:

- interrogar a los componentes de la red como PCs, routers, switches, bridges y terminales para visualizar su estado;
- obtener estadísticas de la red donde están conectados los dispositivos.

Este software de gestión de red utiliza el modelo tradicional cliente/servidor. Sin embargo, para evitar confusiones con otros protocolos de comunicación que usan la misma terminología, se hace referencia a éste como gestor de red o agente SNMP.

Los dispositivos Transparent Ready los puede gestionar un agente SNMP, incluyendo HP Openview, IBM Netview y, desde luego, la herramienta de gestión de redes Transparent Ready ConnexView. El protocolo estándar SNMP ("Simple Network Management Protocol") proporciona acceso a los objetos de configuración y gestión en los MIBs ("Management Information Bases") de los dispositivos. Los MIBs deben cumplir con ciertas normas para hacerlos accesibles para todas las herramientas de gestión, pero según la complejidad de los productos, los fabricantes pueden añadir algunos objetos en la MIB privada. La MIB privada de Transparent Ready tiene objetos de gestión específicos para los servicios de comunicación Transparent Ready como Modbus, Global Data, FDR, etc. Estos objetos facilitan la instalación, implementación y mantenimiento de dispositivos.

9. Redes industriales

Los dispositivos Transparent Ready soportan dos niveles de gestión de red SNMP:

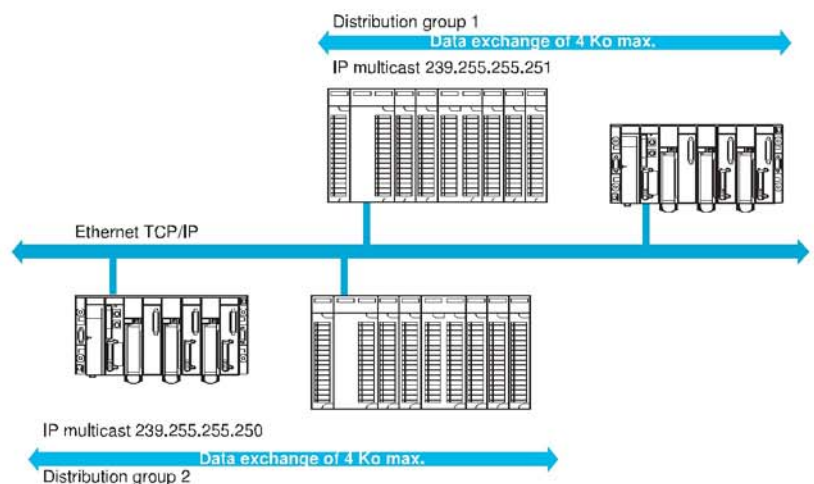
- El interface MIB II Standard: un nivel de gestión de red básico es accesible a través de este interface. El gestor la utiliza para identificar los productos que componen la arquitectura y recuperar información general sobre la configuración y funcionamiento de interfaces Ethernet TCP/IP;
- El interface Transparent Ready MIB: este interface mejora la gestión de dispositivos Transparent Ready. La MIB dispone de un conjunto de información que permite al sistema de gestión de red supervisar todos los servicios Transparent Ready. Puede descargarse desde el servidor FTP de cualquier módulo Transparent Ready Ethernet de un autómatas programable.

■ Servicio de distribución "Global Data" (⇒ Fig.14)

El servicio "Global Data" asegura la distribución de datos multicast en tiempo real entre estaciones en el mismo grupo de distribución. Puede sincronizar aplicaciones remotas o compartir una base de datos común entre aplicaciones distribuidas. Los intercambios están basados en protocolos publicación/suscripción estándar, garantizando unas prestaciones óptimas con una carga mínima de la red. El protocolo RTPS ("Real Time Publisher Subscriber") está promovido por Modbus-IDA ("Interface for Distributed Automation") y ya es una norma adoptada por varios fabricantes. Hasta 64 estaciones pueden formar parte de intercambios via Global Data con el mismo grupo de distribución. Cada estación puede:

- publicar una variable de 1.024 bytes. El periodo de publicación puede ser configurado desde 1 hasta n periodos de la tarea maestra del procesador;
- suscribir desde 1 hasta 64 variables.

La validez de cada variable es controlada por bits de estado ("health status bits") vinculados a un timeout de refresco configurable de 50 ms a 1 s. El acceso a un elemento de variable no es posible. El tamaño total de variables suscritas alcanza 4 Kbytes contiguos. Para optimizar más las prestaciones de Ethernet, se puede configurar el Global Data con la opción "multicast filtering" que, combinada con los switches de la gama ConneXium, garantiza la difusión de los datos solamente sobre los puertos Ethernet donde existe una estación suscrita al servicio Global Data. Si estos switches no se utilizan, éste se emite en "multicast" sobre todos sus puertos.



↑ Fig. 14

Servicio de distribución "Global Data"

■ Servicio de sincronización de la hora NTP

El servicio de sincronización de la hora se basa en el protocolo NTP ("Network Time Protocol") para sincronizar la hora de un cliente o servidor Ethernet TCP/IP desde un servidor o cualquier otra fuente de una hora de referencia (radio, satélite, etc.).

Los módulos de comunicación de Ethernet Modbus TCP: – plataformas de automatización 140 NOE 771 11 para Modicon Quantum Unity V2.0 (o superior); plataformas de automatización TSX ETY 5103 para Modicon Premium Unity V2.0 (o superior) – tienen un componente cliente NTP. Estos módulos se pueden conectar a un servidor NTP utilizando una petición cliente (unicast) para establecer su hora local. Periódicamente (de 1 a 120 segundos), el reloj del módulo se actualiza con un error inferior a 10 ms para procesadores convencionales e inferior a 5 ms para procesadores de altas prestaciones. Si el servidor NTP no se puede localizar, el módulo Ethernet Modbus TCP utiliza un servidor NTP de socorro ("standby").

■ Servicio de notificación por correo electrónico SMTP

Este simple servicio de notificación por correo electrónico se puede programar. La aplicación del autómata lo utiliza para notificar un evento bajo unas condiciones. El autómata crea el correo automática y dinámicamente para alertar un destinatario definido, conectado en local -o remoto-. Hay que remarcar que este servicio está disponible con los últimos módulos de comunicación Ethernet para los autómatas Modicon Premium y Quantum, y con los últimos procesadores con conexión a Ethernet en los mismos autómatas usados con el software Unity Pro. Hay además un servicio más completo e independiente de la aplicación del autómata disponible con el módulo servidor web FactoryCast HMI.

El mecanismo es simple y efectivo: se enlazan encabezamientos de mensajes predefinidos con el cuerpo del correo que se crea dinámicamente a partir de la última información de la aplicación del autómata. La aplicación del autómata prepara el mensaje de acuerdo con unas condiciones predeterminadas. Un bloque función se usa para seleccionar uno de los 3 encabezamientos predefinidos, crea el correo con las variables y texto (hasta 240 bytes) y lo envía directamente desde el autómata. Los 3 encabezamientos contienen los siguientes elementos predefinidos:

- lista de destinatarios de correo electrónico;
- nombre del remitente y asunto.

Esta información está definida y actualizada por un administrador autorizado a través de páginas web de configuración.

■ Servicios web (⇒ Fig. 15)

El nivel de un servicio de servidor web está definido por 4 clases de servicio identificados por una letra:

□ Clase A

Dispositivos Transparent Ready sin servicios web.

□ Clase B

Nivel web básico para gestionar páginas web estáticas preconfiguradas en un dispositivo Transparent Ready. Ofrece servicios de diagnóstico y de supervisión de dispositivos usando un navegador web estándar.

9. Redes industriales

□ **Clase C**

Nivel web configurable para personalizar el sitio web del dispositivo Transparent Ready con páginas web definidas por el usuario para las necesidades de su aplicación. El procedimiento de diagnóstico y supervisión se puede efectuar desde un navegador web estándar. La gama Factorycast incluye esta funcionalidad de nivel web así como herramientas para facilitar la gestión y modificación de sitios web integrados.

□ **Clase D**

Nivel web activo para ejecutar procesos específicos en el mismo dispositivo servidor web Transparent Ready. La capacidad de procesamiento se puede usar para precálculos, gestión de bases de datos en tiempo real, comunicación con bases de datos de tipo relacional y envío de correos electrónicos. La comunicación entre el navegador y el servidor por tanto se reduce y optimiza. La gama Factorycast incluye este nivel de funcionalidad web así como herramientas para configurar los procesos a ejecutar en el dispositivo servidor web.

Web server class		Web services			
		Maintenance	Monitoring and IT link	Diagnostics	Optional
D	Active Web server	- User website update	- Autonomous execution of specific services (e.g. alarm notification by E-mail, exchange with databases, calculations, ...) - SOAP/XML (client/server)	- User-defined states	- User documentation
C	Configurable Web server		- PLC variables editor - Remote commands - User Web pages - SOAP/XML (server)	- Communication service diagnostics - State of internal device resources	
B	Standard Web server	- Remote device software update - Remote auto-tests	- Device description - Data viewer	- Device status - Device diagnostic	- Configuration of network parameters and Ethernet communication services - Device documentation
A	No Web server	- No Web service			

↑ Fig. 15 Servicios web

□ **Dispositivos Transparent Ready**

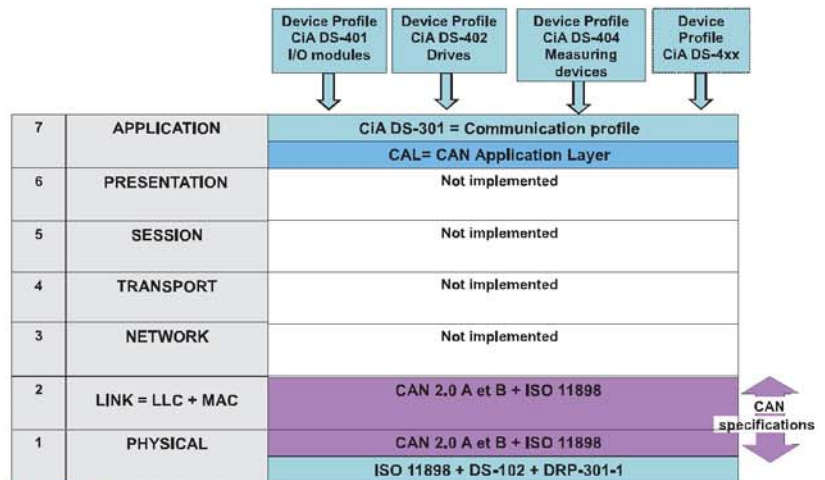
Se identifican por una letra que define el nivel de servicios web seguido de un número que define el nivel de servicio de comunicación Ethernet. Ejemplos:

- Clase A10: es un dispositivo sin servicio web y con servicios básicos de comunicación Ethernet;
- Clase C30: es un dispositivo con un servidor web configurable y con servicios avanzados de comunicación Ethernet.

9. Redes industriales

En el 2001, la publicación del DS-304 permitió la integración de los componentes de seguridad de nivel 4 en un bus CANopen estándar (CANsafe).

A continuación se detallan las características técnicas de CANopen.



↑ Fig. 17 Capas de un bus CAN

■ Ventajas de CANopen

□ CANopen usa tramas cortas

Debido a su gran inmunidad a interferencias electromagnéticas, CANopen permite que una máquina o planta trabaje con precisión, incluso en una atmósfera con grandes interferencias. Las tramas cortas de CANopen y la conexión CANground ofrecen las mismas capacidades para cada dispositivo conectado a la red y los protege de las interferencias electromagnéticas.

□ CANopen para una transmisión fiable

Cuando un dispositivo CANopen transmite datos, el sistema genera el mensaje y automáticamente tiene en cuenta su prioridad. La pérdida de un telegrama por problemas de colisión es imposible, y se evita la pérdida de tiempo de espera del próximo estado inactivo ("idle") de la red. CANopen permite una transmisión de datos perfecta. Ello constituye una de las razones por las que CANopen se utiliza en equipamientos médicos que requieren redes fiables.

□ CANopen elimina la pérdida de tiempo

Las pérdidas de tiempo también suponen una pérdida de dinero. CANopen está diseñado para reducir estas pérdidas al mínimo. Con su distancia de "hamming" de 6, CANopen tiene una gran capacidad de detección de errores y un excelente mecanismo de corrección. Con una probabilidad de un error no detectado cada 1.000 años, CANopen es la red más fiable para máquinas e instalaciones.

1 bit de error cada 0,7s a 500Kbps, 8 horas al día, 365 días al año.

Cuando la red detecta una condición de error, el "perro guardián" es la primera posibilidad de vigilancia del estado del equipamiento. Cada mensaje de diagnóstico contiene la fuente y la causa del error, permitiendo así una rápida respuesta y una menor pérdida de tiempo. Se realiza además un diagnóstico suplementario para mejorar la diagnosis de los dispositivos CANopen complejos y mantener la red. Además, existe un registro de errores para detectar fallos aleatorios.

9. Redes industriales

□ CANopen: prestaciones y flexibilidad

El motivo principal para utilizar una red son sus prestaciones y su flexibilidad de adaptación de forma precisa a las necesidades de la aplicación. CANopen ofrece un único dispositivo para la adaptación de la transmisión de datos. Basado en el modelo productor/consumidor, CANopen puede transferir datos en modo difusión general, punto a punto, cambio de estado y cíclico. Significa que los datos se transfieren sólo si es necesario o en una escala de tiempo específica. Los PDO son configurables individualmente. Los parámetros se pueden cambiar siempre.

• Prestaciones

Aunque CANopen es muy flexible, la respuesta de la red es muy rápida. 256 puntos de E/S numéricas se pueden procesar a 1 Mbps en menos de 1 ms. Típicamente, el Profibus-DP requiere unos 2 ms a 12 Mbps para la misma transferencia de datos. Además de la rapidez de respuesta, en CANopen el control de la prioridad de los mensajes se puede cambiar.

Con CANopen, la transmisión de datos se puede adaptar para ajustarse a las necesidades de la aplicación.

□ CANopen reduce los costes

CANopen ofrece facilidad de instalación y dispositivos de bajo coste. No requiere una conexión equipotencial entre dispositivos como pasa en muchos buses de campo. Una conexión pobre no sólo provoca errores de comunicación, sino que también daña los dispositivos de bus de campo.

Además, los componentes CANopen se producen en grandes cantidades lo que reduce su precio. Schneider Electric ofrece, de forma notable, esta ventaja a sus clientes.

Los precios son un 10-20% más baratos que en otros buses de campo.

■ Cómo funciona CAN

CAN es un bus serie basado en un modelo publicación/suscripción, en el cual un editor envía un mensaje a los suscriptores. CAN fue desarrollado con arquitectura "broadcast".

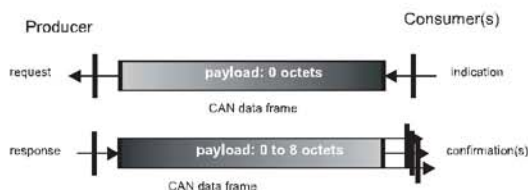
El emisor (editor) envía un mensaje con un identificador. Los destinatarios (suscriptores) filtran los mensajes del bus basándose en el criterio de envío por lo que si un mensaje está destinado a ellos, lo leen y lo procesan. El destinatario se convierte entonces en el emisor (⇒ Fig.18).

El diagrama muestra el modo "push" (envío) del modelo publicación/suscripción. CAN también soporta el modelo "pull" (recepción). Un cliente puede enviar un mensaje basándose en una petición de transmisión remota ("Remote Transmission Request", RTR), que es una trama CAN con "flags" (bits de estado). Cuando el productor recibe tal demanda, transmite la respuesta asociada (⇒ Fig.19).

En una arquitectura "broadcast", los nodos de red pueden transmitir al mismo tiempo. CAN tiene 2 mecanismos para ello: primero, un emisor supervisa la arteria de comunicación para comprobar si otro nodo ya está transmitiendo. Si la arteria está libre, el nodo empieza a transmitir. Varios nodos pueden empezar la transmisión pero nunca al mismo tiempo. Este problema se puede solucionar con un sistema de prioridad.



↑ Fig. 18 Funcionamiento de CAN



↑ Fig. 19 CAN push / pull (modelo publicación / suscripción)

9. Redes industriales

Una trama CAN ($\Rightarrow$ Fig. 20) empieza con un bit de principio de trama ("Start Of Frame", SOF) seguido de once bits de identificación, de más a menos significativo. El siguiente es el bit de solicitud de transmisión remota, seguido de 5 bits de control y hasta 8 bytes de datos útiles. Los bits de control son: el ID extendido (IDE), un bit reservado y tres bits que cifran la longitud en bytes de datos útiles (DLC). Una secuencia de verificación de la trama ("Frame Check Sequence", FCS) de hasta 8 bytes sigue a los datos útiles. El emisor envía un bit de reconocimiento (ACK) que es sustituido por un bit dominante por los destinatarios que hayan recibido la trama sin error.



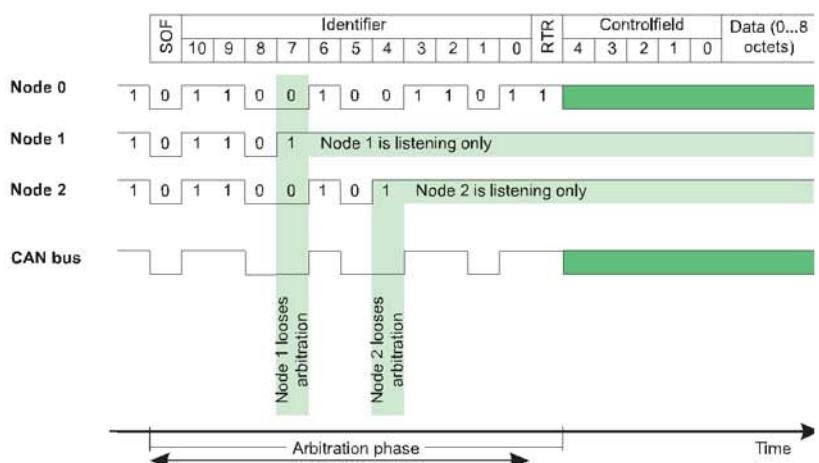
↑ Fig. 20 Trama CAN

El bit de fin de trama ("End Of Frame", EOF) indica el final de la trama.

El bit IFS ("Intermission Frame Space") del bus debe permanecer en posición recesiva antes de la salida de la siguiente trama. Si ningún nudo está dispuesto a transmitir, el bus mantendrá su estado. La codificación de los bits posee dos valores: dominantes y recesivos. Si dos nudos emiten al mismo tiempo, el receptor sólo verá el valor dominante. En binario, "0" es dominante y "1" recesivo. Cuando un nudo emite, el bus automáticamente lo detecta. Si transmite un bit recesivo y recibe uno dominante, deja de transmitirlo de tal manera que pueda continuar recibiendo el dominante. Este simple sistema previene colisiones en el bus CAN. El mensaje con el identificador más pequeño tiene prioridad en el bus.

CAN es un sistema de bus de acceso múltiple, con detección de colisión y priorización de mensajes (CSMA/CD+AMP). Dado que las colisiones nunca ocurren, se dice que el bus CAN es CSMA/CA (siglas del inglés "Carrier Sense Multiple Access/Collision Avoidance").

En la figura 21 se puede ver la trama básica de un mensaje bajo CAN. Para aplicaciones que requieren más identificadores, existe el formato de trama extendida CAN. La trama extendida tiene 18 bits extra de identificación al principio, después de los bits de control. Ello extiende el rango de 211 a 229 identificadores diferentes. Los dos tipos de trama pueden coexistir en un único bus.



↑ Fig. 21 Trama básica de un mensaje bajo CAN

9. Redes industriales

CAN tiene varias maneras de detectar mensajes incorrectos:

- la secuencia de verificación de la trama (FCS) contiene el control por redundancia cíclica (CRC). El receptor comprueba el CRC de la trama y compara el resultado con la FCS. Si éstos no son iguales, entonces se dice que la trama tiene un error CRC;
- el receptor detecta errores en la estructura de la trama. Si la estructura de la trama es errónea, la trama tiene un error de formato;
- el receptor de una trama publica un bit de reconocimiento (ACK) dominante si recibe una trama libre de errores. Si el transmisor no recibe este bit, envía un error de reconocimiento;
- CAN utiliza la codificación sin retorno a cero (NRZ) con relleno de bits. Si el emisor tiene que transmitir 5 bits consecutivos del mismo tipo, inserta otro bit del tipo inverso. El relleno de bits permite al receptor sincronizarse con la cadena de bits. El receptor elimina el relleno de bits de la trama de datos. Si hay más de 5 bits consecutivos del mismo tipo, entonces el receptor detectará un error de relleno de bits.

Existen varios niveles de aplicación de los protocolos que se pueden utilizar con CAN, como por ejemplo DeviceNet y CANopen. CAN no define un nivel de aplicación de protocolo por sí mismo.

■ Presentación de CANopen

CANopen define una capa de aplicación y un perfil de comunicación basado en CAN.

□ CANopen define los siguientes objetos de comunicación (mensajes)

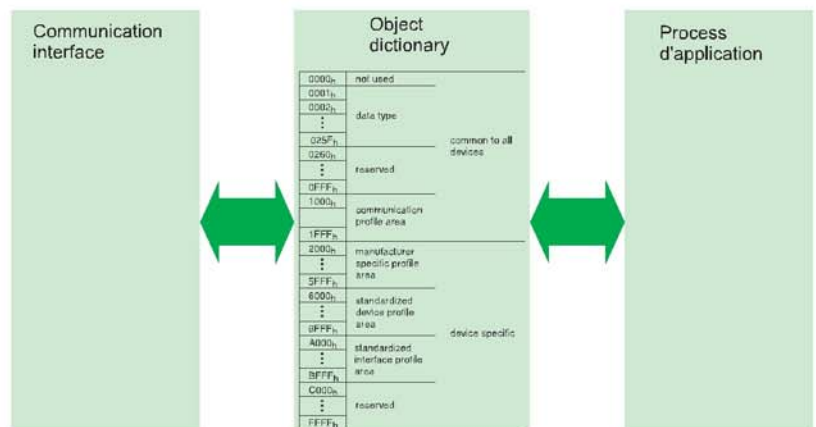
- objetos de datos de proceso (PDO);
- objetos de datos de servicio (SDO);
- objetos de gestión de red (NMT);
- objetos de función especial (SYNC, EMCY, TIME).

□ Propiedades

- transmisión de datos serie basada en CAN;
- hasta 1 Mbps;
- eficiencia aproximada 57%;
- hasta 127 nodos (dispositivos);
- varios maestros permitidos;
- interoperatividad de dispositivos de diferentes fabricantes.

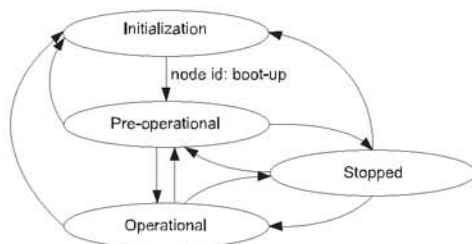
□ Diccionario de objetos

El diccionario de objetos (*≈ Fig. 22*) es un interface entre el programa de aplicación y el interface de comunicación.



↑ Fig. 22 Diccionario de objetos

9. Redes industriales



† Fig. 23 Objetos de gestión de red bajo CANopen

- **Objetos de datos de proceso (PDO)**

Los objetos de datos de proceso (PDO) son usados por su velocidad de transmisión de datos de proceso. Un PDO puede llevar hasta 8 bytes de datos útiles, el valor máximo para una trama CAN. La transmisión PDO usa el modelo CAN productor/consumidor extendido por transferencias sincronizadas. La transferencia sincronizada de PDO se basa en la transferencia de mensajes SYNC sobre el bus CAN. Se envía un PDO en método cíclico después de un número configurable (de 1 a 240) de mensajes SYNC recibidos. Es posible esperar la disponibilidad de las variables del proceso de aplicación y enviar un PDO después de la siguiente recepción de un mensaje SYNC. Esto se conoce como **transferencia sincronizada acíclica**.

- **Objetos de datos de servicio (SDO)**

Los objetos de datos de servicio (SDO) transmiten parámetros. Los SDO dan un acceso remoto al diccionario de objetos. No existe límite de longitud para un SDO. Si los datos útiles no se adaptan a la trama CAN, se dividen en varias tramas CAN. Cada SDO es reconocido.

La comunicación SDO utiliza el modo punto a punto, con un punto actuando como servidor y el resto como clientes.

- **Objetos de gestión de red (NMT)**

Los objetos de gestión de red (NMT) cambian o comprueban el estado de los dispositivos CANopen (⇒ Fig. 23). Un mensaje NMT tiene un identificador CAN 0, lo que proporciona a éste la máxima prioridad.

Un mensaje NMT siempre tiene 2 bytes de datos útiles en la trama CAN. El primer byte contiene el comando NMT codificado y el segundo byte el ID del nudo direccionado.

Un dispositivo CANopen empieza en el estado de inicialización cuando se presiona el botón de ON. Una vez el dispositivo ha completado su inicialización, proporciona un objeto NMT de arranque para notificar la maestro.

El protocolo de detección de colisiones para supervisar el estado del equipamiento se implementa con los objetos NMT.

- **Objetos de función especial (SYNC, EMCY, TIME)**

CANopen debe tener un productor SYNC para sincronizar las acciones de los nodos CANopen. El productor SYNC transmite periódicamente el objeto SYNC. Este objeto tiene el identificador 128. Ello puede conducir a un retraso provocado por la prioridad de este mensaje.

Un error interno en un dispositivo puede desencadenar un objeto de emergencia (EMCY). La respuesta de los clientes EMCY depende de la aplicación. La norma CANopen define varios códigos de emergencia. El objeto de emergencia se transmite en una única trama CAN de 8 bytes.

Una trama CAN con el ID CAN 256 y 6 bytes de datos útiles se puede usar para transmitir la hora a varios nodos CANopen.

El objeto de tiempo (TIME) contiene el valor de la fecha y la hora en un objeto de tipo "Time-Of-Day".

- **Sistemas de "perro guardián"**

CANopen tiene 2 métodos de supervisión del estado de los dispositivos. Uno es un gestor de red que, de forma regular, escanea cada dispositivo a intervalos configurados. Este método es conocido como "node guarding" y presenta el inconveniente de consumir mucho ancho de banda.

El otro método consiste en el envío regular de un mensaje por parte de cada dispositivo. Este método ahorra ancho de banda comparado con el anterior.

9. Redes industriales

• Longitud de la red y tasa de salida

La longitud está restringida por la tasa de salida debido al procedimiento de prioridad de bits ($\Rightarrow$ Fig. 24).

Salida (Kbps)	1000	800	500	250	125	50	20	10
Longitud máx. (m)	20	25	100	250	500	1000	2500	5000

↑ Fig. 24 Longitud de la red y tasa de salida

Dentro de la documentación sobre CANopen, la máxima longitud más común que se menciona para 1 Mbps es 40 m, calculada sin aislamiento eléctrico tal y como se usa en los dispositivos CANopen de Schneider Electric. Cuando se incluye este aislamiento, la mínima longitud de bus es 4 m para 1 Mbps. Sin embargo, la experiencia demuestra que, a la práctica, la longitud máxima ronda los 20 m.

Baud rate (kbps)	1000	800	500	250	125	50	20	10
L max. (m) (1)	0,3	3	5	5	5	60	150	300
Σ L max. (m) local star (2)	0,6	6	10	10	10	120	300	600
Interval min. (m) $0,6 \times \Sigma$ L local (3)	□	3,6	6	6	6	72	180	360
Σ L max. (m) on all bus (4)	1,5	15	30	60	120	300	750	1500

↑ Fig. 25 Límites de longitud en derivaciones

Deben tenerse en cuenta las limitaciones relativas a las derivaciones, establecidas por los parámetros de la figura 25.

- (1) L máx: longitud máxima de una derivación
- (2) EL máx. estrella local: valor máximo de la longitud acumulada de las derivaciones en un mismo punto cuando se utiliza una caja de derivación multipuerto para crear una topología de estrella local.
- (3) Intervalo min: distancia mínima entre dos cajas de derivación. Longitud máxima de las derivaciones en un mismo punto. Este valor se puede calcular de forma individual para cada derivación de la siguiente manera: el intervalo mínimo entre dos derivaciones es igual al 60% de la longitud acumulada de las derivaciones en un mismo punto.
- (4) EL máx (m) de todos los buses: valor máximo de la longitud acumulada del conjunto de los intervalos y derivaciones del bus.

9. Redes industriales

■ Combinaciones según las clases de conformidad

Schneider Electric tiene definidas unas clases de conformidad para dispositivos maestros y esclavos CANopen similar a la clasificación Ethernet Modbus TCP y los servicios web. Las clases de conformidad especifican qué sistemas puede soportar un dispositivo y aseguran la compatibilidad ascendente de las funcionalidades de cada clase (*⇒ Fig.26*).

Characteristics				
Conformance classes		M10	M20	M30
Layer settings	Slave ID	1-16	1-63	1-127
	Data rate	kbps 125, 250, 500	M10 + 50, 1000	M20 +10, 20, 800
	LSS	—		Master
Devices supported		16	63	126
NMT (Network Management object)	NMT Master	NMT Master, according to DS301		
	CANopen Manager	—		
	Boot-up procedure	according to DSP302		
	Time stamp	—		
	Auto configuration	—		
SDO (Service Data Object)	SDO Client	1	1	2
	SDO Server	—	1	1
	SDO Manager	—		
	SDO data transfer	Expedited, segment transfer		
		Expedited, segment block transfer		
PDO (Process Data Object)	COB-ID	ReadOnly	Read/Write	Read/Write
	PDO TT	254, 255	M10 +0, 1-240	
	PDO Inhibit Time	—	TPDO's (Read/Write)	
	PDO Event Timer	—	TPDO's (Read/Write)	RPDO's & TPDO's (Read/Write)
		—		
SYNC	SYNC	—	producer	producer/consumer
	TRIGGER	—		producer
EMCY		consumer	producer/consumer	
HEALTH	Heartbeat	16 consumers 1 producer	63 consumers 1 producer	126 consumers 1 producer
	Node guarding	no	yes	yes
Parameters	Store parameters	no	yes	yes
Conformance classes		S10	S20	S30
Layer settings	Slave ID	1-63	1-127	1-127
	Data rate	kbps 125, 250, 500	S10 + 50, 1000	S20 +10, 20, 800
	LSS	—		Slave
Diagnostic devices		—	LED or display	
NMT (Network Management object)	NMT slave	b Start remote node b Stop remote node b Enter pre-Operational b Reset node b Reset communication		
	Time stamp	—		
		—		
SDO (Service Data Object)	SDO Client	—		1
	SDO Server	1		2
	SDO data transfert	Expedited, segment transfer		
		Expedited, segment, block transfer		
PDO (Process Data Object)	COB-ID	ReadOnly	Read/Write	Read/Write
	PDO TT	254, 255	S10 +0, 1-240	
	PDO mapping parameters	FIX (Read)		—
	Connection set	Predefined connection set	Free	
	PDO Inhibit Time	—	TPDO's (Read/Write)	
	PDO Event Timer	—	TPDO's (Read/Write)	RPDO's & TPDO's (Read/Write)
		—		
SYNC	SYNC	—	consumer	producer/consumer
	TRIGGER	—		consumer
EMCY		producer	producer	consumer/producer
HEALTH	Heartbeat	1 consumer 1 producer		
	Node guarding	no	yes	yes
Parameters	Store parameters	no	no	no

Nota : S00 and M00 are for products not 100% compliant to the conformance class.

↑ Fig. 26

Cuadro de elección de las clases de conformidad

9. Redes industriales

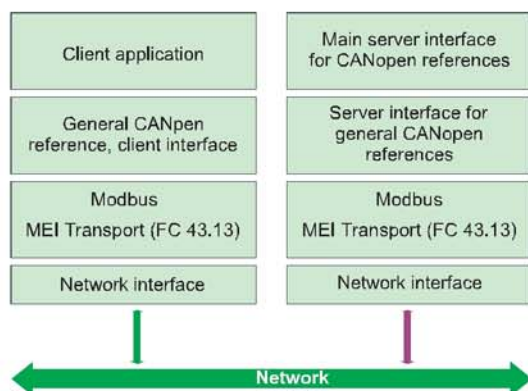
La [tabla 27](#) muestra las mejores combinaciones de producto posibles basadas en las clases de conformidad.

Clase de conformidad	S10	S20	S30
M10	Combinación posible	Restricción de uso	
M20			
M30			

↑ [Fig. 27](#) Clase de conformidad y las mejores combinaciones de producto

Sin embargo, es posible utilizar un dispositivo esclavo con un maestro de una clase de conformidad menor (como un S20 con un M10), o un maestro con un esclavo de clase de conformidad superior (como un M10 con un S20), empleando únicamente dispositivos soportados por la clase de conformidad más baja.

9.9 La sinergia de Ethernet y CANopen



↑ [Fig. 28](#) Sinergia Ethernet / CANopen

Un perfil común de comunicación (DS-301) define entre otras cosas la asignación de los identificadores COB-ID para cada tipo de mensaje.

Los perfiles específicos para cada familia de productos, como E/S digitales (DS-401), E/S analógicas, variadores de velocidad (DS-402) y encoders, describen los distintos objetos asociados.

CiA y Modbus-IDA han trabajado de forma conjunta para crear una norma para una transparencia completa entre CANopen y Ethernet Modbus TCP. El resultado de esta colaboración es la especificación CiA DSP309-2 que define las normas de comunicación entre una red Ethernet Modbus TCP y un bus CANopen. La especificación define los servicios de "mapping" que permiten a los dispositivos CANopen comunicarse en una red Ethernet Modbus TCP a través de una pasarela ([= Fig.28](#)).

Se puede acceder a la información de un dispositivo CANopen en lectura/escritura.

9.10 Bus AS-Interface (AS-I)

■ Descripción general

Actualmente, las máquinas incorporan infinidad de sensores y actuadores. Deben tenerse en cuenta la posibilidad de modernización, el mantenimiento y la seguridad. El AS-Interface es la red de nivel taller enfocada a la automatización industrial.

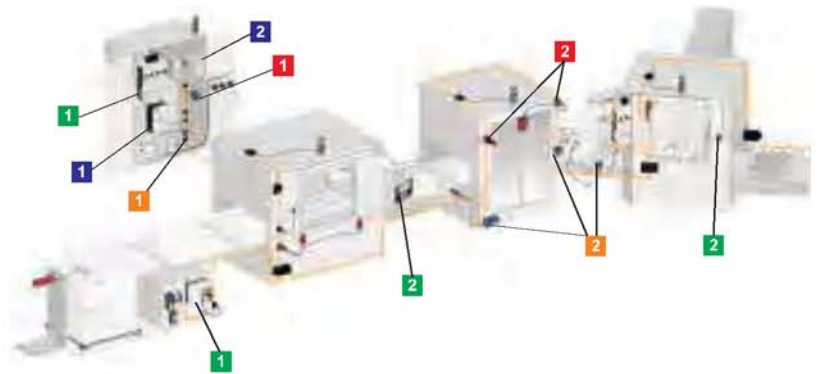
AS-Interface transporta señal y potencia en un único cable de dos hilos. Los componentes conectados a la red pueden ser fácilmente reemplazados para tareas de mantenimiento. El nuevo dispositivo recibe automáticamente la dirección del antiguo.

AS-Interface es una alternativa económica comparada con el cableado paralelo entre autómatas y sensores/actuadores.

Toda la gama Schneider Electric cumple con la norma AS-I tal y como la define la "AS-International Association". Es una tecnología "abierto" compatible con los productos de los fabricantes de automatismos líderes que garantiza la intercambiabilidad y la interoperatividad entre productos.

AS-Interface, como se muestra en la ([= Fig.29](#)), es un protocolo maduro que, durante más de 10 años, ha demostrado ser un sistema sencillo y fiable en un gran número de aplicaciones, incluyendo cintas transportadoras, control de procesos, plantas embotelladoras, sistemas de distribución eléctrica, carruseles de aeropuertos, ascensores y producción alimentaria.

9. Redes industriales



↑ Fig. 29 AS-Interface

- | | |
|-------------------------|--------------------------|
| 1 Interface IP20 | 1 Monitor de seguridad |
| 2 Interface IP67 | 2 Interface de seguridad |
| 1 Componente de control | 1 Alimentación |
| 2 Componente de diálogo | 2 Maestro AS-Interface |

AS-Interface se identifica con un cable amarillo (⇒ Fig.30) de una forma peculiar que imposibilita confundir sus dos hilos. Este cable "autocicatrizante" utiliza una toma de tipo "vampiro" que permite la conexión y el desplazamiento de sensores y actuadores sin la ayuda de herramientas.

AS-Interface es exclusivamente un bus de campo de tipo maestro/esclavo, siendo el maestro un PC, un autómata programable o un controlador que recibe información de sensores y controla los actuadores a través de la instalación. AS-Interface tiene otros beneficios como una topología libre que le permite funcionar en tecnología de red en estrella, punto a punto, línea, árbol o anillo.



↑ Fig. 30 Constituyentes del AS-Interface

Durante más de 10 años, AS-Interface fue sólo adecuado para E/S digitales. Algunos fabricantes disponían de dispositivos analógicos lentos como sensores de temperatura o sensores de nivel, pero en todos los casos eran productos propietarios y el número de direcciones (hasta 31) era una restricción importante.

El consorcio AS-Interface ha lanzado una nueva versión (V2). Con ella, el número de direcciones se ha doblado con posibilidad de hasta 62 E/S digitales por maestro. Pero el cambio más importante es la capacidad para conectar cualquier sensor o actuador analógico a cualquier maestro, a través de un AS-Interface. Además es posible mezclar dispositivos digitales y analógicos. Aunque el número de esclavos se verá reducido, se puede seguir gestionando el funcionamiento.

9. Redes industriales

Esta nueva versión introdujo cambios a nivel diagnóstico. La versión anterior sólo capaz de detectar fallos de la red. La versión V2 tiene en cuenta todos los fallos incluyendo defectos en los dispositivos.

Obviamente, el funcionamiento de V2 y V1 en una misma red es incompatible.

■ Ventajas de AS-Interface (≈ Fig.31)

Simplicidad	La simplicidad del sistema de cableado es debida a: • un único cable para conectar todos los actuadores y sensores de un automatismo; • gestión integrada de la comunicación.
Reducción de costes	Los costes se pueden reducir un 40% debido a: • tiempos de diseño, instalación, puesta en marcha y modernización reducidos; • ahorro de espacio gracias a los dispositivos más compactos y a la eliminación de elementos intermedios ya que hay funciones deslocalizadas; • eliminación canalizaciones de cables de control.
Seguridad	AS-Interface ayuda a incrementar la fiabilidad, la disponibilidad y la seguridad: • los errores de cableado son imposibles; • no hay riesgo de malas conexiones; • gran inmunidad a las interferencias electromagnéticas; • las funciones de seguridad de las máquinas se pueden integrar completamente en AS-Interface.

↑ Fig. 31

Ventajas de AS-Interface

9. Redes industriales

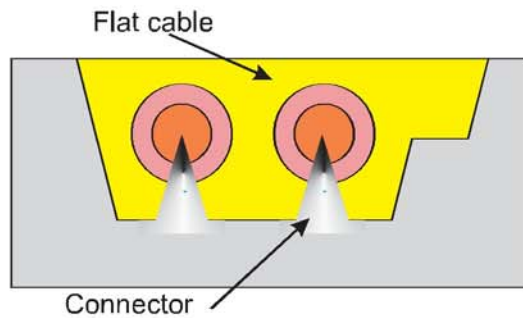
■ Los componentes de AS-Interface

Se agrupan en familias según la (⇒ Fig. 32). Para más información, por favor dirigirse a los catálogos de producto Schneider Electric.

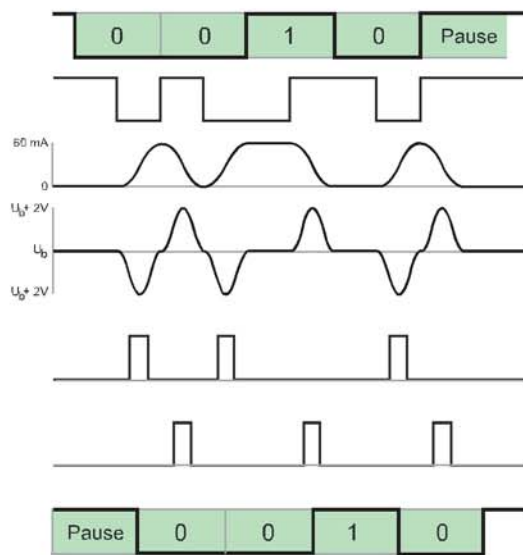
Interfaces para productos genéricos	Permiten que cualquier dispositivo estándar (sensor, actuador, arrancador, etc.) se conecte a AS-Interface. Ofrecen una gran libertad de elección y están especialmente adaptados a las modificaciones y mejoras de la máquina que anteriormente se realizaban con cableado convencional. Estos interfaces están disponibles para su montaje en armario (IP20) o directamente sobre la máquina (IP67).
Interfaces dedicados y componentes	Los interfaces dedicados (módulos de comunicación, etc.) se usan para comunicarse con el cable AS-Interface. Los componentes dedicados están integrados en un interface que se puede conectar directamente a un cable AS-Interface. Permiten un cableado rápido, pero la elección no es tan amplia como en el caso de los genéricos.
Maestro	Este es el componente central del sistema; su función es gestionar los intercambios de datos con los interfaces y componentes (también llamados esclavos) de la instalación. Puede soportar: - 31 interfaces o componentes en versión V1 (tiempo de ciclo 5 ms); - 62 interfaces o componentes en versión V2 (tiempo de ciclo 10 ms). El maestro está: - o bien integrado en un autómata programable, por ejemplo como una extensión, - o conectado al bus de campo, entonces se trata de una pasarela.
Alimentación de AS-Interface	Muy baja tensión de 29,5 a 31,6V para interfaces y componentes alimentados a través del cable AS-Interface. Está protegido contra sobretensiones y cortocircuitos. Este es el único tipo de alimentación que se puede usar en una línea AS-Interface. Dado que el cable AS-Interface tiene una corriente limitada, a menudo es necesario añadir una fuente suplementaria para algunos circuitos, en particular para los actuadores.
Cable plano	El cable amarillo conectado a la alimentación asegura dos funciones: - transmisión de información entre maestro y esclavos; - alimentación de sensores y actuadores. El cable negro conectado a la alimentación auxiliar a 24V suministra potencia a los actuadores y sensores con entradas aisladas. El perfil mecánico de estos cables imposibilita la inversión de polaridad; los materiales usados permiten una rápida y fiable conexión de los componentes. Cuando un dispositivo se desconecta, por ejemplo para alterarlo, el cable recupera su forma inicial por autocicatrizado. Estos cables soportan una corriente máxima de 8A y están disponibles en dos versiones: - en caucho para aplicaciones estándar; - en elastómero termoplástico (TPE) para aplicaciones donde el cable puede ser salpicado por aceite.
Soluciones de seguridad AS-Interface (ver capítulo seguridad)	La información estándar del proceso se puede transmitir al mismo tiempo y por los mismos medios que la información relativa a la seguridad hasta el nivel 4 del estándar EN 60954-1. La integración en AS-Interface se realiza añadiendo un monitor y componentes de seguridad conectados al cable AS-Interface. La información de seguridad sólo se intercambia entre el monitor de seguridad y sus componentes y es transparente para el resto de funciones estándar. Ello significa que un sistema de seguridad se puede añadir a una red AS-Interface existente.
Term. direccionamiento	Dado que los componentes están conectados en paralelo al bus AS-Interface, se debe asignar una dirección diferente a cada uno. Esta función se asegura por un terminal conectado individualmente a cada componente.

† Fig. 32 Los componentes de AS-Interface

9. Redes industriales



↑ Fig. 33 Principio de conexión AS-Interface



↑ Fig. 34 Forma de onda de tensión y corriente

■ Principio de funcionamiento de la red AS-Interface

□ Conexión

El sistema de conexión usado se denomina de forma común "toma vampiro". El conector tiene dos agujas que realizan la conexión eléctrica por perforación del aislante del cable. Las dos partes del conector son entonces atornilladas de forma conjunta para obtener una conexión fiable.

Este sistema (⇒ Fig. 33) está estandarizado y permite obtener hasta un grado IP67 en todo tipo de equipamiento.

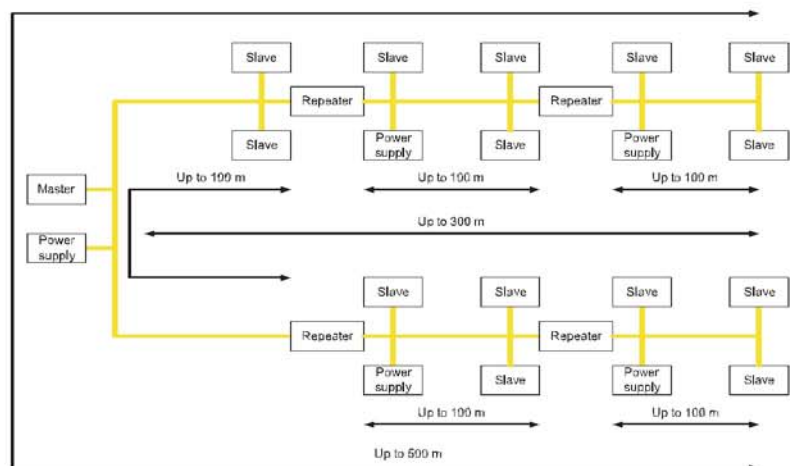
□ Modulación de señal

AS-Interface ha sido diseñado para funcionar sin un conector terminal en cualquier configuración. El principio de funcionamiento utiliza la modulación de corriente basándose en la codificación Manchester. Dos inductancias en la alimentación convierten esta corriente en una onda senoidal. La forma de la onda generada evita el uso de cables blindados (⇒ Fig. 34).

□ Longitud de red

La longitud está relacionada con la distorsión de la señal y la caída de tensión. La longitud máxima entre dos esclavos no debe exceder los 100 m (⇒ Fig. 35). Se puede incrementar esta distancia mediante el uso de repetidores con unos límites:

- no más de dos repetidores por línea,
- la distancia máxima al maestro no debe exceder los 300 m,
- un terminal pasivo extiende la distancia de 100 m a 200 m,
- un terminal activo extiende la distancia 300 m.

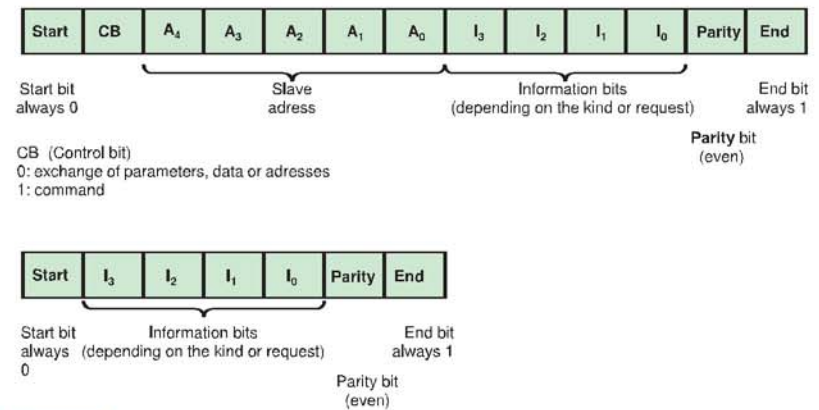


↑ Fig. 35 Longitudes límite de la red AS-Interface

9. Redes industriales

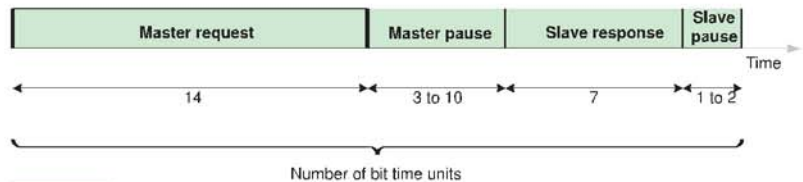
□ Principio del protocolo

El principio de comunicación se basa en un protocolo de un único maestro. El maestro envía una petición a los esclavos y éstos envían los datos requeridos (≈ Fig.36). Cuando todos los esclavos han enviado una respuesta, un nuevo ciclo empieza y así sucesivamente. El tiempo de ciclo se calcula fácilmente con el número de esclavos.



↑ Fig. 36 Trama maestro y trama esclavo

AS-Interface tiene varias maneras de garantizar la seguridad de la transferencia de datos. La señal es comprobada por el receptor; si ésta tiene la forma incorrecta, el mensaje es descartado. La utilización de un bit de paridad, asociado a un mensaje corto (7 y 14 bits), garantiza la integridad lógica de la información. El tiempo muerto del maestro provoca el reconocimiento (≈ fig.37).



↑ Fig. 37 Constitución del tiempo de respuesta

La duración de un bit es de 6 ms. A 166,67 Kbits/s, añadiendo el conjunto de los bites de pausa, el tiempo de ciclo no puede exceder los 5.082 μ s.

- Cada ciclo se divide en 3 partes
 - intercambio de datos,
 - gestión del sistema,
 - actualización/inserción de un esclavo.

El perfil AS-Interface del maestro determina su capacidad exacta. En general, tiene las siguientes funciones:

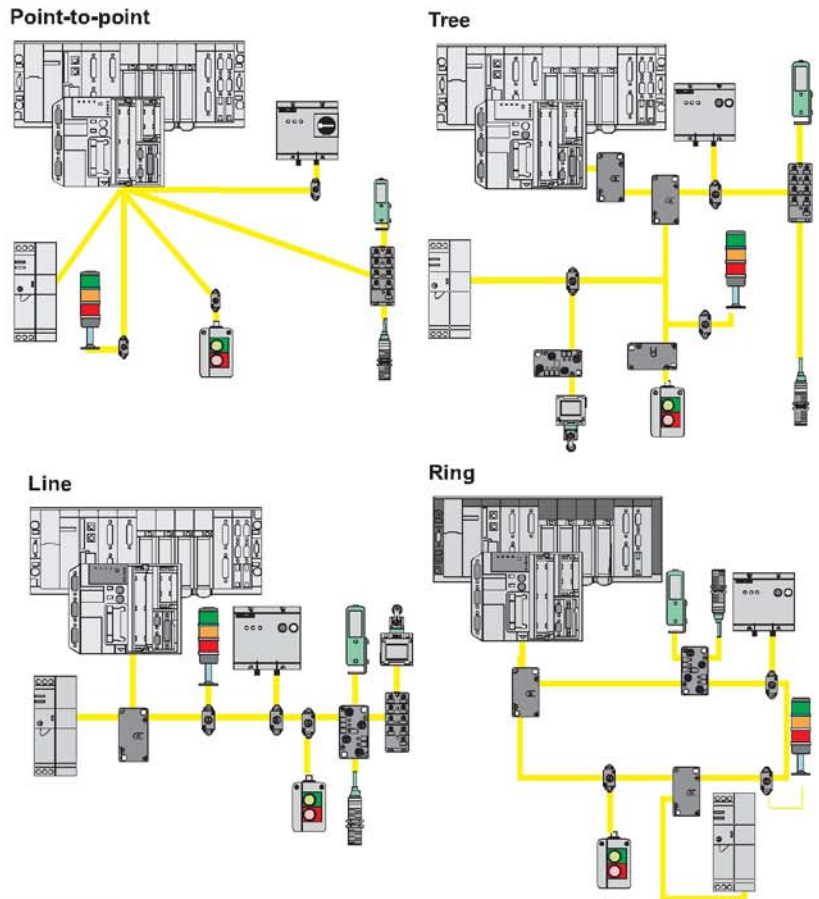
- inicializar el sistema,
- identificar los esclavos conectados,
- enviar los parámetros de los esclavos a éstos,
- comprobar la integridad de los intercambios de datos cíclicos con los esclavos,
- administrar los diagnósticos del sistema (estado de los esclavos, estado de la alimentación, etc.),
- transmitir todos los fallos detectados al supervisor del sistema (autómata, etc.),
- reconfigurar el sistema si éste sufre alguna modificación.

Los esclavos descifran las solicitudes procedentes del maestro y envían la respuesta sin retraso. Sin embargo, un esclavo no responderá a una solicitud incorrecta o inapropiada. La capacidad funcional de un esclavo está definida por su perfil AS-Interface.

9. Redes industriales

■ Topología y cableado de AS-Interface

La ausencia de restricciones permite todo tipo de configuraciones de red, algunas de las cuales se ilustran debajo ($\Rightarrow$ fig. 38).



↑ Fig. 38 Tipos de redes posibles

■ Versiones de AS-Interface

La primera versión (V1) ha sido sustituida por la V2.1 que contiene las siguientes mejoras:

- capacidad para conectar 62 esclavos (el límite de V1 es 31);
- capacidad para transmitir un mensaje de fallo de esclavo sin desconectar éste, que permanece comunicado cuando la continuidad del servicio es un asunto crítico;
- soporta esclavos analógicos.

■ Perfil AS-Interface

El perfil del equipamiento AS-Interface determina su capacidad. Dos dispositivos AS-Interface, fabricados por cualquier marca y con la misma función y perfil, funcionan de forma idéntica en la misma red. Además, son intercambiables en la red. El perfil se fija en origen en la electrónica del producto mediante dos o tres caracteres que no se pueden cambiar.

Actualmente, el consorcio AS-I tiene definidos más de 20 perfiles. Se describen más abajo.

9. Redes industriales

La *tabla 39* muestra la compatibilidad entre la V1 y la V2.1.

	Esclavo V1	Esclavo V2.1 con direcc. estándar	Esclavo V2.1 con direcc. extendido	Esclavo analógico
Maestro V1	Compatible	Compatible pero defectos esclavo no se indican	No compatible	No compatible
Maestro V2	Compatible	Compatible	Compatible	Compatible

† Fig. 39 Compatibilidad entre V1 y V2.1

□ Perfiles de maestro

Los perfiles maestro definen las capacidades individuales de cada maestro AS-I. Hay cuatro tipos de perfil: M1, M2, M3, M4, el último es compatible con las versiones anteriores.

□ Perfiles de esclavo

Todos los esclavos tienen un perfil, lo que significa que son vistos como dispositivos periféricos AS-Interface equipados con ASIC. Los productos dedicados (como los actuadores inteligentes) y los interfaces (que conectan dispositivos tradicionales a AS-Interface) están dentro de esta familia. Los perfiles, similares a tarjetas de identificación, se definieron para distinguir actuadores y sensores en grandes categorías. El sistema de perfiles es especialmente útil cuando se trata de sustituir un esclavo.

9.11 Conclusión

El uso de redes de comunicación en arquitecturas de automatización industrial incrementa su flexibilidad de tal manera que pueden cumplir los requerimientos para adaptar máquinas o plantas. Ello implica hacer decisiones que requieren de un conocimiento específico de las soluciones adecuadas entre una amplia gama de redes de comunicación. Deben utilizarse criterios simples: los productos deben ser abiertos, estandarizados y adecuados.

- Una red abierta, lo contrario a una red propietario, permite la libre elección del fabricante de dispositivos de automatización.
- Un red estandarizada internacionalmente garantiza su durabilidad y posibilidad de actualización o mejora.
- Una elección equilibrada entre los requerimientos de la máquina o de la planta y las prestaciones de la red es la manera de optimizar la inversión.

Este último punto es el que requiere, evidentemente, un conocimiento exacto de la oferta de redes de comunicación, que tradicionalmente se tenían como complicadas de seleccionar, implementar y mantener. Schneider Electric ha decidido enfocar su oferta en redes abiertas basadas en normas internacionales y adaptadas a los requerimientos de todos los niveles de las arquitecturas de automatización, definiendo clases de implementación para una elección simple y óptima.