



UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO

---

---

FACULTAD DE INGENIERÍA

“REDES INDUSTRIALES: ESTADO ACTUAL Y  
RECOMENDACIONES DE IMPLANTACIÓN”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:  
INGENIERO EN COMPUTACIÓN  
P R E S E N T A :  
SUSANA GARCÍA ORTEGA

ASESOR: ING. FRANCISCO J. RODRÍGUEZ R.





Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Esta tesis la dedico a mi mamá,

REMEDIOS ORTEGA QUINTOS

Por incentivarme a cumplir mis metas, por inculcarme los valores y principios que me han formado como ser humano, por su ejemplo de lucha y trabajo arduo, por estar a mi lado en las buenas y sobre todo en las malas y por lo más importante... su amor.

## AGRADECIMIENTOS

Al Ing. Francisco J. Rodríguez Ramírez por aconsejarme y asesorarme durante el desarrollo de este trabajo.

A la Universidad Nacional Autónoma de México, mi alma mater y en particular a la Facultad de Ingeniería por brindarme la oportunidad de ser uno de sus miembros.

A mi mamá Reme, por apoyarme, amarme y darme la oportunidad de ser quien soy ahora. A mi hermanito Chuy por ser quien me ha apoyado y querido sin hacer preguntas; a Clau, mi cuñada por ser parte de mi familia y por quererme, en especial a Tanisu por ser una bendición que Dios me ha dado.

A mis abuelitos, Rebeca y Carlos por su amor.

A mis tíos, Laura y Pepe por ser un ejemplo, por estar pendientes de mí todo el tiempo y por apoyarme en todas mis decisiones.

A mis suegros, Mary y Jorge por ser parte importante de mi familia, por su apoyo y amor, y sobre todo por tener un hijo maravilloso al que adoro con todo mí ser.

A mis otros hermanitos Marco, Jorge y Fabiola por estar a mi lado y por su apoyo.

A Nubia por su ayuda a corregir este trabajo y por su amistad al igual que a Tania, mis amigas de toda la vida a las que agradezco haber recorrido juntas un largo camino.

A mis queridos amigos Edo, Sofi, Rafa, Mario, Elda y a todos los que han formado parte de mí a lo largo de los años y que saben que ocupan un lugar en mi corazón.

Por último y no por eso menos importante, a mi querido esposo Raúl, quien ha compartido experiencias tanto buenas como malas, que me apoya y me quiere no importando cuantas veces me equivoque, MIL GRACIAS mi vida por todo tu apoyo, comprensión y sobre todo por tu amor.

A todos GRACIAS...

Susana García Ortega

<b>INTRODUCCIÓN</b>	<b>I</b>
<b>CAPÍTULO I. NECESIDADES DE CONTROL EN PLANTAS INDUSTRIALES</b>	<b>1</b>
I.1 INTRODUCCIÓN	1
I.2 NIVELES EN UNA RED INDUSTRIAL	3
I.3 REDES DE CONTROL Y REDES DE DATOS	4
I.4 CLASIFICACIÓN DE LAS REDES SEGÚN SU TAMAÑO Y EXTENSIÓN	7
I.5 CLASIFICACIÓN DE LAS REDES SEGÚN EL TIPO DE TRANSFERENCIA DE DATOS QUE SOPORTAN	7
I.6 EQUIPO DE CONECTIVIDAD	8
<b>CAPÍTULO II. EQUIPO DE CONTROL</b>	<b>9</b>
II.1 TRANSMISORES	9
II.2 CONTROLADORES	10
II.3 REGISTRADORES	11
II.4 EQUIPO DE CÓMPUTO	11
II.5 CONTROLADORES LÓGICOS PROGRAMABLES (PLC)	12
II.6 SISTEMAS DE CONTROL SUPERVISORIO Y ADQUISICIÓN DE DATOS (SCADA)	14
II.6.1 Necesidad de un Sistema SCADA .....	16
II.6.2 Funciones .....	17
II.7 SISTEMAS DE CONTROL DISTRIBUIDO (DCS)	17
<b>CAPÍTULO III. TOPOLOGÍAS DE RED</b>	<b>19</b>
III.1 MODELOS DE TOPOLOGÍA	19
III.1.1 BUS .....	20
III.1.2 ANILLO .....	20
III.1.3 ESTRELLA .....	21
III.1.4 ÁRBOL .....	21
III.1.5 MALLA .....	22
III.1.6 RED CELULAR .....	22
III.2 MODELO OSI	23
III.2.1 ANTECEDENTES .....	23
III.2.2 FAMILIA DE PROTOCOLOS DE INTERNET .....	27

<b>CAPÍTULO IV. BUSES DE CAMPO</b>	<b>29</b>
IV.1.1 VENTAJAS DE LOS BUSES DE CAMPO .....	29
IV.1.2 BUSES DE CAMPO EXISTENTES.....	30
<b>IV.2 REDES SENSOR - ACTUADOR. ASI</b>	<b>32</b>
<b>IV.3 INTERBUS</b>	<b>37</b>
<b>IV.4 CAN: CONTROLLER AREA NETWORK</b>	<b>39</b>
<b>IV.5 BITBUS: ESTRUCTURA FÍSICA Y PROTOCOLO</b>	<b>41</b>
IV.5.1 CABLEADO Y TERMINACIONES .....	42
IV.5.2 ESTRUCTURA.....	42
IV.5.3 TIPOS DE NODOS .....	43
IV.5.4 MODOS DE SINCRONIZACIÓN.....	44
IV.5.5 CODIFICACIÓN .....	44
IV.5.6 TRAMA DEL MENSAJE .....	45
<b>IV.6 PROFIBUS</b>	<b>50</b>
IV.6.1 PROFIBUS-DP.....	50
IV.6.2 PROFIBUS-PA.....	50
IV.6.3 PROFIBUS-FMS .....	51
IV.6.4 ESTRUCTURA BÁSICA .....	51
IV.6.5 ARQUITECTURA DE PROTOCOLOS.....	52
IV.6.6 CONTROL DE ACCESO AL MEDIO EN PROFIBUS.....	52
<b>CAPÍTULO V. PROTOCOLOS</b>	<b>54</b>
<b>V.1 MODBUS</b>	<b>54</b>
V.1.1 ESTRUCTURA DE LA RED .....	54
V.1.1.1 MEDIO FÍSICO	54
V.1.1.2 ACCESO AL MEDIO	55
V.1.2 PROTOCOLO .....	55
V.1.3 TRANSACCIONES SOBRE REDES MODBUS.....	56
V.1.4 MODOS DE TRANSMISIÓN EN SERIE .....	57
V.1.4.1 MODO ASCII	57
V.1.4.2 MODO RTU	58
V.1.5 TRAMA DEL MENSAJE MODBUS .....	58
V.1.5.1 TRAMA ASCII	59
V.1.5.2 TRAMA RTU	59
V.1.6 VARIANTES DE MODBUS: JBUS.....	62
V.1.7 COMPARACIÓN ENTRE JBUS Y MODBUS .....	62
<b>V.2 CAN (CONTROLLER AREA NETWORK)</b>	<b>63</b>
V.2.1 FRAMES .....	64
V.2.1.1 Frame de Datos	64
V.2.1.2 Frame Remoto	64
V.2.1.3 Frame de Error	64
V.2.1.4 Frame de Sobrecarga	65
V.2.2 MECANISMOS DE DETECCIÓN DE ERRORES.....	66
V.2.2.1 <i>Bit Monitoring</i>	66
V.2.2.2 <i>Bit Stuffing</i>	67
V.2.2.3 <i>Frame Check</i>	67

V.2.2.4	<i>Acknowledge Check</i>	67
V.2.2.5	<i>CRC (Cyclic Redundancy Check)</i>	67
<b>V.3</b>	<b>ETHERNET</b>	<b>68</b>
V.3.1	TECNOLOGÍA ETHERNET .....	69
V.3.2	FORMATO DE TRAMA ETHERNET .....	72
V.3.3	ARQUITECTURA (ESTRUCTURA LÓGICA) .....	73
<b>V.4</b>	<b>DNP3 (DISTRIBUTED NETWORK PROTOCOL)</b>	<b>74</b>
V.4.1	CARACTERÍSTICAS.....	75
V.4.2	ARQUITECTURA.....	77
V.4.2.1	Uno a uno	78
V.4.2.2	Diseño Multidrop	78
V.4.2.3	Jerárquico	78
V.4.2.4	Concentrador de datos	79
V.4.3	LA TRAMA DNP3 .....	79
V.4.4	BENEFICIOS.....	83
<b>CAPÍTULO VI.</b>	<b>NORMAS</b>	<b>85</b>
<b>CAPÍTULO VII.</b>	<b>RECOMENDACIONES DE IMPLANTACIÓN</b>	<b>90</b>
VII.1.1	REQUISITOS DE LAS APLICACIONES A MODELAR .....	91
VII.1.2	METODOLOGÍA DE MODELADO .....	91
VII.1.3	ESPECIFICACIÓN FUNCIONAL .....	93
VII.1.4	IMPLANTACIÓN DE LOS SISTEMAS DISTRIBUIDOS DE CONTROL INDUSTRIAL .....	94
<b>CONCLUSIONES</b>		<b>96</b>
<b>BIBLIOGRAFÍA</b>		<b>99</b>

## INTRODUCCIÓN

El presente trabajo de tesis busca presentar una descripción formal sobre las redes industriales, sus principales diferencias con respecto a las redes convencionales o de oficina, los componentes que las describen y con los que interactúan, los buses y protocolos que pueden utilizar para el intercambio de información; para que se entiendan los fundamentos y requisitos para conformar una red industrial.

Así pues, en el capítulo uno se aborda las necesidades de control existentes en una planta industrial, para entender las formas de comunicación en cada nivel y entre ellos en la planta. Además, se describen los tipos de redes que podemos encontrar, su clasificación (según su tamaño y extensión) y el equipo de conectividad asociado a éstas.

Continuando con esta idea, el capítulo dos presenta una breve descripción del equipo de control que está asociado a las redes industriales entre los que se encuentran los transmisores, los controladores, el equipo de cómputo y los sistemas de adquisición de datos, por mencionar algunos.

Por otro lado, y debido a que los elementos de control son independientes del arreglo (disposición o topología) de la red, en el capítulo tres se detalla la topología que puede adoptar, así como los modelos existentes y algunas de sus características principales. También se define el modelo OSI de comunicación y el protocolo TCP/IP para el intercambio de información vía Internet.

Posteriormente en el capítulo cuatro se analizan los buses de campo, detallando qué son y cuáles son sus ventajas; de igual forma los buses de campo existentes, en particular de su funcionamiento y las características más relevantes.

Ahora bien, dado a que a la forma de intercambiar información durante la comunicación, entre las entidades que conforman una red, se le denomina protocolo, en el capítulo cinco se describen algunos de éstos, los más utilizados.

A lo largo del capítulo seis se exponen las normas o estándares que existen para proporcionar los fundamentos para la transmisión de datos, para la fabricación de equipos y para el diseño de sistemas operativos que se utilizan en una red. También, se mencionan algunas de las principales organizaciones que realizan dichos estándares.



Finalmente, en el capítulo siete se presentan algunas apreciaciones en cuanto a los requisitos de las aplicaciones a modelar, la metodología del modelado y la implantación de los sistemas distribuidos de control industrial para la conformación de las redes industriales, en este punto es conveniente destacar que algunas de las características al respecto son de tipo comercial e incluso económicas, por encima de las técnicas.

De este modo con la información presentada se está en condiciones para establecer un conjunto de conclusiones y recomendaciones sobre el uso e implantación de las redes industriales.

## Capítulo I. NECESIDADES DE CONTROL EN PLANTAS INDUSTRIALES

### I.1 INTRODUCCIÓN

Los sistemas o redes de comunicación empleados en ambientes industriales se encuentran sometidos a una problemática específica que condiciona enormemente su diseño y los diferencia de las redes tradicionales de datos.

Históricamente, hacia los años 70 se comenzaron a introducir las computadoras en el control de procesos, fundamentalmente para realizar tareas de vigilancia. La computadora se encargaba de supervisar las variables controladas para detectar niveles anómalos, generando entonces las señales de alarma pertinentes y los informes sobre el estado del sistema. Posteriormente, se comenzó a incluir también en las labores de control, ya que debido a su capacidad de cálculo podía sustituir al panel de control y tener programados los bucles de control; el principal inconveniente que se planteaba era la mayor debilidad del sistema al existir un punto de fallo crítico, en el propio ordenador; una posible solución consistió en duplicar el equipo, disponiendo de un ordenador de respaldo, comunicado con el primero y capaz de seguir con el control del proceso en caso de fallo.

El desarrollo de los microprocesadores, microcontroladores y los controladores lógicos programables (PLCs) dio lugar a la aparición del control distribuido. En este tipo de esquema, un PLC o un microprocesador controla una o más variables del sistema realizando un control directo de las mismas. Estos equipos de control local se comunican con otros elementos de su nivel y con el nivel superior de supervisión, por lo que el fallo de un elemento del nivel superior no compromete necesariamente el funcionamiento de los equipos de control local, minimizando su incidencia en el sistema.

De este modo, con la aparición de sensores inteligentes y elementos programables (máquinas de control numérico, PLCs, robots, etcétera), que favorecen la automatización y flexibilizan el proceso productivo, se demanda la necesidad de permitir su programación y control en forma remota.

Por otro lado, desde el punto de vista empresarial, la necesidad de comunicación no se restringe sólo a la producción, ya que otros departamentos de la empresa también pueden participar en la red de comunicaciones para permitir un control global del sistema y de este modo, no sólo se controlaría el propio funcionamiento de la planta de fabricación, sino que en función de las decisiones tomadas en las capas administrativas de la empresa podría actuarse directamente sobre la producción, así se puede establecer un sistema de **control jerarquizado**<sup>1</sup> como se representa a continuación.

---

<sup>1</sup> Sirgo J.A. y González Rafael. *Redes Locales en entornos Industriales. Buses de Campo*. Tema 9. Universidad de Oviedo, Departamento de Eléctrica, Electrónica, de Computadores y de Sistemas. 2003. página 1.

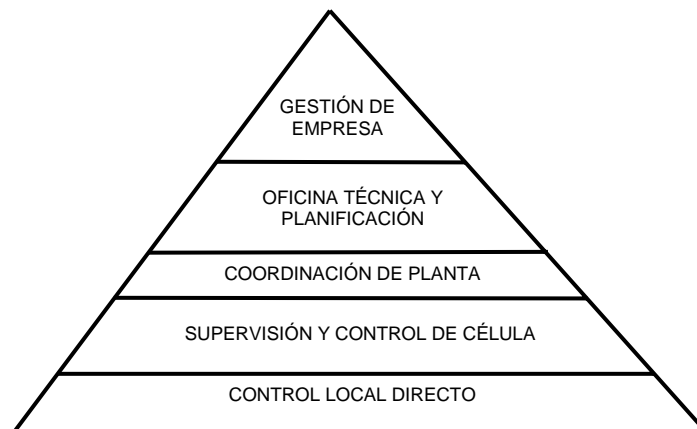


Fig. 1: Niveles jerárquicos en la automatización industrial

Cada uno de los niveles, además de llevar a cabo labores específicas, realiza un tratamiento de filtrado de la información que es transmitida en sentido ascendente o descendente por la pirámide. Así, se limitan los flujos de información a los estrictamente necesarios para cada nivel. También existe un tráfico en sentido horizontal dentro de cada nivel, con distintas condiciones en cada uno de ellos.

El nivel inferior realiza el **control local directo** de las variables del sistema o el control de los elementos de fabricación. Se adquieren datos de los sensores 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.

El siguiente nivel es el de **supervisión** al nivel de célula de fabricación o de control. Elabora la información procedente del nivel inferior y se notifica al operario de la situación de las variables y de las alarmas. Corrige algoritmos de control, consignas y programas.

El tercer nivel lleva a cabo labores de **coordinación de planta**, controla y organiza toda el área de producción tratando de optimizar balances de materiales y energía (flujos de 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 éstos adapten y distribuyan entre los controles directos.

En el siguiente nivel se realiza la **planificación** de la producción del conjunto de la fábrica. Se encuentran en él también los elementos de oficina técnica que mediante herramientas CAD/CAM/CAE (*Computer Aided Design/ Computer Aided Manufacturing/ Computer Aided Engineering*, todas estas herramientas de diseño asistido por computadora) permiten el diseño de productos y la elaboración automática de programas para los elementos de fabricación.

En el nivel superior se establece la **política de la producción** del conjunto de la empresa en función de los recursos y costes del mercado. En él se incluyen labores de contabilidad y gestión empresarial.

## I.2 NIVELES EN UNA RED INDUSTRIAL

En una red industrial coexistirán equipos y dispositivos de todo tipo, los cuales suelen agruparse jerárquicamente para establecer conexiones lo más adecuadas a cada área. De esta forma se definen cuatro niveles (Fig. 2) dentro de una red industrial:

- **Nivel de gestión:** es el nivel más elevado y se encarga de integrar los niveles siguientes en una estructura de fábrica, e incluso de múltiples fábricas. Las máquinas aquí conectadas suelen ser estaciones de trabajo que hacen de puente entre el proceso productivo y el área de gestión, en el cual se supervisan las ventas, *stocks*, etcétera. Se emplea una red de tipo LAN (*Local Area Network*) o WAN (*Wide Area Network*)
- **Nivel de control:** se encarga de enlazar y dirigir las distintas zonas de trabajo. A este nivel se sitúan los autómatas de gama alta y los ordenadores dedicados a diseño, control de calidad, programación, etcétera. Se suele emplear una red de tipo LAN.
- **Nivel de campo y proceso:** se encarga de la integración de pequeños automatismos (autómatas compactos, multiplexores de E/S, controladores PID, etcétera) dentro de sub-redes o "islas". En el nivel más alto de estas redes se suelen encontrar uno o varios autómatas modulares, actuando como maestros de la red o maestros flotantes. En este nivel se emplean los buses de campo.
- **Nivel de E/S:** es el nivel más próximo al proceso. Aquí están los sensores y actuadores, encargados de manejar el proceso productivo.

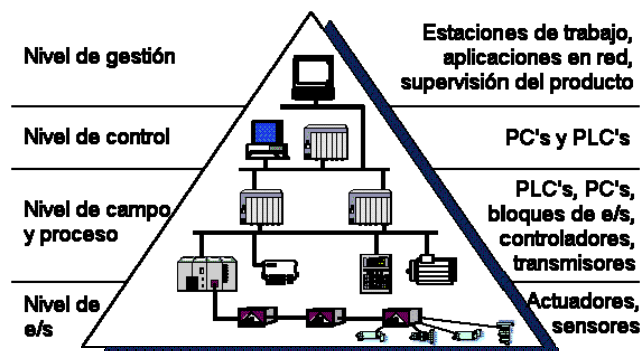


Fig. 2: Niveles de una red industrial

Esta estructura citada no es universal, habrá casos en los que conste de un número mayor o menor de niveles, dependiendo del tamaño del proceso y la propia industria.

### I.3 REDES DE CONTROL Y REDES DE DATOS

Podemos hablar de dos tipos de redes: **redes de control** y **redes de datos**<sup>2</sup>. Las redes de control están ligadas al control local directo y a la supervisión, mientras que las redes de datos están más ligadas a la parte administrativa.

En general, las **redes de datos** están orientadas al transporte de grandes paquetes de datos, que aparecen en forma esporádica (bajo carga), y con un gran ancho de banda para permitir el envío rápido de una gran cantidad de datos, en contraste, las **redes de control** se enfrentan a un tráfico formado por un gran número de pequeños paquetes, intercambiados con frecuencia entre un alto número de estaciones que forman la red y que muchas veces trabajan en tiempo real.

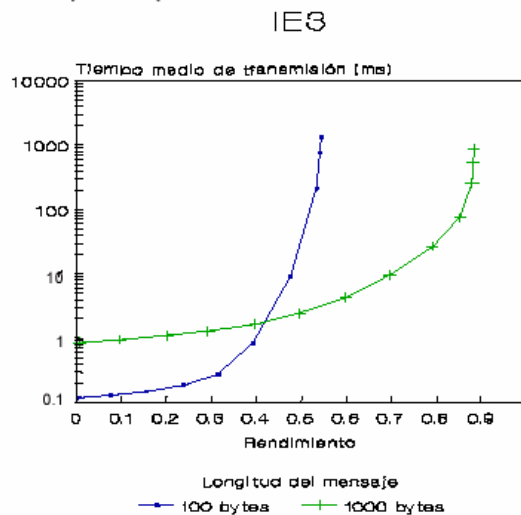


Fig. 3: Comportamiento de la red Ethernet ante variaciones del tamaño de los paquetes.

En principio, las redes de datos podrían emplearse para su uso como redes de control; sin embargo, es evidente que no resultarían adecuadas para las necesidades de este tipo de aplicaciones. Por ejemplo, la red Ethernet tiene una gran eficiencia hasta del 90-95% de la capacidad del canal cuando los mensajes son largos y suficientemente espaciados; sin embargo, la cantidad de información que una red Ethernet es capaz de soportar cae bruscamente cuando se utiliza por encima del 35% de la capacidad del canal, si el mensaje es pequeño (Fig. 3). En las redes de control es habitual encontrar este tipo de carga, porque el tráfico depende directamente de eventos externos que están siendo controlados (o monitorizados) por los diferentes nodos que la componen. A menudo varios nodos necesitan enviar información simultáneamente en función de uno o más eventos externos.

<sup>2</sup> *Ibidem.* p. 3.

Por las razones anteriores es necesario diseñar una arquitectura de red adaptada a las características particulares del tipo de este tipo de tráfico. En el diseño se deberán tener en cuenta aspectos como los tipos de protocolos utilizados, la interoperabilidad, la topología y la facilidad de administración.

Pueden distinguirse 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 con la que un nodo controla el funcionamiento de otro, la principal problemática radica en que si se dispone de un amplio conjunto de tipos de nodos, habrá un aumento exponencial del número de posibles comandos y de la sobrecarga que supone su procesamiento<sup>3</sup>. En las redes orientadas a estado las cosas son más sencillas. En este caso, la funcionalidad de un nodo no depende de ningún otro. Cada nodo enviará mensajes en los que indicará a los demás el estado en que se encuentra, los nodos que reciban estos mensajes modificarán su estado en función de la nueva información.

Por lo que se refiere al tipo de topología que deben adoptar las redes de control, cabe destacar que cualquiera de las topologías clásicas de las redes de datos es válida, las cuales se describirán más adelante. Cualquiera puede satisfacer las necesidades de cableado, prestaciones y costo de alguna aplicación. La elección está determinada fundamentalmente por el control de acceso al medio y el tipo de medio que se emplea, el conjunto formado por el medio, el control de acceso y la topología afectará prácticamente a cualquier otro aspecto de la red, como el costo, la facilidad de instalación, la fiabilidad, las prestaciones, el mantenimiento o la expansión.

Elegida una topología, hay que definir como accederá cada nodo a la red, el objetivo principal es reducir las colisiones (idealmente eliminarlas) entre los paquetes de datos y reducir el tiempo que tarda un nodo en ganar el acceso al medio y comenzar a transmitir el paquete; en otras palabras, maximizar la eficiencia de la red y reducir el retardo de acceso al medio. Este último parámetro es primordial a la hora de determinar si una red sirve para aplicaciones en tiempo real o no.

El direccionamiento de los nodos también es un aspecto clave en una red de control, ya que la información puede ser originada y/o recibida por cualquier

---

<sup>3</sup> *Ibidem.* p. 4.

nodo. La forma en que se direccionen los paquetes de información afectará de forma importante a la eficiencia y la fiabilidad global de la red. Se distinguen tres tipos de direccionamiento:

- a) *Unicast*: el paquete es enviado a un único nodo de 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.

La ventaja principal del direccionamiento **broadcast** es la sencillez y que es sumamente adecuado para proporcionar informaciones de estado, pero el inconveniente que se presenta es que los nodos pueden procesar paquetes que no les afecten directamente.

#### I.4 CLASIFICACIÓN DE LAS REDES SEGÚN SU TAMAÑO Y EXTENSIÓN

Las posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

**Redes LAN.** Las Redes de Área Local (*Local Area Network*) son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Las velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).

**Redes MAN.** Las Redes de Área Metropolitana (*Metropolitan Area Network*) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.

**Redes WAN.** Las Redes de Área Amplia (*Wide Area Network*) tienen un tamaño superior a una MAN, y consisten en una colección de host o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un *router* a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros.

#### I.5 CLASIFICACIÓN DE LAS REDES SEGÚN EL TIPO DE TRANSFERENCIA DE DATOS QUE SOPORTAN

**Redes de transmisión Simple.** Son aquellas redes en las que los datos sólo pueden viajar en un sentido.

**Redes Half-Duplex.** Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.

**Redes Full-Duplex.** Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

## I.6 EQUIPO DE CONECTIVIDAD

Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor.

**Hubs o concentradores:** Un concentrador es un dispositivo que permite centralizar el cableado de una red. Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella.

**Repetidores:** Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.

**Puentes:** Un puente es un dispositivo que conecta subredes separadas para crear lo que aparenta ser una sola.

**Ruteadores:** Los ruteadores son dispositivos hardware de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP).

**Compuertas:** Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos.



## Capítulo II. EQUIPO DE CONTROL

Dentro del equipo de control se describirán los siguientes elementos:

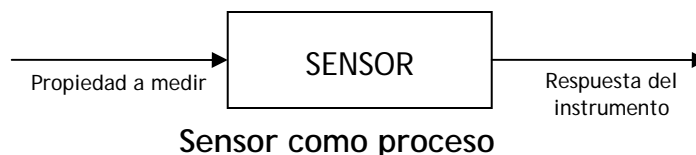
- Transmisores
- Controladores
- Registradores
- Equipo de cómputo
- Controladores Lógicos Programables
- Sistemas SCADA (*Supervisory Control And Data Acquisition*)
- Sistemas de Control Distribuido

### II.1 TRANSMISORES

El conocimiento sobre la marcha del proceso se obtiene a través de dispositivos especiales llamados sensores. El dispositivo crea una interacción con el objeto de medición con intercambio de masa o energía, así se genera una señal conocida como señal primaria la cual es transformada en una señal secundaria que puede ser enviada a distancia (transmisión) La señal transmitida está normalizada y tiene la potencia necesaria para ser inmune a los ruidos anexos a toda transferencia de información. Muchas veces los fabricantes incluyen en un solo instrumento el sensor y el transmisor de manera que es difícil saber sus diferencias, en general, se conocen como un mismo elemento. A continuación se tiene una definición de transmisor:

Un **transmisor** es un transductor que responde a una variable medida, esta variable va de acuerdo al elemento controlado convirtiéndolo en una señal de transmisión estandarizada que es función sólo de la variable medida.

El sensor obedece los principios de conservación al igual que los procesos y, por lo tanto, puede considerarse como un subsistema. La entrada a este subsistema será la variable a medir y la salida será la respuesta que genera la entrada; esta respuesta será la señal a determinar.<sup>4</sup>



---

<sup>4</sup> *Apud.* Solar Iván, Pérez Ricardo. *Control Automático de Procesos Químicos*. Ediciones Universidad Católica de Chile, 1993, Capítulo 3.

Un **transductor** es un dispositivo capaz de transformar o convertir un determinado tipo de energía de entrada, en otra diferente de salida. El nombre del transductor ya nos indica cual es la transformación que realiza, aunque no necesariamente la dirección de la misma. Es un dispositivo usado principalmente en las ciencias eléctricas para obtener la información de entornos físicos y conseguir (a partir de esta información) señales o impulsos eléctricos o viceversa.

## II.2 CONTROLADORES

Se define a los controladores, como aquellos instrumentos para medir, registrar y/o controlar variables de proceso (como temperatura, presión, caudal, etcétera) y dispositivos auxiliares, como sensores, transductores y válvulas de control.

En los Sistemas Automáticos (SA) de control de lazo cerrado la medición y el control de las variables se efectúan dentro de un rango continuo de valores, lo cual es esencial para regular la operación del proceso, de acuerdo con el diagrama clásico mostrado en la Figura 4.

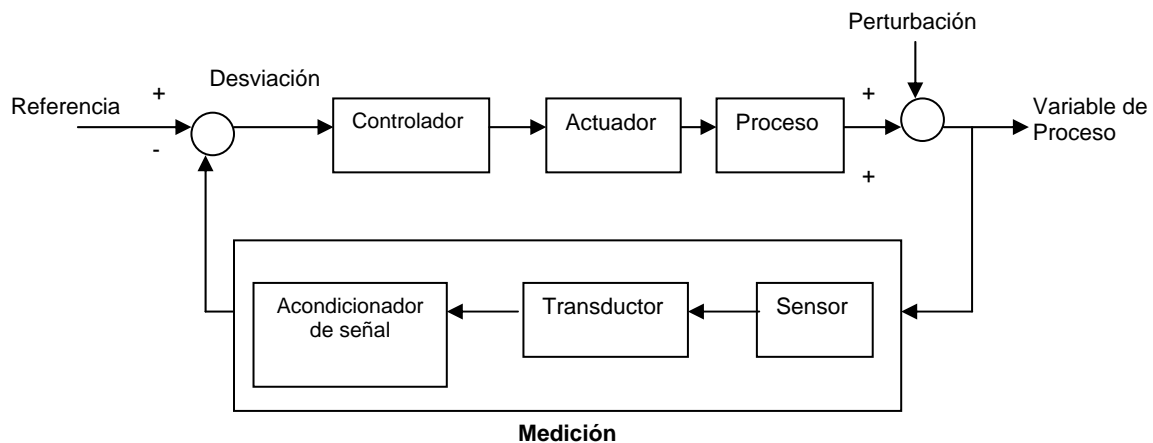


Fig. 4. SA de Lazo Cerrado Típico.

Esta forma de control es conocida en el ámbito industrial como control de lazo cerrado o control PID, debido a que el algoritmo de ese nombre es el que con mayor frecuencia se emplea y con mayor eficiencia. Es muy importante considerar que la medición y las funciones de actuación se efectúan dentro de un rango continuo de valores, lo que hace posible mantener el control de la variable de proceso en un rango especificado, de acuerdo con el valor de referencia, aún en presencia de perturbaciones.<sup>5</sup>

<sup>5</sup> *Apud.* Garibay Jiménez Ricardo. *Especialización en Mantenimiento a Equipo de Instrumentación y Control en Plataformas Marinas*. Unidad 1. paginas 7-9.

### II.3 REGISTRADORES

Los conceptos del registro de información medida han sido abordados en las pasadas décadas hasta el punto en que las gráficas en papel, en tira o en círculo constituyeron la gran mayoría de los instrumentos de registro. De hecho el término registro ha extendido su definición para incluir funciones que van más allá de la preservación histórica de los datos medidos, así un **registrador** es un instrumento de registro electrónico que monitorea y reporta los diversos cambios en las condiciones del medio ambiente en el tiempo.

Los instrumentos de registro, alguna vez interpretados como simples gráficas de datos medidos contra el tiempo, incluyen técnicas más sofisticadas de almacenaje electrónico de la información como cintas magnéticas, tarjetas perforadas y tarjetas plásticas magnéticas.

### II.4 EQUIPO DE CÓMPUTO

Una **computadora**, conocida en algunos países como ordenador y en otros países como computador, es un sistema digital con tecnología microelectrónica capaz de procesar datos a partir de un grupo de instrucciones denominado programa. La estructura básica de una computadora incluye microprocesador (CPU), memoria y dispositivos de entrada/salida (E/S), junto a los buses que permiten la comunicación entre ellos. En resumen la computadora es una dualidad entre hardware (parte física) y software (parte lógica), que interactúan entre sí para una determinada función.

La característica principal que la distingue de otros dispositivos similares, como una calculadora no programable, es que puede realizar tareas muy diversas cargando distintos programas en la memoria para que los ejecute el procesador.<sup>6</sup>

La característica principal que distingue una computadora de otros dispositivos similares, como una calculadora no programable, es que puede realizar tareas muy diversas cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Todos los sistemas digitales están hechos de una combinación de *hardware* y *software*. El *hardware* se refiere a las partes físicas del sistema digital, tales

---

<sup>6</sup>[http://es.wikipedia.org/wiki/Computadora#Evoluci.C3.B3n\\_del\\_t.C3.A9rmino\\_computadora](http://es.wikipedia.org/wiki/Computadora#Evoluci.C3.B3n_del_t.C3.A9rmino_computadora).  
Junio 9, 2006.

como microprocesadores, circuitos de conversión analógica-digital, cables, unidades de video (VDU), fuentes de poder, entre otros. Por otra parte, el *software* se refiere a la porción del sistema digital que existe como datos binarios y es ejecutado o utilizado por el microprocesador. El *software* utilizado por el microprocesador existe en varias capas funcionales, la primera capa del *software* permite al microprocesador el acceso y el control de otras piezas de *hardware* a su alrededor como la memoria RAM, monitores de video y teclados; en este nivel el *software* es conocido como sistema operativo.

El siguiente nivel del *software* es usado para la configuración y ejecución del control lógico y las funciones de adquisición de datos, en este nivel los módulos del *software* sirven para diferentes funciones que permiten al usuario la configuración de las aplicaciones. Por ejemplo, un módulo puede permitir la configuración de las entradas y salidas (I/O) del sistema, mientras que otro proporciona al usuario las herramientas para configurar la interfaz gráfica.

Es importante evaluar tanto el *hardware* como el *software* en un sistema digital para así poder determinar si están presentes en dicho sistema las herramientas necesarias para poder implementar de forma segura, efectiva y eficiente las aplicaciones.

## II.5 CONTROLADORES LÓGICOS PROGRAMABLES (PLC)

Los Sistemas Automáticos (SA) aplicados al control binario, también llamado lógico y de secuencias, se caracterizan por manejar variables de tipo binario, en lo que corresponde a la adquisición de datos del estado del proceso, como por las acciones de control que se realizan por medio de actuadores binarios, que habilitan o deshabilitan una acción correctiva o de seguridad. En la Figura 5 se presenta el esquema fundamental de este tipo de SA.

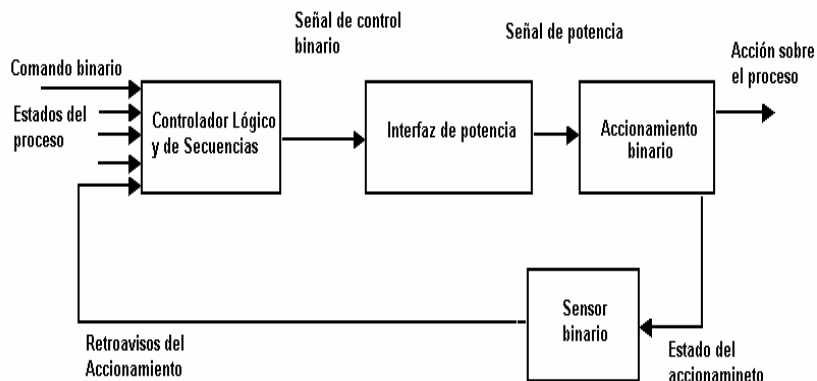


Fig. 5. Sistema Automático de Control Lógico

Los SA de control binario más representativos en aplicaciones industriales son los controladores lógicos programables (PLC's). Por su naturaleza, estos SA son los que predominan en aplicaciones de seguridad, ya que son de acción rápida y porque lleva el proceso o equipo a un estado seguro.

Un Autómata Programable Industrial (API) o *Programable Logic Controller* (PLC), es un equipo electrónico, programable en lenguaje no informático, diseñado para controlar en tiempo real y en ambiente de tipo industrial, procesos secuenciales.

Un PLC trabaja con base a la información recibida por los captadores y el programa lógico interno, actuando sobre los accionadores de la instalación.

Un PLC es una combinación de *software* y *hardware* usado para controlar. Este control se realiza sobre la base de una lógica definida a través de un programa.

El PLC por sus especiales características de diseño tiene un campo de aplicación muy extenso. La constante evolución del *hardware* y *software* amplía constantemente este campo para poder satisfacer las necesidades que se detectan en el espectro de sus posibilidades reales.

Su utilización se da fundamentalmente en aquellas instalaciones en donde es necesario un proceso de maniobra, control, señalización, entre otros; por tanto, su aplicación abarca desde procesos de fabricación industriales de cualquier tipo a transformaciones industriales, control de instalaciones, etcétera.

Sus reducidas dimensiones, la extremada facilidad de su montaje, la posibilidad de almacenar los programas para su posterior y rápida utilización, la modificación o alteración de los mismos, hace que su eficacia se aprecie fundamentalmente en procesos en que se producen necesidades tales como:

- ✓ Espacio reducido
- ✓ Procesos de producción periódicamente cambiantes
- ✓ Procesos secuenciales
- ✓ Maquinaria de procesos variables
- ✓ Instalaciones de procesos complejos y amplios
- ✓ Chequeo de programación centralizada de las partes del proceso

Dentro de las aplicaciones generales de los PLC's, se tienen los siguientes ejemplos:

- ✓ Maniobra de máquinas
- ✓ Maquinaria industrial de plástico

- ✓ Maquinaria de embalajes
- ✓ Maniobra de instalaciones
- ✓ Instalación de aire acondicionado, calefacción...
- ✓ Instalaciones de seguridad
- ✓ Señalización y control
- ✓ Chequeo de programas

## II.6 SISTEMAS DE CONTROL SUPERVISORIO Y ADQUISICIÓN DE DATOS (SCADA)

### Definición de sistema SCADA.

SCADA es el acrónimo de *Supervisory Control And Data Acquisition* (Supervisión, Control y Adquisición de Datos). Es un sistema basado en computadores que permite supervisar y controlar a distancia una instalación de cualquier tipo. A diferencia de los Sistemas de Control Distribuido (DCS), el lazo de control es generalmente cerrado por el operador.

Comprende todas aquellas soluciones de aplicación para referirse a la captura de información de un proceso o planta industrial (aunque no es absolutamente necesario que pertenezca a este ámbito), con esta información es posible realizar una serie de análisis o estudios con los que se pueden obtener valiosos indicadores que permitan una retroalimentación sobre un operador o sobre el propio proceso, tales como:

- Indicadores sin retroalimentación inherente (no afectan al proceso, sólo al operador):
  - Estado actual del proceso. Valores instantáneos;
  - Desviación o deriva del proceso. Evolución histórica y acumulada;
- Indicadores con retroalimentación inherente (afectan al proceso, después al operador):
  - Generación de alarmas;
  - HMI *Human Machine Interface* (Interfaces hombre-máquina);
  - Toma de decisiones:
    - Mediante operatoria humana;
    - Automática (mediante la utilización de sistemas basados en el conocimiento o sistemas expertos).<sup>7</sup>

---

<sup>7</sup> <http://es.wikipedia.org/wiki/SCADA>. Diciembre 7, 2006.

En la tabla No.1 se muestra un cuadro comparativo de las principales características de los sistemas SCADA y los sistemas de Control Distribuido (DCS).

Tabla No. : Algunas diferencias típicas entre sistemas SCADA y DCS.

ASPECTO	SCADAs	DCS
TIPO DE ARQUITECTURA	CENTRALIZADA	DISTRIBUIDA
TIPO DE CONTROL PREDOMINANTE	SUPERVISORIO: Lazos de control cerrados por el operador. Adicionalmente: control secuencial y regulatorio.	REGULATORIO: Lazos de control cerrados automáticamente por el sistema. Adicionalmente: control secuencial, batch, algoritmos avanzados, etcétera.
TIPOS DE VARIABLES	DESACOPLADAS	ACOPLADAS
ÁREA DE ACCIÓN	Áreas geográficamente distribuidas.	Área de la planta.
UNIDADES DE ADQUISICIÓN DE DATOS Y CONTROL	Remotas, PLCs.	Controladores de lazo, PLCs.
MEDIOS DE COMUNICACIÓN	Radio, satélite, líneas telefónicas, conexión directa, LAN, WAN.	Redes de área local, conexión directa.
BASE DE DATOS	CENTRALIZADA	DISTRIBUIDA

El flujo de la información en los sistemas SCADA es como se describe a continuación: el fenómeno físico lo constituye la variable que deseamos medir. Dependiendo del proceso, la naturaleza del fenómeno es muy diversa: presión, temperatura, flujo, potencia, intensidad de corriente, voltaje, ph, densidad, etcétera. Este fenómeno debe traducirse a una variable que sea inteligible para el sistema SCADA, es decir, en una variable eléctrica. Para ello, se utilizan los transductores.

Sin embargo, esta variedad de tipos de señales eléctricas debe ser procesada para ser entendida por el computador digital. Para ello se utilizan **acondicionadores de señal**, cuya función es la de referenciar estos cambios eléctricos a una misma escala de corriente o voltaje. Además, provee aislamiento eléctrico y filtraje de la señal con el objeto de proteger el sistema de ruidos originados en el campo.

Una vez acondicionada la señal, la misma se convierte en un valor digital equivalente en el bloque de conversión de datos. Generalmente, esta función es llevada a cabo por un circuito de conversión analógico/digital. El computador almacena esta información, la cual es utilizada para su análisis y para la toma de

decisiones. Simultáneamente, se muestra la información al usuario del sistema, en tiempo real.

Basado en la información, el operador puede tomar la decisión de realizar una acción de control sobre el proceso. El operador comanda al computador a realizarla, y de nuevo debe convertirse la información digital a una señal eléctrica. Esta señal eléctrica es procesada por una salida de control, el cual funciona como un acondicionador de señal, la cual la escala para manejar un dispositivo dado: bobina de un relé<sup>δ</sup>, *set point* de un controlador, etcétera.

### II.6.1 Necesidad de un Sistema SCADA

Para evaluar si un sistema SCADA es necesario para manejar una instalación dada, el proceso a controlar debe cumplir las siguientes características:

- a) El número de variables del proceso que se necesita monitorear es alto.
- b) El proceso está geográficamente distribuido. Esta condición no es limitativa, ya que puede instalarse un SCADA para la supervisión y control de un proceso concentrado en una localidad.
- c) La información del proceso se necesita en el momento en que los cambios se producen en el mismo, o en otras palabras, la información se requiere en tiempo real.
- d) La necesidad de optimizar y facilitar las operaciones de la planta, así como la toma de decisiones, tanto gerenciales como operativas.
- e) Los beneficios obtenidos en el proceso justifican la inversión en un sistema SCADA. Estos beneficios pueden reflejarse como aumento de la efectividad de la producción, de los niveles de seguridad, etcétera.

La complejidad y velocidad del proceso permiten que la mayoría de las acciones de control sean iniciadas por un operador. En caso contrario, se requerirá de un Sistema de Control Automático, el cual lo puede constituir un Sistema de Control Distribuido, PLC's, Controladores de Lazo Cerrado o una combinación de ellos.

---

<sup>δ</sup> El relé es un dispositivo en el que por medio de un electroimán se acciona un juego de uno o varios contactos que permiten abrir o cerrar circuitos eléctricos. Dependiendo del número de contactos, intensidad admisible por los mismos, tipo de corriente de accionamiento, tiempo de activación y desactivación, etcétera.



## II.6.2 Funciones

Dentro de las funciones básicas realizadas por un sistema SCADA están las siguientes:

- a) Recabar, almacenar y mostrar información, en forma continua y confiable, correspondiente a la señalización de campo: estados de dispositivos, mediciones, alarmas, etcétera.
- b) Ejecutar acciones de control iniciadas por el operador, tales como: abrir o cerrar válvulas, arrancar o parar bombas, etcétera.
- c) Alertar al operador de cambios detectados en la planta, tanto aquellos que no se consideren normales (alarmas) como cambios que se produzcan en la operación diaria de la planta (eventos). Estos cambios son almacenados en el sistema para su posterior análisis.
- d) Aplicaciones en general, basadas en la información obtenida por el sistema, tales como: reportes, gráficos de tendencia, historia de variables, cálculos, predicciones, detección de fugas, etcétera.

## II.7 SISTEMAS DE CONTROL DISTRIBUIDO (DCS)

Los Sistemas de Control Distribuido se caracterizan por realizar las acciones de control en forma automática (Fig. 6).

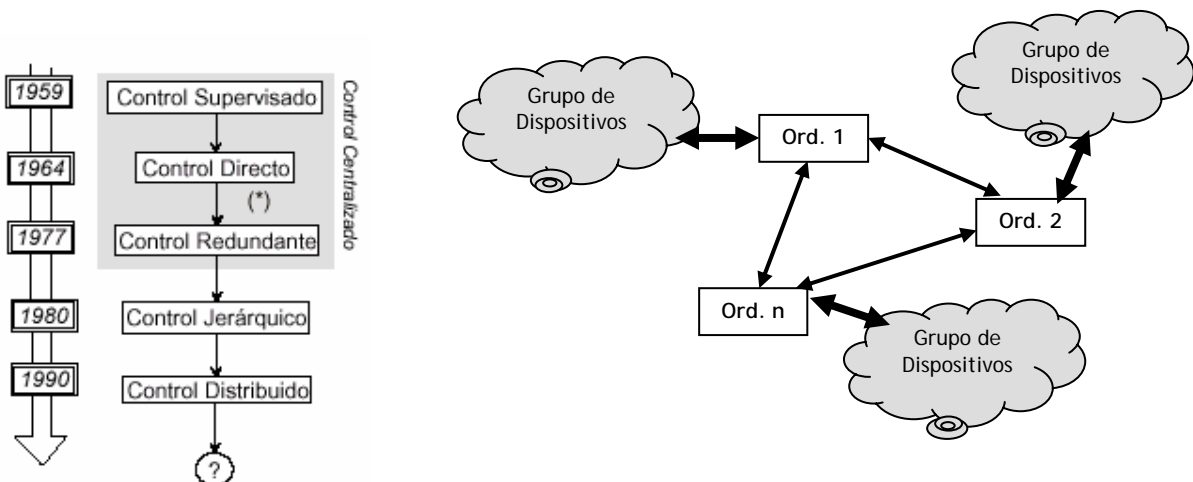


Fig. 6. Diagrama de Control Distribuido.

Las principales características del Control Distribuido son:

- Ordenadores similares entre los que se dividen todas las tareas de control.
- Mayor robustez a fallos de algún ordenador.
- Mayor eficiencia debida al proceso paralelo.
- Mayor rigidez en los dispositivos.
- Mayor escalabilidad.
- Cobertura de plantas de mayor tamaño.
- Necesidad de mayor flujo de datos en caso de distribución automática de tareas.

## Capítulo III. TOPOLOGÍAS DE RED

Los nodos de red necesitan estar conectados para comunicarse, y a la representación física y lógica de una red se le conoce como **topología**, la cual va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etcétera.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

La **topología física**, es la disposición física y real de las máquinas, dispositivos de red y cableado (los medios), la manera en que los nodos están conectados unos con otros.

La **topología lógica** es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la misma, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (*Ethernet*) y transmisión de *tokens* (*Token Ring*).

La topología de **broadcast** significa que cada nodo envía sus datos hacia todos los demás nodos del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona *Ethernet*.

En cambio, la transmisión de **tokens** controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada nodo. Cuando un nodo recibe el *token* significa que puede enviar datos a través de la red. Si el nodo no tiene ningún dato para enviar, transmite el *token* hacia el siguiente nodo y el proceso se vuelve a repetir.

### III.1 MODELOS DE TOPOLOGÍA

Las principales modelos de topología son:

- Bus
- Anillo
- Estrella
- Árbol
- Malla
- Red celular

Las cuales se describen a continuación:

### III.1.1 BUS

En una topología de bus (Fig. 7), cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma. El cable puede ir por el piso, por las paredes, por el techo, o puede ser una combinación de éstos, siempre y cuando el cable sea un segmento continuo.

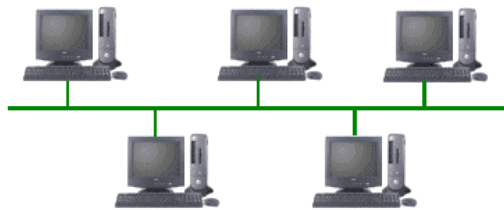


Fig. 7. Topología de Bus.

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red.

### III.1.2 ANILLO

Una topología de anillo (Fig. 8) consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional; no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o contraseña de paso.

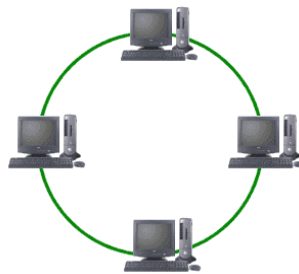


Fig. 8. Topología de Anillo.

### III.1.3 ESTRELLA

Uno de los tipos más antiguos de topologías de redes es la estrella (Fig. 9), la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de red en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos, el nodo central, generalmente está ocupado por un hub y a través de él pasa toda la información que circula por la red.

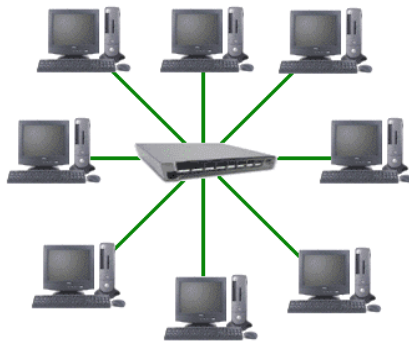


Fig. 9. Topología en Estrella.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente además de facilitar la administración de la red. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

### III.1.4 ÁRBOL

La topología en árbol (Fig.10) es similar a la topología en estrella, salvo que no tiene un nodo central. En cambio, cuenta con un nodo de enlace troncal, que generalmente está ocupado por un hub o *switch*, desde el que se ramifican los demás nodos.



Fig. 10. Topología en Árbol.

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un nodo servidor.

### III.1.5 MALLA

En una topología de malla (Fig. 11), cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada nodo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

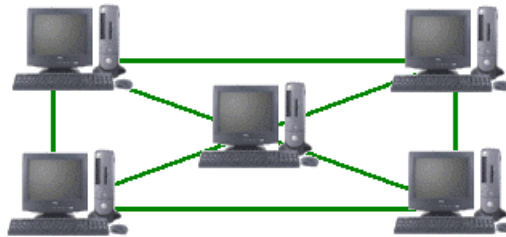


Fig. 11. Topología en Malla.

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces y, la cantidad de conexiones con los enlaces se torna abrumadora.

### III.1.6 RED CELULAR

La topología celular (Fig. 12) está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

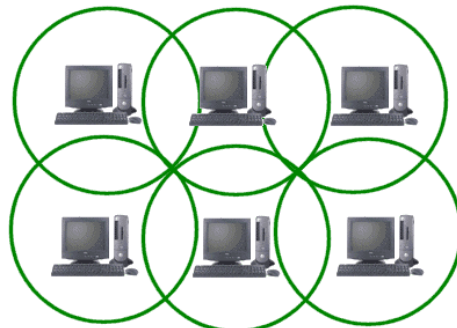


Fig. 12. Topología de Red Celular.

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas.

La ventaja de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

## III.2 MODELO OSI

El modelo OSI define en siete capas los protocolos de comunicación. Cada uno de los niveles tiene funciones definidas, que se relacionan con las funciones de las capas siguientes. Los niveles inferiores se encargan de acceder al medio, mientras que los superiores, definen cómo las aplicaciones acceden a los protocolos de comunicación.

### III.2.1 ANTECEDENTES

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, *Open System Interconnection*) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de *networking*, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de *networking* privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controla todo uso de la

tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de *networking* como la red de *Digital Equipment Corporation* (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El OSI fue desarrollado como modelo de referencia, para la conexión de los sistemas abiertos (heterogéneos). No es una arquitectura de red, pues no define que aplicaciones ni protocolos usar, sino dice que hace cada capa.

**Capa Física:** Se ocupa de la transmisión de los bits de información por el canal de comunicación o medio utilizado para la transmisión.

Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (*simplex*, *duplex* o *full-duplex*). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

Esta es la encargada de que si un extremo envía un bit, con valor 0 o 1, llegue al otro extremo de la misma manera.

Como resumen, podemos decir que se encarga de transformar un paquete de información binaria (*Frame*) en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); electromagnéticos (transmisión *Wireless*) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

Por ejemplo: este nivel define la medida del cable coaxial y de los conectores BNC utilizados.

**Capa de Enlace:** esta capa traslada los mensajes hacia o desde la capa física a la capa de red. Especifica como se organizan los datos cuando se transmiten en un medio particular, esta capa define como son los *frames*, las direcciones y las sumas de control (*Checksum*) de los paquetes.



Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Las tramas recibidas son comprobadas por el receptor y cuando una trama es totalmente destruida por una ráfaga de ruido, la capa de enlace de la computadora emisora, se encarga de retransmitirla. También se encarga de resolver la duplicidad de tramas, debido a que se puede destruir el acuse de recibo de la misma.

La capa de enlace puede considerarse dividida en dos subcapas:

Control lógico de enlace LLC (*Logical Link Control*) define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

Control de acceso al medio MAC (*Medium Access Control*). Esta subcapa actúa como controladora del *hardware* subyacente (el adaptador de red). Su principal tarea consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) utilizado en *Ethernet* es un típico ejemplo de esta subcapa.

**Capa de Red:** Se ocupa de controlar las operaciones de las subredes y resuelve como enviar los paquetes del origen al destino en la dirección adecuada. Controla también la congestión en la red ocasionada por la presencia de muchos paquetes, debido a que esto puede llevar a un cuello de botella.

Esta capa resuelve los problemas de comunicación, que resulta de unir redes heterogéneas, causados por uniones de redes que manejan diferentes protocolos y tienen formas diferentes de direccionamiento. Por ejemplo, una red puede no querer recibir un mensaje por ser demasiado largo, esta capa lo soluciona.

**Capa de Transporte:** La función de esta capa es aceptar los datos de la Capa de Sesión, dividirlos si es necesario y pasarlos a la Capa de Red y asegurarse que lleguen correctamente al destino. Esta capa crea una conexión de red, distinta para cada conexión de transporte solicitada por la capa de sesión. Si el caudal es grande puede realizar más de una conexión para mejorarlo. Debido a que estas conexiones son costosas, esta capa puede multiplexar varias conexiones de transporte sobre la misma conexión de red, para abaratarlo.

La conexión más conocida es el canal punto a punto, en el cual se entregan los mensajes en el mismo orden que fueron enviados. Otra forma del servicio de transporte es el envío de mensajes aislados, que no garantizan el orden de difusión, ni la distribución de mensajes a destinos múltiples.

La capa de transporte se encarga de establecer y liberar conexiones en la red.

**Capa de Sesión:** Permite que usuarios en distintas computadoras establezcan una sesión entre ellos, a través de la misma se puede llevar a cabo un transporte de datos, tal como lo hace la capa de transporte. La mejora de los servicios, le permite al usuario acceder a un sistema de tiempo compartido a distancia o transferir un archivo.

Servicios de esta capa:

- **controlar el diálogo:** las sesiones permiten que el tráfico se realice en ambas direcciones o en una sola en un momento dado, cuando se realiza en un solo sentido, esta capa ayudará en el seguimiento de quien tiene el turno.
- **administración de testigo:** esto es para que en algunos protocolos los dos extremos no quieran transmitir al mismo tiempo, de esta forma sólo lo hace el que posee el testigo (*token*).
- **sincronización:** esta capa proporciona la inserción de puntos de verificación para el control de flujo. Esto es pues, si dos computadoras desean transmitir un archivo que lleva dos horas, y al cabo de una hora se interrumpen las conexiones de red, la transmisión se debe desarrollar nuevamente desde el principio, con el servicio que brinda esta capa sólo se transmite lo posterior al punto de verificación.

**Capa de Presentación:** Esta capa no cumple las mismas funciones que las anteriores, quienes se encargaban de la transmisión fiable de los bits, sino que se ocupa de la sintaxis y la semántica de la información, estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Esta capa es buena candidata para implementar aplicaciones de criptografía.

**Capa de Aplicación:** Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia de ficheros, etcétera) Por ejemplo, esta capa implementa la operación con ficheros del sistema. Por un lado interactúan con la capa de presentación; por otro representan la interfaz con el usuario, entregándole la información y recibiendo los comandos que dirigen la comunicación. Las aplicaciones más comunes son: transferencia de archivos (FTP), acceso de archivos remotos (TELNET) o cuando dos personas trabajan sobre computadoras distintas, para un mismo proyecto.

### III.2.2 FAMILIA DE PROTOCOLOS DE INTERNET

El protocolo TCP (*Transmission Control Protocol*) / IP (*Internet Protocol*) es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software* incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de *hardware*.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).
- **Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- **Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- **Enlace:** Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada *host*, como puede ser una línea punto a punto o una red *Ethernet*.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo se tiene que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de datagrama, y son conjuntos de datos que se envían como mensajes independientes.

## Capítulo IV. BUSES DE CAMPO

Un bus de campo es el término genérico que describe un conjunto de redes de comunicación para uso industrial, cuyo objetivo es sustituir las conexiones punto a punto entre los elementos de campo y el equipo de control a través del tradicional bucle de corriente de 4-20 mA. Típicamente son redes digitales, bidireccionales, multipunto, montadas sobre un bus serie, que conectan dispositivos de campo como PLCs, transductores, actuadores y sensores. 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 será capaz de ejecutar funciones simples de diagnóstico, control o mantenimiento, así como comunicarse bidireccionalmente a través del bus.

El objetivo de este tipo de bus es reemplazar a los sistemas de control centralizados por redes para 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/o reciben los dispositivos de campo es digital, lo que resulta mucho más preciso que si se recurre a métodos analógicos. Así cada nodo de la red puede informar en caso de fallo del dispositivo asociado, esta monitorización permite aumentar la eficiencia del sistema y reducir la cantidad de horas de mantenimiento necesarias.<sup>8</sup>

### IV.1.1 VENTAJAS DE LOS BUSES DE CAMPO

La principal ventaja que ofrecen los buses de campo, y la que los hace más atractivos a los usuarios finales, es la **reducción de costos**. El ahorro proviene de tres fuentes: en costo de instalación, en el mantenimiento y en los derivados de la mejora del funcionamiento del sistema.

El hecho de que los buses de campo sean más sencillos que otras redes de uso industrial, hace que las necesidades de **mantenimiento de la red** sean menores, de modo que la fiabilidad del sistema a largo plazo aumenta. Además, este tipo de bus permite a los operadores monitorizar todos los dispositivos que integran el sistema e interpretar fácilmente las interacciones entre ellos. De esta forma, la detección de las fuentes de problemas en la planta y su corrección resulta mucho más sencilla, reduciendo los costes de mantenimiento y el tiempo de inactividad de la planta.

---

<sup>8</sup> *Apud.* Sirgo, J.A., González Rafael. *Op Cit.* Pág. 9

Estos buses ofrecen mayor **flexibilidad** al usuario en el diseño del sistema, ya que algunos algoritmos y procedimientos de control radican en los propios dispositivos de campo. Hay que tener en cuenta que las prestaciones del sistema mejoran con el uso de la tecnología de este tipo de bus, debido a la **simplificación** en la forma de obtener información de la planta desde los distintos sensores; las mediciones realizadas están disponibles para todos los demás elementos de la red permitiendo así el diseño de sistemas de control más eficientes.

Otra de las ventajas del bus de campo es que sólo incluyen cuatro capas del modelo OSI (Física, Enlace, Aplicación y Usuario), y un conjunto de **servicios de administración**.<sup>9</sup> El usuario no tiene que preocuparse de las capas de enlace o de aplicación, sólo necesita saber cual es la funcionalidad.

#### IV.1.2 BUSES DE CAMPO EXISTENTES

Debido a la falta de estándares, diferentes compañías han desarrollado diversas soluciones, cada una de ellas con prestaciones y campos de aplicación variados. En una primera clasificación se pueden clasificar como:

a) Buses de alta velocidad y baja funcionalidad

Los buses de alta velocidad y baja funcionalidad están diseñados para integrar dispositivos simples como fotocélulas y actuadores simples, funcionando en aplicaciones de tiempo real y agrupándose en una pequeña zona de la planta. Suelen especificar las capas física y de enlace del modelo OSI. Algunos ejemplos son:

- ◆ CAN: diseñado originalmente para su aplicación en vehículos
- ◆ SDS: Bus para la integración de sensores y actuadores, basado en CAN
- ◆ ASI: Bus serie diseñado por Siemens para la integración de sensores y actuadores.

b) Buses de alta velocidad y funcionalidad media

Los buses de alta velocidad y funcionalidad media se basan en una capa de enlace para el envío eficiente de bloques de datos tamaño medio. Estos mensajes permiten que el dispositivo tenga mayor funcionalidad de modo

---

<sup>9</sup> *Íbidem*. Pág. 11

que permite incluir aspectos como la configuración, calibración o programación del dispositivo. Son buses capaces de controlar dispositivos de campo complejos, de forma eficiente y a bajo costo.

Normalmente incluyen la especificación completa de la capa de aplicación, lo que significa que se dispone de funciones utilizables desde programas basados en PCs para acceder, cambiar y controlar los diversos dispositivos que constituyen el sistema. Algunos ejemplos son:

- ♦ DeviceNet: desarrollado por Allen-Bradley, utiliza como base el bus CAN, e incorpora una capa de aplicación orientada a objetos.
- ♦ LONWorks: red desarrollada por Echelon.
- ♦ BitBus: red desarrollada por INTEL.
- ♦ DIN MessBus: estándar alemán de bus de instrumentación, basado en comunicación RS-232.
- ♦ InterBus-S: bus de campo alemán de uso común en aplicaciones medias.

#### c) Buses de altas prestaciones

Los buses de altas prestaciones son capaces de soportar comunicaciones a nivel de toda la planta, en muy diversos tipos de aplicaciones. Aunque se basan en buses de alta velocidad, algunos presentan problemas debido a la sobrecarga necesaria para alcanzar las características funcionales y de seguridad que se les exigen. La capacidad de aplicación oferta un gran número de servicios a la capa del usuario. Entre sus características incluyen:

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

Algunos ejemplos son:

- ◆ Profibus
- ◆ FIP
- ◆ Fieldbus Foundation

## IV.2 REDES SENSOR - ACTUADOR. ASI

El bus ASI (*Actuator Sensor Interface*) es un bus de campo desarrollado por Siemens para la interconexión de actuadores y sensores. Actualmente está recogido por el estándar IEC TG 17B.

ASI, es una simple red para la conexión directa de sensores binarios y actuadores al nivel más bajo de automatización (nivel de e/s) hacia redes de más alto nivel y dispositivos de control. Reemplazando complejos cableados y paneles, ASI reduce el tiempo de diseño, costo de instalación y complejidad de mantenimiento. Todo esto desemboca en la reducción de los costos totales.

A nivel físico, la red puede adoptar cualquier tipo de topología: ya sea en bus, árbol, estrella o en anillo. Permite la interconexión de un máximo de 31 esclavos, la longitud máxima de cada segmento es de 100 metros. Dispone de repetidores que permiten la unión de hasta 3 segmentos, y de puentes hacia redes Profibus. Como medio físico de transmisión, emplea un único cable que permite tanto la transmisión de datos como la alimentación de los dispositivos conectados a la red. Su diseño evita errores de polaridad al conectar nuevos dispositivos a la red. La incorporación o eliminación de elementos a la red no requiere la modificación del cable.

El cable consta de dos hilos sin apantallamiento. Para lograr inmunidad al ruido, la transmisión se hace basándose en una codificación Manchester (Fig. 13), esta codificación se traduce en pulsos de corriente, que producen pulsos positivos y negativos en la tensión de alimentación, que indican las transiciones en la señal. A partir de la detección de dichas transiciones se reconstruye la secuencia de bits transmitida.



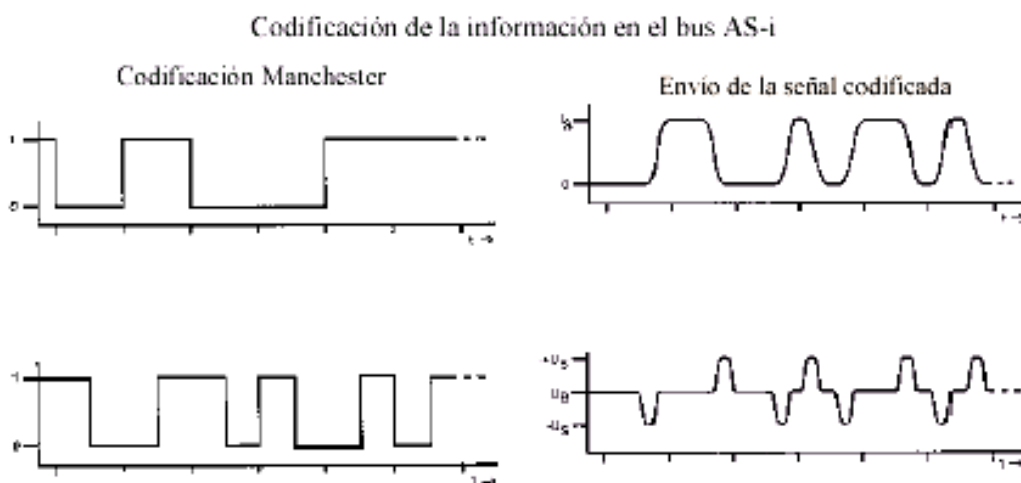


Fig. 13. Codificación Manchester.

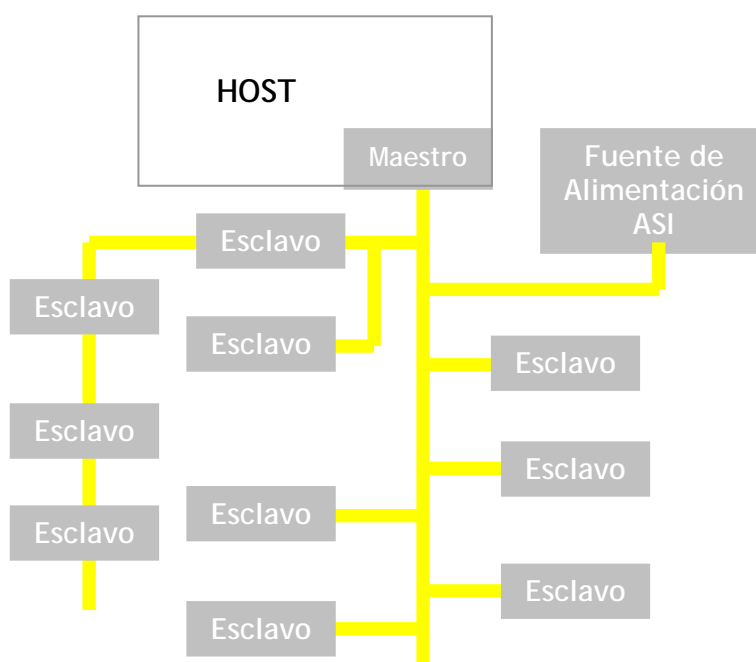


Fig. 14A. Esquema de distribución de una red ASi.

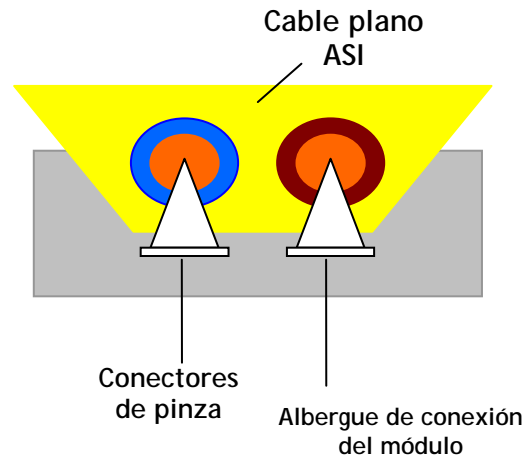


Fig. 14B. Cable ASI y método de conexión.

Tal y como lo muestra la figura anterior (Fig. 14A y 14B), la instalación de esta red requiere como elementos esenciales:

**Un maestro:** suele estar conectado a un autómata programable o al elemento de control principal. También puede estar conectado a un *gateway* que permita comunicarse con el bus ASI desde diferentes dispositivos a través de una red de nivel superior.

**Una fuente de alimentación:** proporciona 30 VDC y hasta 8A para alimentar a los esclavos a través de un solo cable. Adicionalmente es posible conectar otro tipo de tensión de alimentación para proporcionar mayores corrientes si es necesario; para ello, se instalan fuentes que proporcionen alimentación a través de cables adicionales de 24 VDC y 230 VAC.

**Los esclavos:** existen dos tipos principales, aquellos que integran el protocolo en el mismo elemento de entrada/salida mediante la inclusión de un chip ASIC (Circuito Integrado de Aplicación Específica), y aquellos módulos ASI genéricos que disponen de 4 entradas/salidas de tensión para poder conectarles cualquier elemento sensor/actuador binario tradicional. Esta última opción resulta aconsejable para las instalaciones ya existentes pues no es necesario sustituir los elementos, sino únicamente cables de conexión.

**Cables de conexión:** generalmente es cable plano de dos hilos no apantallado. Su color amarillo y su muesca en un lado suele identificarlo y facilitar la instalación. También es admisible el uso de cable normal uno de dos hilos con 1.5 mm<sup>2</sup> de sección por hilo, tanto apantallado como no apantallado, pero en este caso es necesario ser más cuidadoso en la instalación para no confundir polaridades.

Existen algunos módulos de esclavos que incorporan un “*watchdog*” o vigilante supervisor que revisa continuamente la comunicación con el maestro y actúan en caso de que ésta sea interrumpida o se produzca la detección de errores (paridad y reenvío, etcétera), poniendo en modo de seguridad las entradas/salidas controladas por él. Si no se reciben mensajes del maestro durante 40 ms., las salidas pasan a estar apagadas (*off*) o simulan un estado de reset continuo del sistema. Las causas habituales de una pérdida de comunicación pueden ser la rotura de un cable, un fallo en el maestro (o su paso a estado de parada), o bien una falta de direccionamiento del módulo. La utilización de ASi en entornos con fuertes interferencias (sistemas de soldadura, convertidores de frecuencia, por ejemplo) puede hacerse sin problemas.

También existen módulos específicos para la detección de fallos y protección de seguridad eléctrica llamado “monitor de seguridad”, encargado de monitorear que las señales eléctricas transmitidas sean adecuadas, y verifica la aparición de derivaciones a tierra o la protección contra sobretensiones, en cuyo caso es posible enviar un mensaje al módulo maestro para que permita ejecutar acciones de protección o incluso controlar relés de protección directamente.

#### ESPECIFICACIONES TÉCNICAS

1. **Medio de transmisión** Par de cable sin apantallar para transporte de datos y alimentación (24V DC, 8A típicos para el bus)
2. **Longitud máxima de cable de bus** 100m
3. **Número máximo de esclavos** 31
4. **Número de participantes** Hasta 4 sensores y 4 actuadores por esclavo (máximo 124 bidireccionales = máximo 248 participantes binarios)
5. **Direccionamiento** Cada esclavo posee una dirección, la cual es definida por el maestro o por designación manual.
6. **Mensajes** El maestro transmite los datos para una sola dirección, respondiendo de forma inmediata el esclavo correspondiente.
7. **Bit-rate** 4 bits por esclavo y mensaje
8. **Tiempo de ciclo con 31 esclavos** 5 ms.
9. **Detección de errores** Los mensajes incorrectos son identificados y reparados

10. Dispositivo interfaz 4 puertos de datos configurables (como entradas o salidas bidireccionales) además de 4 salidas parametrizadas y dos salidas de control (*strobe*)

11. Servicios del dispositivo maestro

- Inicializar la red
- Identificar los participantes
- Configuración acíclica de los parámetros a los esclavos
- Mensajes de error al Host
- Configuración de las direcciones en los esclavos reemplazados

12. Principio de funcionamiento basado en la técnica de sondeo con un maestro y varios esclavos. La cual el maestro interroga a las estaciones enviándoles mensajes (telegramas) de 14 bits y el esclavo responde con un mensaje de 7 bits.

Los telegramas tienen un formato sencillo, el del maestro contiene los siguientes campos:



- St: Bit de inicio. 0 indica el comienzo de la trama
- SB: Tipo de telegrama. 0 indica trama de datos y 1 trama de comandos
- A0...A4: Dirección del esclavo
- I0...I4: Información
- PB: Bit de paridad
- EB: Bit de fin

El esclavo responde con un telegrama de 7 bits de la forma:



- St: Bit de inicio. 0 indica el comienzo de la trama
- I0...I4: Información
- PB: Bit de paridad
- EB: Bit de fin

13. Es posible la comunicación con módulos analógicos.

14. Admite cualquier topología de red (incluyendo topologías mixtas), con una longitud máxima de 100 metros sin repetidores con caída de tensión máxima de 3V.

15. La tensión de operación de los esclavos debe estar entre 26.5V y 31.6V.
16. Típicamente, la corriente de consumo de cada esclavo es de 200 mA.

### IV.3 INTERBUS

El INTERBUS es un bus de campo para la interconexión de sensores y actuadores, las partes claves de INTERBUS han sido estandarizadas en Alemania por la DKE (*Deutsche Elektrotechnische Kommission* para DIN y VDE) en 1993 se publicó la norma DIN E 19258, que cubre los protocolos de transmisión y los servicios que necesita para la comunicación de datos de proceso.

INTERBUS se basa en un esquema maestro - esclavo, el maestro del bus actúa simultáneamente como interfaz con los niveles superiores de la jerarquía de comunicaciones. La topología es de anillo, es decir, todos los dispositivos están conectados formando un camino cerrado. El anillo principal es el que parte del maestro, aunque pueden formarse otros anillos para adaptarse a la estructura particular de cada sistema. Este tipo de conexiones se lleva a cabo mediante unos equipos denominados módulos terminadores de bus.

Un rasgo definitivo de INTERBUS es que las líneas de envío y recepción de datos están contenidas dentro de un mismo cable que une todos los dispositivos, de esta forma el sistema tiene el aspecto físico de un bus o un árbol. Típicamente la capa física se basa en el estándar RS-485; requiere un cable de 5 hilos para interconectar dos estaciones con velocidades de transmisión de 500 Kbits, pudiendo alcanzar distancias de hasta 400 metros entre dispositivos. Cada dispositivo incorpora una función de repetidor que permite extender el sistema hasta 13 Km. y para facilitar el funcionamiento de este bus, el número máximo de estaciones está limitado a 512.

La estructura de anillo ofrece dos ventajas: la primera es que permite el envío y recepción simultánea de datos (*full duplex*); y, la segunda, es que la capacidad de autodiagnóstico del sistema se ve mejorada, ya que la conexión de cada nodo a la red es activa. Para facilitar la detección de errores y la puesta en marcha del sistema, INTERBUS permite la desconexión transparente de los subanillos conectados al anillo principal.

El protocolo de transmisión se estructura en tres capas que corresponden al modelo OSI. La capa uno es la capa física, donde se especifican los aspectos como la velocidad y modos de codificación de la señal física. La capa dos corresponde a la capa de enlace, donde se garantiza la integridad de los datos y permite el soporte de dos tipos de datos, por una parte los datos correspondientes a procesos cíclicos, y por otra los datos que aparecen

asíncronamente. La capa de enlace es determinista, es decir, garantiza un tiempo máximo para el transporte de datos entre dispositivos.

El control de acceso al medio se encuentra dentro de los mecanismos *Time Division Multiple Access* (TDMA), eliminando así la posibilidad de colisiones; cada dispositivo tiene reservado un slot de tiempo adecuado para su función dentro del sistema, así el tiempo de ciclo es la suma de los tiempos asignados a cada dispositivo. Otra ventaja que incorpora este tipo de control de acceso al medio, es que todos los elementos insertan sus datos en el bus simultáneamente, lo que garantiza que las mediciones en las que se basan los bucles de control, fueron realizadas simultáneamente.

La trama se forma por concatenación de los datos de cada estación, de forma física se realiza mediante un registro. Cada dispositivo se une al anillo mediante un registro cuya longitud depende de la cantidad de información que debe transmitir; así los datos provenientes de las distintas estaciones van llegando al maestro en función de su posición dentro del anillo. Cada ciclo de transmisión comienza con una secuencia de datos que contiene la palabra de *loop back* seguida de los datos de salida de los distintos dispositivos en la línea de salida. Durante el envío de datos, el flujo de retorno entra al maestro como flujo de entrada, tras el envío de la trama completa se envía un CRC de 32 bits. Debido a la estructura de conexiones punto a punto, el cálculo siempre se hace entre cada dos nodos, por lo que no es necesario dar una vuelta completa al anillo. Por último se envía una palabra de control para indicar el estado de cada dispositivo y en caso de no haber errores, se inicia un nuevo ciclo.

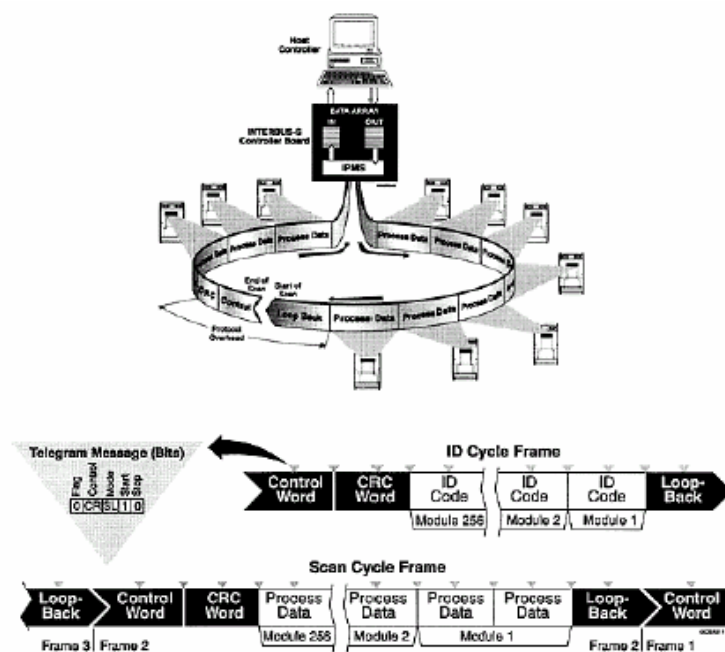


Fig. 15. Red INTERBUS.

La tercera de las capas de INTERBUS corresponde a la capa de aplicación (Fig. 15). En el maestro se ejecuta de forma cíclica un programa que actualiza continuamente los datos correspondientes a los distintos procesos conectados a la red, y los deja accesibles para el sistema de control, de modo que por ejemplo un PLC puede acceder a ellos de forma sencilla mediante instrucciones de entrada/salida.

INTERBUS implementa en la capa de aplicación un subconjunto de servicios que se denominan PMS (*Peripherals Message Specification*). Incluye servicios que permiten la comunicación con dispositivos de procesos inteligentes, entre éstos están el establecimiento y monitorización de conexiones, la lectura y escritura de parámetros o la ejecución remota de programas.

#### IV.4 CAN: CONTROLLER AREA NETWORK

*Controller Area Network* (CAN) es un bus de comunicaciones estandarizado por ISO, que fue desarrollado inicialmente a finales de los 80 para la industria del automóvil. En su especificación básica, se exigía alta velocidad, alta inmunidad al ruido y capacidad para la detección de cualquier tipo de error; con el tiempo, CAN ha pasado de la industria automovilística a la fabricación y a la industria aeronáutica.

CAN define sólo las dos capas más bajas del modelo OSI: física y de enlace. El medio físico consiste en un cable de par trenzado, lo que permite una velocidad máxima de 250 Kbps, mientras que la versión ampliada alcanza velocidades de 1 Mbps.

La implantación básica de CAN presenta un fuerte acoplamiento entre el CPU y el controlador CAN, los mensajes son difundidos por toda la red y son comprobados por el CPU de cada una de las estaciones que la forma, con este tipo de funcionamiento se disminuye el aprovechamiento de la velocidad de transmisión de la red. En la versión conocida como "*Full CAN*", el controlador de red incorpora un filtro de selección de mensajes en base a un campo de identificación y de esa forma el CPU sólo recibirá aquellos mensajes que le interesen.

Full CAN permite dos tamaños distintos de identificadores de mensajes: la versión A permite identificadores de 11 bits (2032 identificadores), mientras que la versión extendida (B) tiene identificadores de 29 bits.

La capa de enlace define el formato y la temporización usada para la transmisión de los mensajes. Las tramas CAN tienen 2 bytes descriptores y hasta 8 bytes de datos. Los descriptores definen la prioridad de los mensajes y su tipo; el primer

campo, o campo de arbitraje, está formado por los 11 bits del identificador (en tramas tipo A) y el bit RTR. Si RTR vale 0, indica que se trata de una trama de datos, mientras que si vale 1 indica que se trata de una petición de datos. En ese caso, el campo de datos indicará los bytes que formarán la respuesta.

### Trama tipo A

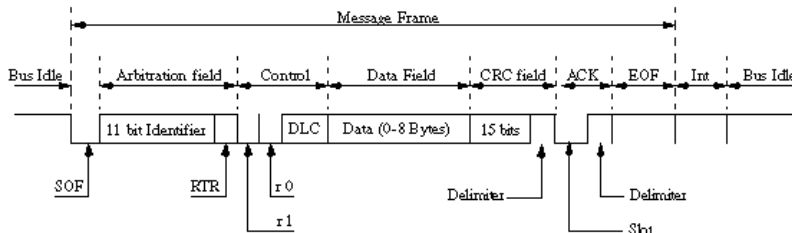


Fig. 16. Trama tipo A.

### Trama Tipo B

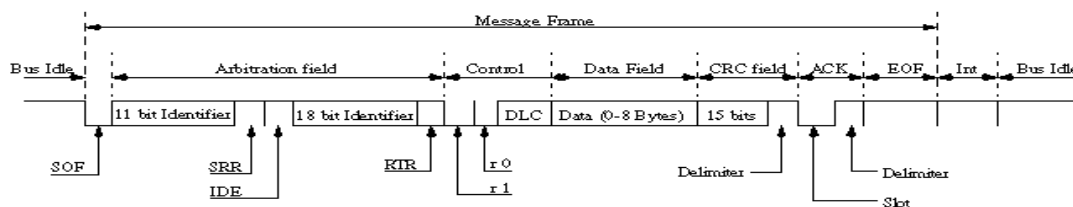


Fig. 17. Trama tipo B.

El campo de control está formado por 6 bits, los bits r1 r0 están reservados para futuras ampliaciones del protocolo. Los cuatro bits que forman el DCL indican el número de bytes que forman la trama de datos y que van a continuación.

El campo de datos contiene de cero a ocho bytes. El bit más significativo de cada byte es el primero que se transmite. A continuación hay un campo de CRC, que contiene un código de redundancia cíclica de 15 bits y 1 bit delimitador que siempre vale 1. El campo de acuse de recibo consiste en dos bits, el primer bit se envía a 1 y es puesto a 0 por las estaciones que reciben correctamente el mensaje y el segundo es un bit delimitador que vale 1. El delimitador de final de trama consiste en 7 bits a 1, tras cada trama hay un periodo de 3 bits (deben estar en 1), destinado a dar un tiempo mínimo a las estaciones a prepararse para la recepción o envío de otro mensaje.

Las tramas de tipo B se diferencian en el campo de arbitraje, en este caso hay un primer grupo de 11 bits similar al de las tramas tipo A que actúa como valor base del identificador; la segunda parte del identificador (18 bits) es la extensión del identificador. Para distinguir ambos formatos, la trama tipo B incorpora 2 bits que separan las dos partes de identificador, el primero es el bit SRR (*Substitute*



*Remote Request*). Se envía siempre a 1 para dar prioridad a las tramas de datos estándar de tipo A con el mismo identificador base. El bit IDE que sigue al bit SRR se envía siempre a 1, y permite distinguir tramas tipo A y tipo B.

Una característica fundamental de CAN es que cuanto menor sea el identificador mayor es su prioridad. Si dos nodos intentan transmitir simultáneamente el primero que envíe un 0 cuando el otro intente enviar un 1 obtendrá el acceso al medio, ya que el valor cero es dominante frente al valor uno. Como cada estación es capaz de monitorizar el medio físico, podrá detectar si su trama ha sido sobrescrita por otra de mayor prioridad (que permanece inalterada) La estación que no ha podido enviar el mensaje, reintentará el envío en cuanto detecte un periodo de inactividad.

Las ventajas de este mecanismo de acceso son la minimización del retardo en el acceso al no tener que esperar por turno como sucede en un sistema de paso de testigo, y la mejora de la eficiencia al evitar las colisiones destructivas. Los mensajes son enviados por orden de prioridad.

Un bus CAN puede tener un máximo de 32 nodos y el número de mensajes por segundo varía entre 2000 y 5000 en un bus de 250 Kbps, según el número de bytes por mensaje.

Aunque CAN se basa en un medio físico de par trenzados, también existen interfaces para la conexión mediante fibra óptica. El método más común es el par trenzado, de modo que las señales se envían mediante una diferencia de tensión entre los dos hilos; los hilos reciben el nombre de CAN\_H y CAN\_L respectivamente y en estado inactivo la diferencia de tensión entre ambos es de 2.5 V. El uso de tensiones diferenciales permite continuar con el uso de CAN incluso si una de las líneas está dañada, o en ambientes muy ruidosos.<sup>10</sup>

## IV.5 BITBUS: ESTRUCTURA FÍSICA Y PROTOCOLO

Introducido por Intel a principios de los 80. Es un bus maestro-esclavo soportado sobre RS485 y normalizado en IEEE- 1118. Debido a su sencillez ha sido adoptado en redes de pequeños fabricantes o integradores. En su capa de aplicación se contempla la gestión de tareas distribuidas, es decir es, en cierto modo, un sistema multitarea distribuido.

Este sistema de bus tiene una estructura maestro/esclavo, la cual soporta tanto una topología de bus o árbol (con repetidores). Un maestro y 27 esclavos se pueden comunicar entre ellos. Se puede alcanzar una velocidad de transferencia

---

<sup>10</sup> *Íbidem*. Pág. 18

de 62.5 Kbit/seg con una longitud de onda de 1.2 km y si la longitud de línea se reduce a 300 m, la velocidad de transferencia puede aumentar a 375 Kbit/seg. Los datos pueden ser transmitidos sobre cable de par trenzado o Fibra Óptica. La velocidad de transferencia de 375 Kbit/seg en modo asíncrono. Se accede al Bus por elección (*polling*). Son necesarios un par de cables adicionales si se utilizan repetidores. Pueden ser implementados en topología multicapa por conexión de una unidad maestra y una esclava a un nodo.

#### IV.5.1 CABLEADO Y TERMINACIONES

El cableado puede estar formado por uno o dos pares de cables trenzados y apantallados, siendo el apantallamiento común para todos los cables.

Normalmente se emplea un par de cables para la línea de datos semiduplex y el segundo par para una de las siguientes aplicaciones:

- Transmisión del reloj en modo síncrono.
- Conmutación de la línea en repetidores en modo autoreloj.

La impedancia característica de cada par de cables debe ser 120 ohmios. Las terminaciones serán resistencias de 120 ohmios para evitar el efecto de reflexión.

#### Conectores

El estándar especifica que los conectores deben ser del tipo sub-D9. El patillaje es el mismo que para un conector RS-232, pero sólo se emplean las señales RxD, TxD y masa.

#### IV.5.2 ESTRUCTURA

La estructura de la red BITBUS puede ser de varios tipos:

- **Básica:** estructura lógica del tipo maestro-esclavo.
- **Árbol:** se emplean repetidores para largas distancias, se considera todo un único bus y se opera en modo autoreloj (debido a que los repetidores no transmiten la señal de reloj).
- **Árbol multinivel:** se emplean uniones esclavo-maestro para formar sub-buses en varios niveles. Cada nivel puede operar a una velocidad propia y posee sus propias direcciones (Fig.18).

Ejemplo:

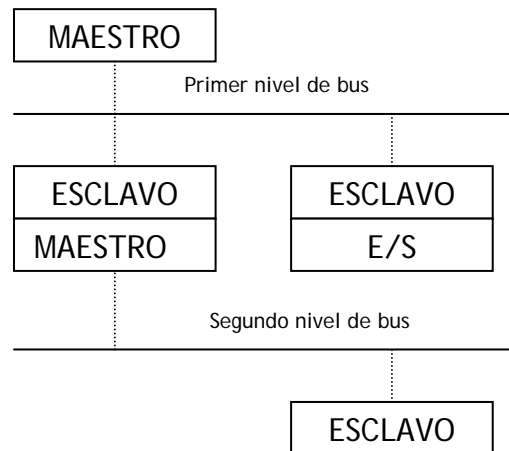


Fig. 18. Árbol multinivel.

En la siguiente tabla (Tabla No.2) se muestran las distintas posibilidades de nodos y repetidores:

Modo	Nº máx. de nodos	Nº máx. de repetidores	Velocidad (bits/s)	Distancia máx. (m)
Autoreloj	28	Ninguno	62,5 K	1200
Autoreloj	28	Ninguno	375 K	300
Autoreloj	250	10	62,5 K	1200 entre repetidores (4800 máx.)
Autoreloj	250	2	375 K	300 entre repetidores (900 máx.)
Síncrono	28	Ninguno	62,5 K o 375 K	300 o 1200 (según velocidad)

#### IV.5.3 TIPOS DE NODOS

Todo bus BITBUS se compone de elementos básicos denominados nodos. Un nodo es cualquier dispositivo que contenga al menos una interfaz con el bus. Los nodos posibles son:

- **Maestro:** permite controlar el acceso a un bus de cualquier nivel mediante un protocolo de comunicación del tipo pregunta-respuesta. En cada nivel sólo existe un maestro, aunque es posible la existencia de un maestro flotante (desaconsejado por el estándar).
- **Esclavo:** es un bloque controlado por el maestro, el cual sólo transmite si el maestro lo indica. El esclavo puede estar conectado a su vez con un maestro o un bloque de E/S.
- **Repetidor:** se encarga de regenerar la señal de datos del bus (no el reloj). Se emplea para aumentar la longitud del bus.
- **Expansión E/S:** es cualquier dispositivo de E/S que se quiera conectar al bus o a un esclavo.

#### IV.5.4 MODOS DE SINCRONIZACIÓN

Existen dos modos de sincronización de bits:

- **Síncrono:** en este modo los datos se transmiten por un par trenzado y el reloj mediante otro par adicional. No se admiten repetidores y la estructura del bus es completamente lineal (sólo hay un nivel).
- **Autoreloj:** en este modo cada nodo genera su propio reloj, sincronizando con la línea de datos. Los datos se codifican en formato NRZI. Se permiten repetidores (obligatorio para más de 28 nodos). Las derivaciones a partir del repetidor requieren una línea de control además de la línea de datos, por lo que se emplean dos pares trenzados.

#### IV.5.5 CODIFICACIÓN

Nivel de bits:

- **Modo síncrono:** la codificación se realiza mediante el procedimiento NRZ (0 es nivel bajo y 1 es nivel alto).
- **Modo autoreloj:** la codificación se realiza mediante el procedimiento NRZI (0 es cambio de nivel y 1 es un NO cambio de nivel).

A nivel de byte se emplea un juego reducido del protocolo SDLC de IBM. Este protocolo inserta un "0" después de cinco "1" consecutivos. Este sistema, combinado con la codificación de bit por NRZI, permite sincronizar el reloj en el receptor en modo autoreloj cada 6 bits como mínimo.

El controlador de Intel 8044 proporciona la inserción y eliminación de ceros del protocolo SDLC de forma automática.

#### IV.5.6 TRAMA DEL MENSAJE

La comunicación entre nodos se realiza mediante mensajes. Dicha comunicación siempre se efectúa a petición del maestro y consta siempre de un mensaje de pregunta al esclavo y de un mensaje de respuesta del mismo.

La trama de mensaje se compone de entre 6 y 255 bytes, siendo su estructura la siguiente:

Flag (7Eh)	Dirección esclavo	Control	Información (funciones/datos)	CRC (16 bits)	Flag (7Eh)
---------------	----------------------	---------	----------------------------------	------------------	---------------

##### Flag

Longitud: 1 byte.

Todo mensaje debe estar delimitado mediante dos Flag al comienzo y al final del mismo. Se denomina Flag a un carácter de valor fijo e igual a 7E (hexadecimal).

##### Dirección esclavo

Longitud: 1 byte.

En todos los mensajes este campo indica la dirección del esclavo, entre 1 y 250. Las direcciones 0 y 251 a 255 están reservadas.

##### Control

Longitud: 1 byte

Este campo clasifica las tramas en tres tipos:

- Control.
- Supervisión.
- Información.

De los tres tipos sólo la trama de información contiene un campo de información dentro del mensaje. En el resto todos los mensajes se componen de 6 bytes (no incluyen el campo de información).

A continuación se muestra una tabla (Tabla No.3) con todas las funciones:

Función	Tipo de trama	Código (campo de control)	Descripción
Modo de respuesta normal (SNRM)	Control M > E	93h	Se ordena al esclavo pasar al estado de respuesta normal (NRM)
Desconexión (DISC)	Control M > E	53h	Se ordena al esclavo pasar al estado de desconexión (NDM)
Reconocimiento no numerado (UA)	Control E > M	53h	Respuesta del esclavo indicando que ha recibido una orden válida estando en estado de desconexión.
Trama rechazada (FRMR)	Control E > M	97h	Respuesta del esclavo indicando que ha recibido una orden incorrecta estando en estado normal (NRM)
Consulta o test ( <i>polling</i> )	Supervisión M > E	RRR10001 (binario)	RRR=n° de secuencias anteriores recibidas como correctas El maestro indica que el esclavo debe contestar como consulta o test, respondiendo con RR o RNR.
Receptor dispuesto (RR)	Supervisión E > M	RRR10001 (binario)	RRR=n° de secuencias anteriores recibidas como correctas Respuesta del esclavo indicando que la consulta es correcta y que no tiene datos que transmitir.
Receptor no dispuesto (RNR)	Supervisión E > M	RRR10101 (binario)	RRR=n° de secuencias anteriores recibidas como correctas Respuesta del esclavo indicando que la consulta es correcta pero que no puede aceptarla por tener el buffer lleno.
Información (I)	Información M > E E > M	RRR1EEEE0 (binario)	RRR=n° de secuencias anteriores recibidas como correctas EEE=n° de secuencias enviadas Tramas normales de intercambio de información. En cada trama se comprueba los números de secuencia para evitar duplicidad de mensajes y detectar la pérdida de tramas o errores de transmisión.

**Información**

Longitud: máximo 250 bytes

Este campo es de longitud variable y sólo existe en las tramas de información.

**CRC**

Longitud: 2 bytes

El CRC es un conjunto de 16 bits que sirven para detectar errores de transmisión. Los dos bytes se obtienen mediante un polinomio H4 del tipo  $(XE16 + XE12 + XE5 + 1)$ .

**Trama del campo de información**

El campo de información de la trama obedece a un formato que especifica un mínimo de 7 bytes y un máximo de 250 (aunque se acepta como dispositivo estándar aquel que permite entre 7 y 20 bytes de longitud). Los bytes se corresponden con el siguiente formato:

Byte	Descripción
1	Longitud de información
2	MT - SE - DE - TR - 4 bits de reserva
3	Dirección esclavo
4	Tarea fuente - Tarea destino
5	Tareas usuario / Errores
6 en adelante (hasta byte 250)	Otros datos (Mínimo 2 bytes)

**Longitud de información:** Indica la longitud del campo de información (entre 7 y 250).

**Tipo de mensaje (MT):** 0 = orden 1 = respuesta

**Fuente de la orden (SE):** Indica si la fuente de una orden o el destino de una respuesta es:

0 = bloque maestro 1 = bloque de expansión E/S de éste

**Destino de la orden (DE):** Indica si el destino de una orden o la fuente de una respuesta es:

0 = bloque esclavo 1 = bloque de expansión E/S de éste

**Pista (TR):** 0 = mensaje de maestro a esclavo 1 = respuesta de esclavo a maestro

**4 bits reservados:** Se reservan para futuras ampliaciones, deben ser puestos a 0 al enviar el mensaje.

**Dirección esclavo:** El valor debe estar comprendido entre 1 y 250 (como ya se ha comentado anteriormente).

### Codificación de tareas

Este byte se compone de dos grupos de 4 bits:

Tarea fuente (4 bits altos): las tareas 12 a 15 están libres y pueden ser definidas por el usuario.

La tarea 0 está reservada a los servicios RAC (ver tabla adjunta) y las tareas 1 a 11 están reservadas por Intel.

Tarea destino (4 bits altos): definibles por el usuario (salvo que la tarea fuente sea la 0).

La tarea 0 o RAC (*Remote Access and Control*) proporciona una serie de funciones que todo dispositivo BITBUS debe soportar:

Código	Tipo	Tarea
00h	Control	Reset esclavo
01h	Control	Llamar tarea programada en un esclavo
02h	Control	Finalizar tarea
03h	Control	Obtener identificador/puntero de la función.
04h	Control	Habilitar/deshabilitar el resto de tareas (excepto RAC) en un esclavo.
05h	Acceso	Leer 1 byte de E/S
06h	Acceso	Escribir 1 byte de E/S
07h	Acceso	Actualizar líneas de E/S
08h	Acceso	Leer n bytes de la memoria del esclavo
09h	Acceso	Grabar n bytes en la memoria del esclavo
0Ah	Acceso	Operación O (OR) con byte de E/S
0Bh	Acceso	Operación Y (AND) con byte de E/S
0Ch	Acceso	Operación O-exclusiva (XOR) con byte de E/S
0Dh	Acceso	Leer registro de estado
0Eh	Acceso	Escribir registro de estado
0Fh a BFh	-	Funciones reservadas por INTEL
C0h a FFh	-	Funciones definibles por el usuario



### Tareas usuario/Errores

Este byte, en los mensajes de órdenes de maestro a esclavo, contendrá los datos necesarios para las subfunciones definidas por el usuario. En los mensajes de respuesta contendrá los códigos de error.

La siguiente tabla muestra los códigos de error que contempla el estándar y señala aquellos definibles por el usuario:

Código	Error
00h	No hay error
01h a 7Fh	Errores definidos por el usuario
80h	No se encuentra la tarea destino
81h	Imposible iniciar tarea debido a que se está realizando otra
82h	Imposible crear tarea por falta de banco de registros
83h	Solicitud de tarea ya activa
84h	Imposible iniciar tarea por falta de memoria
85h a 90h	Reservado por Intel
91h	Error de protocolo
92h	Reservado por Intel
93h	El nodo de destino no responde
94h	Reservado por Intel
95h	Tareas deshabilitadas por RAC
96h	Orden RAC desconocida
97h a FFh	Reservado por Intel

### Datos

Estos bytes están libres para uso general, pero al menos deben existir los bytes 6 y 7 en cualquier trama que tenga campo de información.

### Registros de estado y contadores de secuencia

Todo esclavo posee un registro que indica su estado dentro de los dos posibles:

- **Modo de respuesta normal (NRM):** en este modo el esclavo puede intercambiar mensajes con el maestro normalmente.
- **Modo de desconexión (NDM):** en este modo el esclavo no puede intercambiar mensajes con el maestro. Un esclavo pasa a este modo tras un

reset (inicio) del sistema o cuando detecta un error de sincronización o una trama que no puede interpretar. Para pasar al modo NRM se requiere una inicialización por parte del maestro.

Cada esclavo dispone, además, de un contador de intercambios que es comprobado con cada intercambio (excepto en tramas de control) y permite detectar errores de interpretación o pérdida de una trama.

El maestro mantiene una tabla con los registros de estado y los contadores de intercambio de todos los esclavos.

## IV.6 PROFIBUS

Profibus es un bus de campo abierto independiente del fabricante. Su área de aplicación abarca manufacturación, procesos y automatización de edificios. La independencia del fabricante y el ser un sistema abierto está garantizada por el estándar Profibus EN 50 170. Con profibus los dispositivos de diferentes fabricantes pueden comunicarse sin necesidad de adaptaciones mediante interfaces especiales, puede ser empleado tanto para transmisiones de datos de alta velocidad, en las aplicaciones en las que el tiempo de respuesta de las comunicaciones es crítico, como para tareas intensivas de comunicación compleja que involucren un gran número de necesidades de comunicación.

La familia Profibus consiste en tres versiones compatibles:

### IV.6.1 PROFIBUS-DP

Optimizado para aplicaciones de alta velocidad y bajo costo. Esta versión de Profibus está diseñada especialmente para comunicación entre sistemas automáticos de control y E/S distribuidos a nivel de campo. Puede ser empleado para reemplazar transmisiones bucles de señales con 24V o de 0 a 20mA.

### IV.6.2 PROFIBUS-PA

Está especialmente diseñado para automatización en la industria de procesos. Su principal diferencia con PROFIBUS-DP es que la capa física permite que sensores y actuadores puedan ser conectados a un bus común en áreas intrínsecas de seguridad. Permite comunicación de datos y la alimentación de los equipos sobre el mismo bus empleando tecnología de dos cables, acorde con el estándar internacional IEC 1158-2.

### IV.6.3 PROFIBUS-FMS

Es la solución de propósito general para tareas de comunicación a nivel de célula. Los potentes servicios de PROFIBUS-FMS abren un amplio rango de aplicaciones y proveen gran flexibilidad. También puede ser empleado para tareas de comunicaciones extensas y complejas.

Subfamilia	Principal aplicación	Principal ventaja	Características más relevantes
PROFIBUS-FMS	Automatización para propósitos generales	Universal	Gran variedad de aplicaciones Comunicaciones multimaestro
PROFIBUS-DP	Automatización de factorías	Rápido	<i>Plug and Play</i> Eficiente y efectivo en costo
PROFIBUS-PA	Automatización de procesos	Orientado a aplicación	Suministro de energía a través del propio bus Seguridad intrínseca

### IV.6.4 ESTRUCTURA BÁSICA

Profibus especifica las características técnicas y funcionales de un sistema basado en un bus de campo en el que controladores digitales descentralizados pueden ser conectados entre sí desde el nivel de campo al nivel de control. Se distinguen dos tipos de dispositivos:

- **Dispositivos maestros:** determinan la comunicación de datos a través del bus. Un maestro puede enviar mensajes sin necesidad de recibir una petición externa para que lo haga cuando mantiene el control de acceso al bus (la señal). Los maestros también se denominan **estaciones activas** en el protocolo Profibus.
- **Dispositivos esclavos:** son dispositivos periféricos. Los esclavos son normalmente dispositivos de E/S, válvulas, actuadores y transmisores de señal. No tienen capacidad para acceder directamente al bus y sólo pueden recibir mensajes, enviar mensajes al maestro cuando son permitidos para ello o enviar acuses de recibo de mensajes enviados por algún maestro. Los esclavos también son denominados **estaciones pasivas**. Por todo lo anterior

sólo necesitan una parte del protocolo del bus, siendo su implantación particularmente económica.

#### IV.6.5 ARQUITECTURA DE PROTOCOLOS

La arquitectura del protocolo PROFIBUS se basa en el modelo de referencia OSI, de acuerdo con el estándar ISO 7498.

PROFIBUS-DP define la capa física y de enlace, así como el interfaz de usuario. El DDML (*Direct Data Link Mapper*) proporciona una interfaz de usuario sencillo para el acceso a la capa 2, como medio físico se usa la tecnología RS-485, fibra óptica o ambas.

En PROFIBUS-FMS se definen las capas física, de enlace y aplicación, donde la capa de aplicación consiste en el FMS (*Fieldbus Message Specification*) y el LLI (*Lower Layer Interface*). El FMS contiene un protocolo de aplicación que proporciona al usuario un amplio conjunto de servicios. LLI permite proporcionar a FMS una interfaz independiente del dispositivo con la capa de enlace, dicha capa implementa el protocolo de acceso al bus y la seguridad de datos.

PROFIBUS-PA utiliza el protocolo de PROFIBUS-DP y le añade como característica particular la definición de los perfiles de dispositivo. 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, y por su parte PROFIBUS-DP y PROFIBUS-FMS usan las mismas tecnologías de transmisión y un protocolo uniforme de acceso al medio, por ello, ambas pueden operar simultáneamente sobre el mismo cable.

#### IV.6.6 CONTROL DE ACCESO AL MEDIO EN PROFIBUS

Las tres versiones de PROFIBUS usan el mismo control de acceso al medio (Fig. 19), incluyendo los aspectos relacionados con la seguridad de los datos y el manejo de los protocolos de transmisión y los telegramas. En PROFIBUS, la capa 2 se denomina FDL (*Fieldbus Data Link*), en el MAC solo una estación tiene derecho a transmitir en cada momento. Ha sido diseñado para cumplir dos objetivos:

- En las comunicaciones entre sistemas activos (maestros), encargados de tareas de control complejas, debe asegurarse que cada estación tenga suficiente tiempo para ejecutar sus tareas de comunicación dentro de un intervalo de tiempo definido.

- Las tareas de comunicación cíclicas se implementarán de la forma más sencilla posible para permitir la comunicación entre un maestro y uno o varios esclavos.

Por tanto, el control de acceso al medio de PROFIBUS 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 casa maestro y su periferia.

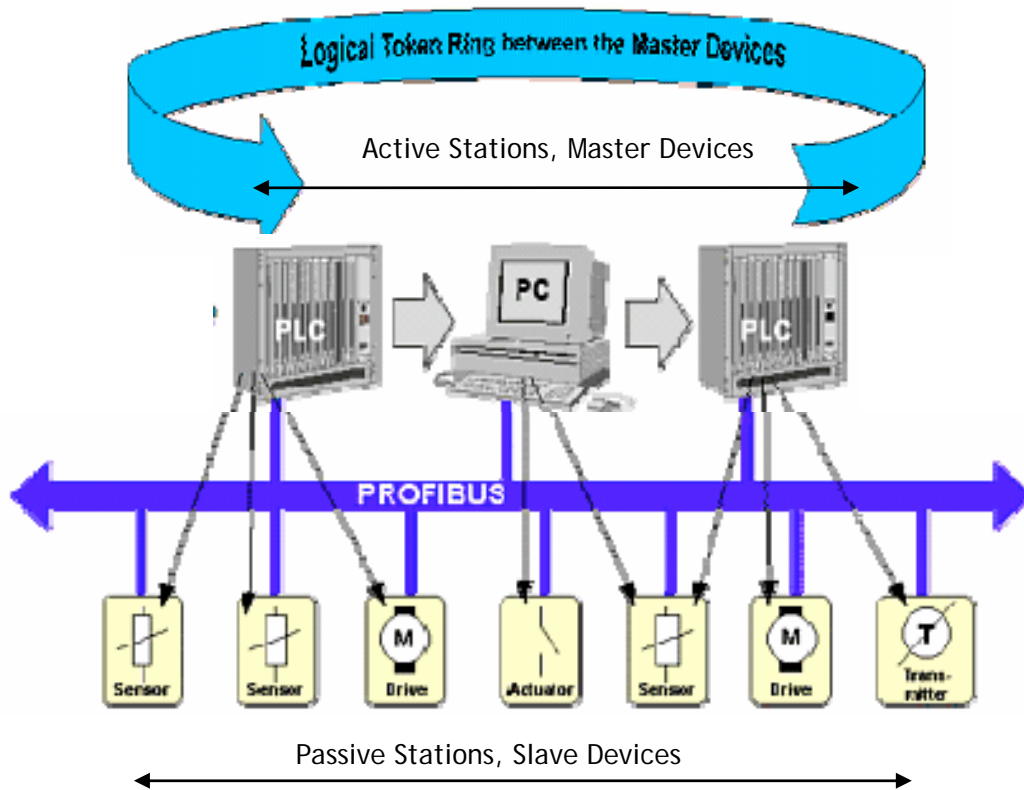


Fig. 19. Control de Acceso al Medio de PROFIBUS.

El mecanismo de paso de testigo garantiza el derecho a acceder al bus de cada maestro durante un determinado periodo de tiempo. El paso de testigo es un telegrama especial que permite la cesión al nodo que lo recibe, del derecho a acceder al bus. El testigo sigue una secuencia según un anillo lógico, con un tiempo máximo predeterminado para la rotación completa del testigo.

La comunicación maestro-esclavo permite que el maestro que posee el testigo en un instante determinado se comunique con los esclavos que dependan de él. El maestro puede enviar mensajes a los esclavos y leer las contestaciones de éstos. 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.

## Capítulo V. PROTOCOLOS

En este capítulo se desarrollarán los siguientes protocolos:

- MODBUS
- CAN
- ETHERNET
- DNP3

### V.1 MODBUS

La designación Modbus Modicon corresponde a una marca registrada por Gould Inc. Como en tantos otros casos, la designación no corresponde propiamente al estándar de red, incluyendo todos los aspectos desde el nivel físico hasta el de aplicación, sino a un protocolo de enlace (nivel OSI 2). Puede, por tanto, implementarse con diversos tipos de conexión física y cada fabricante suele suministrar un software de aplicación propio, que permite parametrizar sus productos.

El lenguaje común utilizado por todos los controladores Modicon es el protocolo Modbus. Este protocolo define una estructura de mensaje que los controladores reconocerán y usarán, con independencia del tipo de redes sobre la que comuniquen. Describe el proceso que usa un controlador para pedir acceso a otro dispositivo, cómo responderá a las peticiones desde otros dispositivos y cómo se detectarán y notificarán los errores. Establece un formato común para la disposición y contenido de los campos de mensaje.

Se suele hablar de MODBUS como un estándar de bus de campo, cuyas características esenciales son las que se detallan a continuación.

#### V.1.1 ESTRUCTURA DE LA RED

La estructura de la red esta dividida en dos partes: el medio físico y el acceso al medio.

##### V.1.1.1 MEDIO FÍSICO

El medio físico de conexión puede ser un bus semiduplex (*half duplex*) (RS-485 o fibra óptica) o dúplex (*full duplex*) (RS-422, BC 0-20mA o fibra óptica).

La comunicación es asíncrona y las velocidades de transmisión previstas van desde los 75 baudios a 19.200 baudios.

La máxima distancia entre estaciones depende del nivel físico, pudiendo alcanzar hasta 1200 m sin repetidores.

#### V.1.1.2 ACCESO AL MEDIO

La estructura lógica es del tipo maestro-esclavo, con acceso al medio controlado por el maestro.

El número máximo de estaciones previsto es de 63 esclavos más una estación maestra.

Los intercambios de mensajes pueden ser de dos tipos:

- **Intercambios punto a punto:** se conforman siempre de dos mensajes: una demanda del maestro y una respuesta del esclavo (puede ser simplemente un reconocimiento "*acknowledge*").
- **Menajes difundidos:** estos consisten en una comunicación unidireccional del maestro a todos los esclavos. Este tipo de mensajes no tiene respuesta por parte de los esclavos y se suelen emplear para mandar datos comunes de configuración, reset, etcétera.

#### V.1.2 PROTOCOLO

La Figura 20 muestra cómo se pueden interconectar los dispositivos en una jerarquía de redes que emplean técnicas de comunicación que difieren ampliamente. En la transacción de mensajes, el protocolo Modbus integrado en la estructura de paquetes de cada red proporciona el lenguaje común por el cual los dispositivos pueden intercambiar datos.

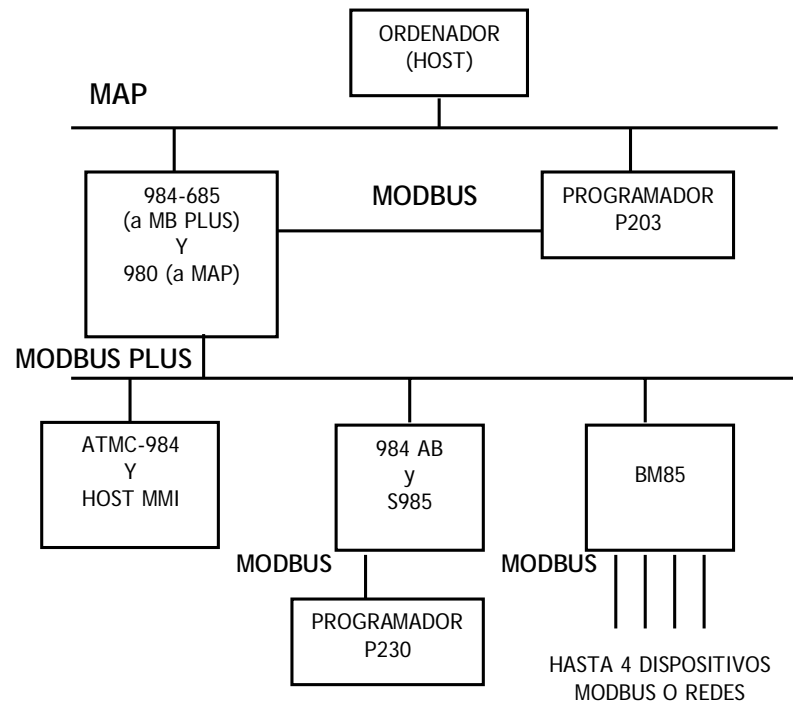


Fig. 20. Vista general de aplicación del Protocolo Modbus.

### V.1.3 TRANSACCIONES SOBRE REDES MODBUS

Los controladores se comunican usando una técnica maestro - esclavo, en la cual sólo un dispositivo (el maestro) puede iniciar transacciones (llamadas peticiones *queries*). Los otros dispositivos (los esclavos) responden suministrando al maestro el dato solicitado, o realizando la acción solicitada en la petición. Entre los dispositivos maestros típicos se incluyen los procesadores centrales y los paneles de programación. Los esclavos típicos son los PLC's.

El maestro puede direccionar esclavos individualmente o puede generar un mensaje en modo difusión a todos los esclavos. Los esclavos devuelven un mensaje (llamado respuesta) a las peticiones que les son direccionadas individualmente. No se devuelven respuestas a peticiones en modo difusión enviadas desde el maestro.

El protocolo Modbus establece el formato para la petición del maestro, colocando en ella la dirección del dispositivo esclavo (0 en caso de difusión), un código de función que define la acción solicitada, cualquier dato que haya de enviarse y un campo de comprobación de error. El mensaje de respuesta del esclavo está también definido por el protocolo Modbus. Contiene campos



confirmando la acción tomada, cualquier dato que haya de devolverse y un campo de comprobación de error. Si el mensaje recibido por el esclavo es defectuoso o el esclavo es incapaz de realizar la acción solicitada, construirá un mensaje de error y lo enviará como respuesta.

#### V.1.4 MODOS DE TRANSMISIÓN EN SERIE

Los controladores pueden ser configurados para comunicar sobre redes estándar Modbus utilizando cualquiera de los dos modos de transmisión: ASCII o RTU. Los usuarios seleccionan el modo deseado, junto con los parámetros de comunicación del puerto serie como por ejemplo velocidad y paridad, durante la configuración de cada controlador. El modo y los parámetros serie deben ser los mismos para todos los dispositivos conectados a una red Modbus.

La selección del modo ASCII o RTU tiene que ver únicamente con redes Modbus estándar y esto define los bits contenidos en los campos del mensaje transmitido en serie en esas redes, así se determina cómo debe ser empaquetada y decodificada la información en los campos del mensaje.

##### V.1.4.1 MODO ASCII

Cuando los controladores se configuran para comunicar en una red Modbus según el modo ASCII (*American Standard Code for Information Interchange*), cada byte (8 bits) en un mensaje se envía como dos caracteres ASCII. La principal ventaja de este modo es que permite intervalos de tiempo de hasta un segundo entre caracteres sin dar lugar a error. El formato para cada byte en modo ASCII es:

<b>Sistema de codificación:</b>	Hexadecimal, caracteres ASCII 0-9, A-F. Un carácter hexadecimal contenido en cada carácter ASCII del mensaje
<b>Bits por byte:</b>	1 bit de arranque. 7 bits de datos, el menos significativo se envía primero. 1 bit para paridad Par o Impar; ningún bit para No paridad. 1 bit de paro si se usa paridad; 2 bits si no se usa paridad
<b>Campo de Comprobación de error:</b>	Comprobación Longitudinal Redundante (LRC).

#### V.1.4.2 MODO RTU

Cuando los controladores son configurados para comunicar en una red Modbus usando el modo RTU (*Remote Terminal Unit*), cada byte en un mensaje contiene dos dígitos hexadecimales de 4 bits. La principal ventaja de este modo es que su mayor densidad de caracteres permite mejor rendimiento que el modo ASCII para la misma velocidad. Cada mensaje debe ser transmitido en un flujo continuo. El formato para cada byte en modo RTU es:

**Sistema de codificación:** Binario 8-bits, hexadecimal 0-9, A-F.  
Dos dígitos hexadecimales contenidos en cada campo de 8 bits del mensaje.

**Bits por byte:** 1 bit de arranque.  
8 bits de datos, el menos significativo se envía primero.  
1 bit para paridad Par o Impar; ningún bit para No paridad.  
1 bit de paro si se usa paridad; 2 bits si no se usa paridad

**Campo de Comprobación de error:** Comprobación Cíclica Redundante (CRC).

#### V.1.5 TRAMA DEL MENSAJE MODBUS

En cualquiera de los modos de transmisión en serie (ASCII o RTU), un mensaje es situado por el dispositivo que transmite en una trama que tiene un comienzo y un final conocidos. Esto permite a los dispositivos receptores comenzar en el arranque del mensaje, leer la parte de la dirección y determinar qué dispositivo es direccionado (o todos los dispositivos si es una difusión dirección = 0) y conocer cuándo se ha completado el mensaje.

Mensajes parciales pueden ser detectados y establecer errores como resultado.

El protocolo de red manipula la trama de los mensajes con delimitadores de comienzo y final que son específicos de la red. Esos protocolos también manipulan el envío al dispositivo de destino, haciendo innecesario el campo de la dirección Modbus integrado en el mensaje para la transmisión actual. (La dirección modbus es convertida a una dirección de nodo de la red y enrutada por el controlador remitente o sus adaptadores de red.)

### V.1.5.1 TRAMA ASCII

En modo ASCII, los mensajes comienzan con un carácter ( : ) 'dos puntos' (ASCII 3A hex) y terminan con un par de caracteres (CRLF) 'Retorno de Carro + Avance de Línea' (ASCII 0D hex y 0A hex) (Fig. 21).

Los caracteres a transmitir permitidos para todos los demás campos son 0-A, A-F hexadecimal. Los dispositivos conectados en red monitorizan el bus de red continuamente para detectar un carácter 'dos puntos'. Cuando se recibe, cada dispositivo decodifica el próximo campo (el campo de dirección) para enterarse si es el dispositivo direccionado.

Pueden haber intervalos de hasta un segundo entre caracteres dentro del mensaje. Si transcurre más tiempo entre caracteres, el dispositivo receptor asume que ha ocurrido un error.

Se muestra debajo una trama de mensaje típica.

ARRANQUE	DIRECCIÓN	FUNCIÓN	DATOS	COMPROB LRC	FINAL
1 carácter :	2 caracteres	2 caracteres	N caracteres	2 caracteres	2 caracteres CRLF

Fig. 21. Trama del Mensaje ASCII.

**Excepción:** Con los controladores 584 y 984A/B/X, un mensaje ASCII puede terminar normalmente después del campo LRC sin enviar los caracteres CRLF. En ese caso, debe tener lugar una pausa de al menos 1 segundo. Si esto sucede, el controlador asumirá que el mensaje ha terminado normalmente.

### V.1.5.2 TRAMA RTU

En modo RTU, los mensajes comienzan con un intervalo silencioso de al menos 3.5 tiempos de carácter. Esto es más fácilmente implementado como un múltiplo de tiempos de carácter a la velocidad de transmisión configurada en la red (mostrado como T1-T2-T3-T4 en la Figura 22). El primer campo transmitido es entonces la dirección del dispositivo destinatario.

Los caracteres a transmitir permitidos para todos los campos son 0-A, A-F hexadecimal. Los dispositivos conectados en red monitorizan el bus de red continuamente incluso durante los intervalos 'silencioso'. Cuando el primer campo (el campo de dirección) es recibido, cada dispositivo lo decodifica para enterarse si es el dispositivo direccionado.

Seguindo al último carácter transmitido, un intervalo de al menos 3.5 tiempos de carácter señala el final del mensaje. Un nuevo mensaje puede comenzar después de este intervalo.

La trama completa del mensaje debe ser transmitida como un flujo continuo. Si un intervalo silencioso de más de 1.5 tiempos de carácter tiene lugar antes de completar la trama, el dispositivo receptor desecha el mensaje incompleto y asume que el próximo byte será el campo de dirección de un nuevo mensaje.

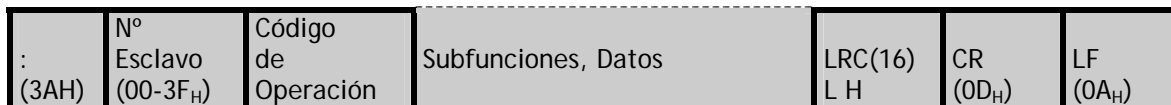
De forma similar, si un nuevo mensaje comienza antes de que transcurran 3.5 tiempos de carácter después de un mensaje previo, el dispositivo receptor lo considerará una continuación del mensaje previo. Esto dará lugar a un error, ya que el valor en el campo final CRC no será válido para el mensaje combinado.

Enseguida se muestra una trama de mensaje típica.

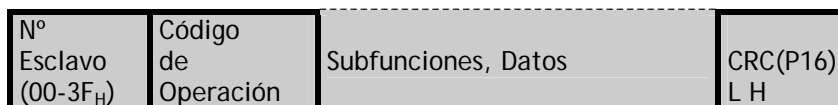
ARRANQUE	DIRECCIÓN	FUNCIÓN	DATOS	COMPROB LRC	FINAL
T1-T2-T3-T4	8 BITS	8 BITS	N x 8 BITS	16 BITS	T1-T2-T3-T4

Fig. 22. Trama del Mensaje RTU.

La codificación de datos dentro de la trama puede hacerse en modo ASCII o puramente binario, según el estándar RTU (*Remote Transmission Unit*). En cualquiera de los dos casos, cada mensaje obedece a una trama que contiene cuatro campos principales, según se muestra en la Figura 23. La única diferencia estriba en que la trama ASCII incluye un carácter de encabezamiento (":"=3AH) y los caracteres CR y LF al final del mensaje. Pueden existir también diferencias en la forma de calcular el CRC, puesto que el formato RTU emplea una fórmula polinómica en vez de la simple suma en módulo 16. Con independencia de estos pequeños detalles, a continuación se da una breve descripción de cada uno de los campos del mensaje:



Codificación ASCII



Codificación RTU

Figura 23. Trama genérica del mensaje según el código empleado

**Número de esclavo (1 byte):** permite direccionar máximo 63 esclavos con direcciones que van del 01h hasta 3fh. El número 00h se reserva para los mensajes difundidos.

**Código de operación o función (1 byte):** cada función permite transmitir datos u órdenes al esclavo. Existen dos tipos básicos de órdenes:

- Ordenes de lectura / escritura de datos en los registros o en la memoria del esclavo.
- Ordenes de control del esclavo y el propio sistema de comunicaciones (RUN/STOP, carga y descarga de programas, verificación de contadores de intercambio, entre otros)

La tabla No.8 muestra la lista de funciones disponibles en el protocolo MODBUS con sus correspondientes códigos de operación.

**Campo de subfunciones/datos (n bytes):** este campo suele contener, en primer lugar, los parámetros necesarios para ejecutar la función indicada por el byte anterior. Estos parámetros podrán ser códigos de subfunciones en el caso de órdenes de control (función 00h) o direcciones del primer bit o byte, número de bits o palabras a leer o escribir, valor del bit o palabra en caso de escritura, etcétera.

**Palabra de control de errores (2 bytes):** en código ASCII, esta palabra es simplemente la suma de comprobación (checksum) del mensaje en módulo 16 expresado en ASCII.

**Tabla No.8. Funciones básicas y códigos de operación**

Función	Código	Tarea
0	0 00 <sub>H</sub>	Control de estaciones esclavas
1	1 01 <sub>H</sub>	Lectura de <i>n</i> bits de salida o internos
2	2 02 <sub>H</sub>	Lectura de <i>n</i> bits de entradas
3	3 03 <sub>H</sub>	Lectura de <i>n</i> palabras de salidas o internos
4	4 04 <sub>H</sub>	Lectura de <i>n</i> palabras de entradas
5	5 05 <sub>H</sub>	Escritura de un bit
6	6 06 <sub>H</sub>	Escritura de una palabra
7	7 07 <sub>H</sub>	Lectura rápida de 8 bits
8	8 08 <sub>H</sub>	Control de contadores de diagnósticos número 1 a 8
9	9 09 <sub>H</sub>	No utilizado
10	10 0A <sub>H</sub>	No utilizado
11	11 0B <sub>H</sub>	Control del contador de diagnósticos número 9
12	12 0C <sub>H</sub>	No utilizado
13	13 0D <sub>H</sub>	No utilizado
14	14 0E <sub>H</sub>	No utilizado
15	15 0F <sub>H</sub>	Escritura de <i>n</i> bits
16	16 10 <sub>H</sub>	Escritura de <i>n</i> palabras

### V.1.6 VARIANTES DE MODBUS: JBUS

JBUS es una designación utilizada por la firma APRIL para un bus propio que presenta gran similitud con MODBUS, con protocolos prácticamente idénticos. La designación JBUS, de la misma forma que MODBUS, corresponde a un protocolo de enlace más que a una red propiamente dicha. Puede, por tanto, implementarse con cualquiera de las conexiones físicas normalizadas.

### V.1.7 COMPARACIÓN ENTRE JBUS Y MODBUS

La arquitectura de la red, el formato general de la trama y muchos de los códigos de función de ambos buses coinciden exactamente. Existen, sin embargo, algunos códigos de función cambiados, otros que presentan ligeras diferencias o funciones añadidas.

Como diferencias más relevantes citaremos las siguientes:

- Posee un registro de estado en cada estación que permite un diagnóstico de la estación.
- El número de esclavo para JBUS (1er byte de la trama) permite valores que van del 01H hasta el FFH. Permite, por tanto, direccionar 255 esclavos en vez de 63.  
El número 00H se reserva igualmente para mensajes difundidos.
- Las funciones disponibles son prácticamente las mismas en ambos protocolos, pero algunos códigos de función (2º byte de la trama) y de las subfunciones no coinciden.

**Tabla No.9. Funciones idénticas Modbus Jbus**

Función	Código	Tarea
0	01 <sub>H</sub>	Lectura de <i>n</i> bits de salida o internos
1	02 <sub>H</sub>	Lectura de <i>n</i> bits de entradas
2	03 <sub>H</sub>	Lectura de <i>n</i> palabras de salidas o internos
3	04 <sub>H</sub>	Lectura de <i>n</i> palabras de entradas
4	05 <sub>H</sub>	Escritura de un bit
5	06 <sub>H</sub>	Escritura de una palabra
6	07 <sub>H</sub>	Lectura rápida de 8 bits
7	0F <sub>H</sub>	Escritura de <i>n</i> bits
8	10 <sub>H</sub>	Escritura de <i>n</i> palabras

## V.2 CAN (*CONTROLLER AREA NETWORK*)

El protocolo CAN fue creado a mediados de la década de los 80 por la firma alemana Robert Bosch con la finalidad de interconectar diversos dispositivos inteligentes a bordo de un automóvil para que intercambien información a través de un bus de tipo serie. La idea principal era disminuir el cableado necesario para interconectar estos dispositivos entre sí al mismo tiempo que se aumentaba la confiabilidad de la comunicación.

En la actualidad, las aplicaciones de CAN exceden el ámbito puramente automotriz y puede encontrarse en ambientes industriales, equipos de medición y hasta equipamiento electromédico debido a su bajo costo, alto rendimiento y la disponibilidad del protocolo para varias puestas en práctica.

El protocolo está definido por el estándar ISO 11898 y se puede resumir de la siguiente manera:

- La capa física utiliza la transmisión diferencial mediante un cable de par trenzado.
- Los mensajes son pequeños (máximo de 8 bytes) y están protegidos por el CRC.
- En los mensajes no hay direcciones específicas, en lugar de eso cada mensaje lleva un valor numérico el cual controla la prioridad en el bus y también sirve como identificación del contenido del mensaje.
- Utilización de un esquema para el manejo de errores que retransmite los mismos cuando no son recibidos apropiadamente.
- Implantación de maneras para aislar los nodos que proveen errores del bus.

En el protocolo CAN se definen la Capa de Datos (*Data Link Layer*), en donde se describe cómo se transmiten y reciben los mensajes de datos, los mecanismos de *acknowledge*, sincronización y detección de errores, y parte de la Capa Física (*Physical Layer*) que describe cómo se transmiten las señales, aunque no se hace referencia al medio de transmisión utilizado.

El protocolo CAN se comunica mediante mensajes de longitud corta, como máximo, 94 bits sin especificar ninguna dirección de nodo, en lugar de esto, los mensajes contienen implícita su dirección.

## V.2.1 FRAMES

Existen 4 tipos de mensajes:

### V.2.1.1 Frame de Datos

El mensaje de Datos (*Frame* de Datos) (Fig. 24) es el tipo de mensajes más comunes puesto que engloba la mayoría de órdenes, comandos y datos que se transmiten. Existen 4 campos:

1. *El Campo de Arbitraje*: Determina la prioridad del Mensaje.
2. *Campo de Datos*: Contiene hasta 8 bytes de datos.
3. *CRC*: Contiene 15 bits de CRC.
4. *Slot de Acknowledge*: Se trata de un campo con el cual un nodo confirma que ha recibido correctamente el mensaje.

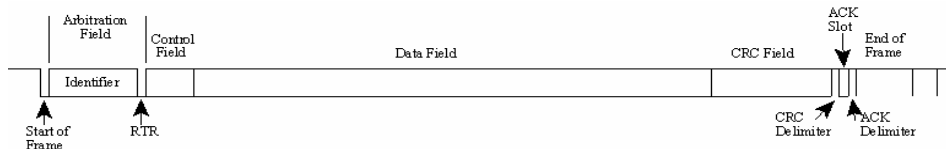


Fig. 24. Frame de Datos.

### V.2.1.2 Frame Remoto

El *frame* remoto es básicamente similar al *frame* de datos, con la excepción de que no contiene el campo de Datos de 8 bytes. El propósito del *frame* remoto es solicitar la transmisión del correspondiente *frame* de datos. Existe una característica destacable en este *frame* y es que se debe especificar exactamente la longitud del campo de datos del mensaje que se va a recibir, si esto no se cumple, no funcionará. (Fig. 25)

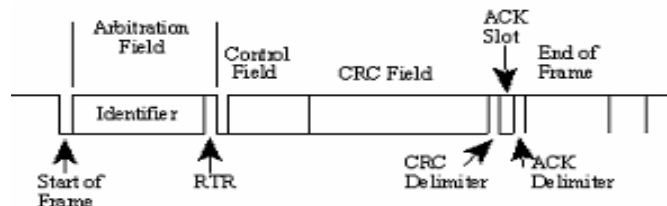


Fig. 25. Frame Remoto.

### V.2.1.3 Frame de Error

El *frame* de error es, simplemente, un mensaje que viola las reglas de transmisión de los mensajes CAN Cuando el transmisor de un mensaje recibe un



*frame* de error, inmediatamente vuelve a enviar el mensaje. Existe un método (que ya explicaremos) para evitar que un nodo genere excesivos mensajes de error y sature la red (Fig. 26).

El *frame* de error consiste en realidad en una bandera de error con un mensaje de 6 bits con el mismo valor, lo cual, viola el protocolo de NRZ y un delimitador de error de 8 bits. Este delimitador de errores es en realidad un campo donde el resto de nodos pueden incluir su bandera de errores cuando se detecta el primer *frame* de error.

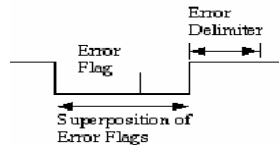


Fig. 26. Frame de Error.

#### V.2.1.4 Frame de Sobrecarga

El *frame* de sobrecarga es similar al *frame* de error y es transmitido por un nodo que comienza a estar demasiado ocupado. En la actualidad, este tipo de mensajes es poco utilizado, puesto que las redes actuales contienen nodos suficientemente rápidos como para procesar adecuadamente la información y no saturarse. De hecho solo un controlador ya obsoleto (el 82526) continúa utilizando este tipo de mensajes.

La velocidad máxima de transmisión es de 1Mbit/s. Este valor se aplica a redes de hasta 40 metros de longitud. A distancias mayores la velocidad disminuye: a distancias de 500m, la velocidad no puede exceder los 125 Kbit/s y a 1 Km., la velocidad máxima cae a 50 Kbit/s

Existen varias capas físicas en el protocolo CAN:

- La normativa ISO 11989 define un esquema de señal balanceada de dos vías.
- ISO 11519 para aplicaciones de baja velocidad define otro esquema de señal balanceado de dos vías para buses de baja velocidad.
- Las modificaciones del RS485 fueron utilizadas cuando los *drivers* del CAN todavía no habían sido implementados.
- SAE J2411 define una capa con una única vía de comunicación, aunque el estándar todavía no ha sido implantado.

Para la máxima velocidad establecida por el estándar podemos disponer de un cable de como máximo 10 metros, sin embargo, pueden crearse CAN de mayor longitud de cable.

A continuación mostramos una tabla de las máximas longitudes de cable y su consecuente velocidad máxima:

LONGITUD MÁXIMA	VELOCIDAD MÁXIMA
100 metros	500 Kbits/segundo
200 metros	250 Kbits/segundo
500 metros	125 Kbits/segundo
6 kilómetro	10 Kbits/segundo

El controlador CAN puede ajustar, reduciendo o ampliando, el tiempo de espera del reloj.

Existen dos tipos de sincronización:

- **Resynchronization:** Cuando un bit se transmite fuera del segmento de Sincronización del mensaje.
- **Hard synchronization:** El bit de tiempo se reinicia a cero.

Todo controlador CAN a lo largo de un bus puede tratar de detectar errores en un mensaje. Si uno de estos controladores descubre un error en un mensaje el nodo que lo descubre genera un mensaje de error y elimina el tráfico del bus.

El resto de nodos detectará el mensaje de error generado por el nodo y actuarán en consecuencia, normalmente eliminando el mensaje. Cada nodo mantiene dos contadores de error para lograr un mejor manejo de los errores.

## V.2.2 MECANISMOS DE DETECCIÓN DE ERRORES

El protocolo CAN incorpora 5 maneras diferentes de detectar errores. Dos de estas son a nivel de bit mientras que las otras tres son a nivel de mensaje:

### V.2.2.1 *Bit Monitoring*

Cada transmisor del bus controla el nivel de señal transmitido. Si el nivel del bit actualmente leído difiere del bit transmitido se genera un bit de error.

#### V.2.2.2 *Bit Stuffing*

Cuando se han transmitido 5 bits consecutivos de un mismo nivel (0 o 1) se añade un sexto bit con el nivel opuesto a la cadena de salida. El receptor eliminará este sexto bit al recibirlo. En caso de que este bit no sea del valor opuesto se generará el consecuente mensaje de error.

#### V.2.2.3 *Frame Check*

Algunas partes de los mensajes de datos transmitidos por el CAN contienen un formato prefijado, por ejemplo, el estándar define exactamente que niveles deben ocurrir y cuando. Estos niveles son el delimitador de CRC, el delimitador de *Acknowledge* y el delimitador de final de *frame*. Si un controlador detecta un valor inválido en uno de estos niveles se genera el mensaje de error.

#### V.2.2.4 *Acknowledge Check*

Todos los nodos del bus que reciben correctamente un mensaje envían a su vez un mensaje de *acknowledge* en el Slot de *Acknowledge* que anteriormente habíamos comentado.

#### V.2.2.5 *CRC (Cyclic Redundancy Check)*

Cada mensaje contiene un campo de 15 bits destinado al CRC y todo nodo que detecte un CRC en el mensaje que sea diferente del CRC que él ha calculado para el mensaje generará una señal de error.

Cada nodo dentro de un bus CAN contiene dos contadores de error: el Contador de Error de Transmisiones y el Contador de Recepción de Errores. Existen diferentes mecanismos para saber cómo y cuando incrementar o decrementar el valor de los contadores. En general, un transmisor que detecta un error incrementa su contador de Errores más rápidamente que el nodo receptor que detecta el mensaje.

Todos los nodos comienzan en un estado conocido como Estado de Error Activo. Cuando uno de los dos contadores de error supera los 127 errores, el nodo entra en un estado conocido como Estado de Error Pasivo y cuando el contador de Error de Transmisiones es mayor que 255 el nodo entra en estado de Bus *Off*.

El reglamento para el incremento de estos contadores es complejo pero responde a un principio muy sencillo. Transmitir un error se penaliza con 8 puntos y recibir un error con 1 punto. Recibir o Transmitir correctamente un mensaje se bonifica con la resta de 1 punto.

### V.3 ETHERNET

Ethernet es probablemente el estándar más popular para las redes de área local (LAN). A fines de 1996 más del 80% de las redes instaladas en el mundo eran Ethernet, esto representaba unos 120 millones de PCs interconectadas. El 20% restante utilizaban otros sistemas como *Token-Ring*, FDDI (*Fiber Distributed Data Interface*) y otros.

En una configuración Ethernet, los equipos están conectados mediante cable coaxial o de par trenzado (*Twisted-pair*) y compiten por acceso a la red utilizando un modelo denominado CSMA/CD Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (*Carrier Sense Multiple Access with Collision Detection*). Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor encada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos. Inicialmente podía manejar información a 10 Mb/s, aunque actualmente se han desarrollado estándares mucho más veloces.

Fue desarrollado inicialmente en 1973 por el Dr. Robert M. Metcalfe en el PARC (Palo Alto *Research Center*) de la compañía Xerox, como un sistema de red denominado Ethernet Experimental, que posteriormente sirvió como base de la especificación 802.3 publicada en 1980 por el *Institute of Electrical and Electronic Engineers* (IEEE).

Estos primeros trabajos del PARC contribuyeron substancialmente a la definición de la norma IEEE 802.3, que define el método de acceso CSMA/CD. En 1980 se propuso un estándar Ethernet a 10 Mbps (también conocido como 10Base), cuya especificación fue publicada conjuntamente por *Digital Equipment Corporation*, Intel y la propia Xerox. Por esta razón las primeras Ethernet eran denominadas DIX (Digital Intel Xerox); también "Libro azul", por el color de la primera edición. Los primeros productos comenzaron a comercializarse en 1981.

Además de las tecnologías a 10 Mbps, se han desarrollado extensiones de la norma que aumentan la velocidad de transmisión: la conocida como 100Base a 100 Mbps; Gigabit Ethernet a 1000 Mbps y 10 Gigabit Ethernet

A partir de 1982, Ethernet fue gradualmente adoptada por la mayoría de los organismos de estandarización:

ECMA European Computer Manufacturers Association  
IEEE Institute of Electrical and Electronics Engineers  
NIST National Institute of Standards and Technology

ANSI American National Standards Institute  
ISO International Standards Organization

Desde entonces Ethernet se ha convertido en la tecnología LAN más popular. Aunque comenzó a utilizarse en ambientes de ingeniería y de fabricación, se expandió rápidamente a los mercados comercial y gubernamental. La segunda generación de Ethernet, que se usa actualmente, es Ethernet II, aunque este nombre se usa raramente.

Otros organismos que tienen gran influencia en el establecimiento de normas para la industria de redes y telecomunicaciones son:

EIA (*Electronic Industries Alliance*) Asociación de Industrial Electrónicas  
TIA (*Telecommunications Industry Association*) Asociación de las industrias de telecomunicaciones.

Estas dos asociaciones editan normas de forma conjunta, que se conocen como normas TIA/EIA; son las de mayor influencia en el diseño e instalación de redes.

### V.3.1 TECNOLOGÍA ETHERNET

Las redes Ethernet son de carácter no determinista, en la que los *hosts* pueden transmitir datos en cualquier momento. Antes de enviarlos, escuchan el medio de transmisión para determinar si se encuentra en uso. Si lo está, entonces esperan. En caso contrario, los host comienzan a transmitir. En caso de que dos o más host empiecen a transmitir tramas a la vez se producirán encontronazos o choques entre tramas diferentes que quieren pasar por el mismo sitio a la vez. Este fenómeno se denomina **colisión**, y la porción de los medios de red donde se producen colisiones se denomina **dominio de colisiones**.

Una colisión se produce pues cuando dos máquinas escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde.

Para intentar solventar esta pérdida de paquetes, las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación que determinan el momento en que aquellas que han enviado tramas que han sido destruidas por colisiones pueden volver a transmitir las.

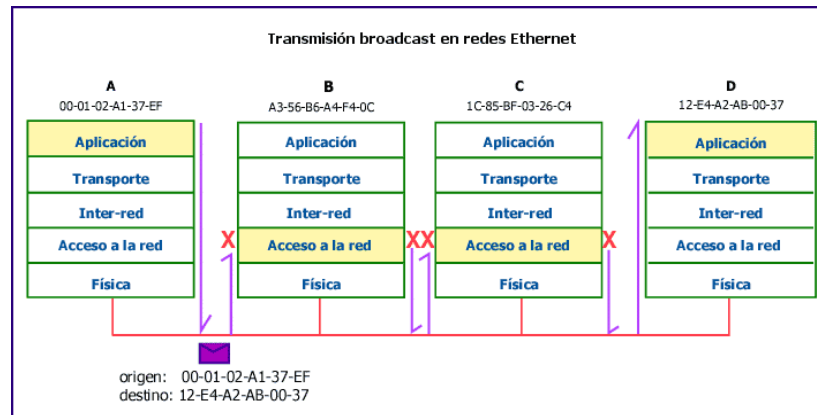


Fig. 27. Transmisión Broadcast.

Existen dos especificaciones diferentes para un mismo tipo de red, Ethernet y IEEE 802.3. Ambas son **redes de broadcast** (Fig. 27), lo que significa que cada máquina puede ver todas las tramas, aunque no sea el destino final de las mismas. Cada máquina examina cada trama que circula por la red para determinar si está destinada a ella. De ser así, la trama pasa a las capas superiores para su adecuado procesamiento. En caso contrario, la trama es ignorada.

Ethernet proporciona servicios correspondientes a las capas física y de enlace de datos del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física y la porción de acceso al canal de la capa de enlace de datos, pero no define ningún protocolo de Control de Enlace Lógico.

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos.
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
3. Detectar errores dentro de los paquetes de datos o en la red.

Tanto Ethernet como IEEE 802.3 se implementan a través de la **tarjeta de red** o por medio de circuitos en una placa dentro del host.

Existen por lo menos 18 variedades de Ethernet, relacionadas con el tipo de cableado empleado y con la velocidad de transmisión.

Variedades de red Ethernet

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

Las tecnologías Ethernet más comunes y más importantes las son:

- **Ethernet 10Base2.** Usa un cable coaxial delgado, por lo que se puede doblar más fácilmente, y además es más barato y fácil de instalar, aunque los segmentos de cable no pueden exceder de 200 metros y 30 nodos. Las conexiones se hacen mediante conectores en T, más fáciles de instalar y más seguros.
- **Ethernet 10Base5.** También llamada Ethernet gruesa, usa un cable coaxial grueso, consiguiendo una velocidad de 10 Mbps. Puede tener hasta 100 nodos conectados, con una longitud de cable de hasta 500 metros. Las conexiones se hacen mediante la técnica denominada *derivaciones de vampiro*, en las cuales se inserta un polo hasta la mitad del cable, realizándose la derivación en el interior de un transmisor-receptor, que contiene los elementos necesarios para la detección de portadores y choques. El transmisor-receptor se une al computador mediante un cable de hasta 50 metros.
- **Ethernet 10Base-T.** Cada estación tiene una conexión con un hub central, y los cables usados son normalmente de par trenzado. Son las LAN más comunes hoy en día. Mediante este sistema se palian los conocidos defectos de las redes 10Base2 y 10Base5, a saber, la mala detección de derivaciones no deseadas, de rupturas y de conectores flojos. Como desventaja, los cables tienen un límite de sólo 100 metros, y los hubs pueden resultar caros.
- **Ethernet 10Base-FX.** Basada en el uso de fibra óptica para conectar las máquinas, lo que la hace cara para un planteamiento general de toda la red, pero idónea para la conexión entre edificios, ya que los segmentos pueden

tener una longitud de hasta 2000 metros, al ser la fibra óptica insensible a los ruidos e interferencias típicos de los cables de cobre. Además, su velocidad de transmisión es mucho mayor.

- **Fast Ethernet.** Las redes 100BaseFx (IEEE 802.3u) se crearon con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10Base-T y buscar una alternativa a las redes FDDI. Son también conocidas como redes *Fast Ethernet*, y están basadas en una topología en estrella para fibra óptica. Con objeto de hacerla compatible con Ethernet 10Base-T, la tecnología *Fast Ethernet* preserva los formatos de los paquetes y las interfaces, pero aumenta la rapidez de transmisión hasta los 100 Mbps. En las redes *Fast Ethernet* se usan cables de cuatro pares trenzados de la clase 3, uno de los cuales va siempre al hub central, otro viene siempre desde el hub, mientras que los otros dos pares son conmutables. En cuanto a la codificación de las señales, se sustituye la codificación Manchester por señalización ternaria, mediante la cual se pueden transmitir 4 bits a la vez. También se puede implementar *Fast Ethernet* con cableado de la clase 5 en topología de estrella (100BaseTX), pudiendo entonces soportar hasta 100 Mbps con transmisión full dúplex.

### V.3.2 FORMATO DE TRAMA ETHERNET

Según hemos visto, los datos generados en la capa de aplicación pasan a la capa de transporte, que los divide en segmentos, porciones de datos aptas para su transporte por red, y luego van descendiendo por las sucesivas capas hasta llegar a los medios físicos. Conforme los datos van bajando por la pila de capas, paso a paso cada protocolo les va añadiendo una serie de cabeceras y datos adicionales; necesarios para poder ser enviados a su destino correctamente. El resultado final es una serie de unidades de información denominadas tramas, que son las que viajan de un host a otro.

La forma final de la trama obtenida, en redes Ethernet, es la siguiente:

Trama Ethernet

Cabecera Ethernet	Cabecera IP (20 bytes)	Cabecera TCP (20 bytes)	Datos	Checksum Ethernet
-------------------	---------------------------	----------------------------	-------	-------------------



Y los principales campos que la forman son:

**Campos de la trama Ethernet**

?	1	6	6	2	46-1500	4
Preámbulo	Inicio de delimitador de trama	Dirección Destino	Dirección Origen	Tipo	Datos	Secuencia de verificación de trama

- **Preámbulo:** Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.
- **Inicio de trama (SOF):** Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.
- **Direcciones destino y origen:** Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).
- **Tipo (Ethernet):** Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.
- **Longitud (IEEE 802.3):** Indica la cantidad de bytes de datos que sigue este campo.
- **Datos:** Incluye los datos enviados en la trama. En las especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.
- **Secuencia de verificación de trama (FCS):** Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

### V.3.3 ARQUITECTURA (ESTRUCTURA LÓGICA)

La arquitectura Ethernet puede definirse como una red de conmutación de paquetes de acceso múltiple y difusión amplia (broadcast), que utiliza un medio

pasivo y sin ningún control central. Proporciona detección de errores, pero no corrección. El acceso al medio (de transmisión) está gobernado desde las propias estaciones mediante un esquema de arbitraje estadístico.

Los paquetes de datos transmitidos alcanzan a todas las estaciones (difusión amplia), siendo cada estación responsable de reconocer la dirección contenida en cada paquete y aceptar los que sean dirigidos a ella.

Ethernet realiza varias funciones que incluyen empaquetado y desempaquetado de los datagramas; manejo del enlace; codificación y decodificación de datos, y acceso al canal. El manejador del enlace es responsable de vigilar el mecanismo de colisiones escuchando hasta que el medio de transmisión está libre antes de iniciar una transmisión (solo un usuario utiliza la transmisión cada vez -Banda base-). El manejo de colisiones se realiza deteniendo la transmisión y esperando un cierto tiempo antes de intentarla de nuevo.

Existe un mecanismo por el que se envían paquetes a intervalos no estándar, lo que evita que otras estaciones puedan comunicar. Es lo que se denomina *captura del canal*.

#### V.4 DNP3 (DISTRIBUTED NETWORK PROTOCOL)

Este protocolo fue creado originalmente por Westronic, Inc. (ahora GE Harris) en 1990. Los protocolos definen las reglas para que los dispositivos se comuniquen entre sí. DNP3 fue diseñado para optimizar la transmisión de la adquisición de datos, información y comandos de control de una computadora a otra. No es un protocolo de propósito general, como aquellos que se pueden encontrar en internet para transmitir correos electrónicos, documentos de hipertexto, consultas en SQL, multimedia y archivos muy grandes; está diseñado para aplicaciones SCADA.<sup>11</sup>

DNP3 es un sistema de protocolos de comunicaciones usados entre los componentes en sistemas de proceso de la automatización. Específicamente, fue desarrollado para facilitar comunicaciones entre los varios tipos de adquisición de datos y el equipo del control. Desempeña un papel crucial en los sistemas de SCADA, donde es utilizado por las estaciones principales de SCADA, las RTU, y los dispositivos electrónicos inteligentes (IED) (Fig. 28).<sup>12</sup>

---

<sup>11</sup> DNP3 Users Group. *A DNP3 Protocol Primer*. Marzo 20, 2005. Página 1.

<sup>12</sup> <http://en.wikipedia.org/wiki/DNP3>. Abril 27, 2006.

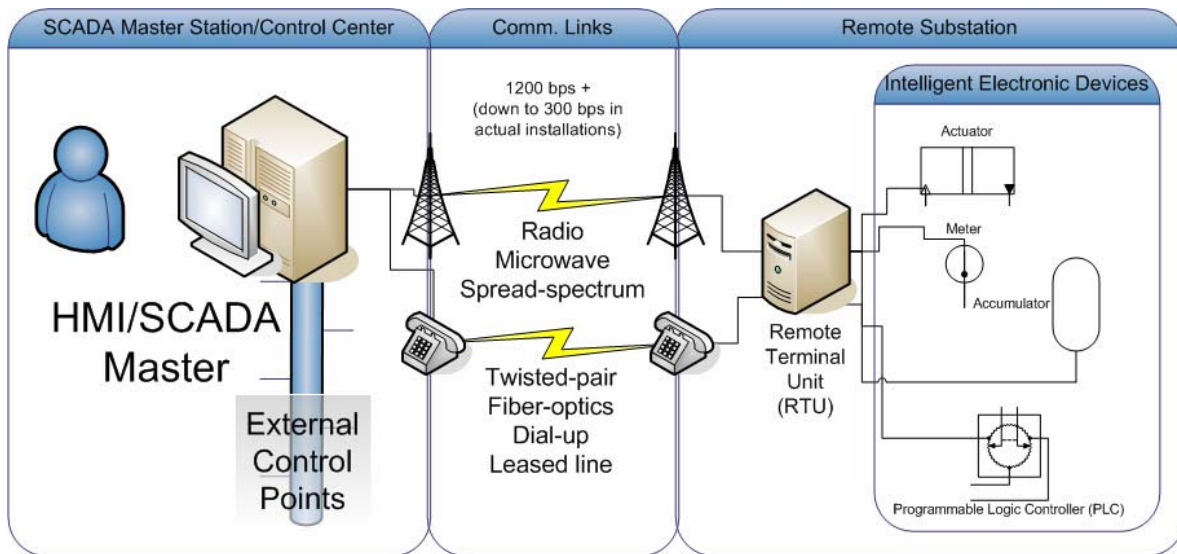


Fig. 28. Protocolo DNP3.

#### V.4.1 CARACTERÍSTICAS

DNP3 provee las reglas para que los esclavos y maestros se comuniquen comandos de control y de datos.

La computadora de la subestación recopila los datos para la transmisión al maestro como:

1. Los datos de entrada binarios son útiles para supervisar dispositivos de doble estado. Por ejemplo si un interruptor es cerrado o activado o la alarma de presión de una tubería se muestran normales o excesivas.
2. Los datos de entrada análoga que transportan los voltajes, corrientes, energía, niveles del agua del depósito y temperaturas.
3. Cuenta de los datos de entrada que reportan kilowatts por hora de energía o volumen de fluidos.
4. Archivos que contengan la configuración de los datos.

La estación principal publica los comandos de control que toman la forma de:

1. Cerrar o disparar un interruptor, subir o bajar una puerta y abrir o cerrar una válvula cercana.
2. Valores análogos de salida para regular la presión o que fijan el nivel de voltaje deseado.

Otras cosas que se comunican las estaciones entre sí son para sincronizar el tiempo y la fecha, enviar historiales o registrar datos, datos de la forma de onda, etcétera.

Los términos de servidor y cliente son aplicables a los sistemas DNP3, donde se define como servidor a un dispositivo o proceso de software que tiene datos o información que alguien más requiere, las computadoras de subestaciones son servidores; un cliente es un dispositivo o proceso de software que requiere datos del servidor.

### Relación cliente-servidor

De la Figura 30 se pueden ver que la serie de bloques del servidor representan sus bases de datos y sus dispositivos de salida, los diversos tipos de datos están organizados conceptualmente en arreglos. El valor de un arreglo binario de entrada binaria representa estados físicos o dispositivos lógicos boléanos. Un arreglo de contadores que representa valores contados como kilowatts hora, que están incrementándose constantemente. Las salidas de control están organizadas en un arreglo que representan encendido-apagado, elevar-disminuir y puntos de salida. Finalmente, el arreglo de salidas análogas representa física o lógicamente cantidades análogas por ejemplo esos usados para los *setpoints*.

El maestro, o cliente, utiliza los valores de su base de datos para propósitos específicos para mostrar los estados del sistema, control de lazo cerrado, notificaciones de alarma, facturación entre otros. Un objetivo del cliente es mantener actualizada su base de datos, esto se logra enviando una petición al servidor pidiendo que le devuelvan los valores contenidos en la base de datos del servidor.

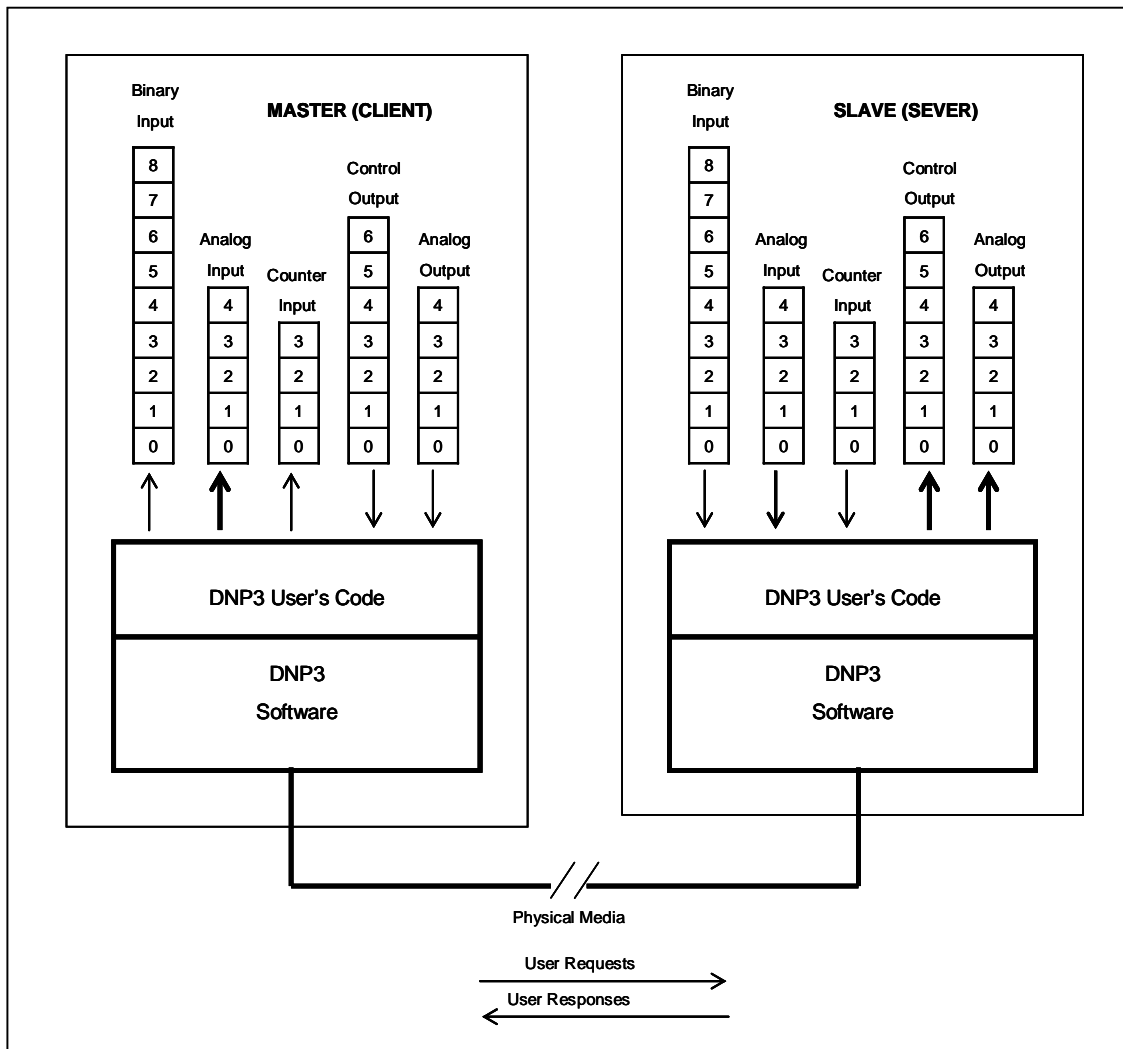


Fig. 290. Relación Cliente-Servidor.

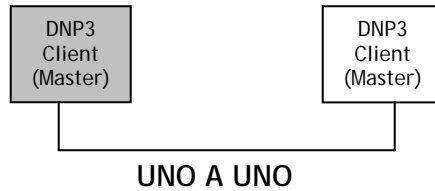
El cliente y el servidor mostrados en la Figura 29, cada uno tienen dos capas de software. La capa superior es la capa del usuario DNP3. En el cliente, es el software el que interactúa entre la base de datos e inicia las peticiones de los datos al servidor. En el servidor, es el software el que trae los datos solicitados de la base de datos del servidor para responder las peticiones del cliente.

#### V.4.2 ARQUITECTURA

Las arquitecturas usadas hoy en día son:

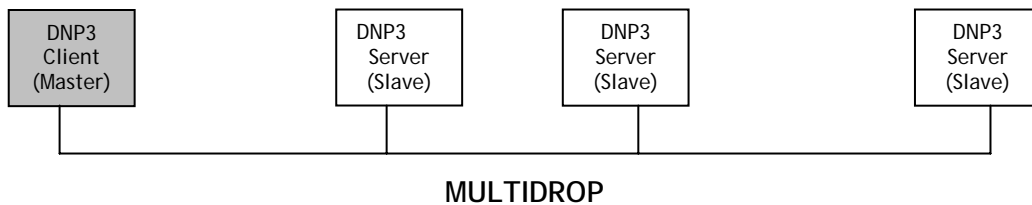
#### V.4.2.1 Uno a uno

El sistema uno a uno es muy sencillo, tiene una estación maestra y un esclavo, la conexión física entre los dos es típicamente una línea dedicada o una línea de discado.



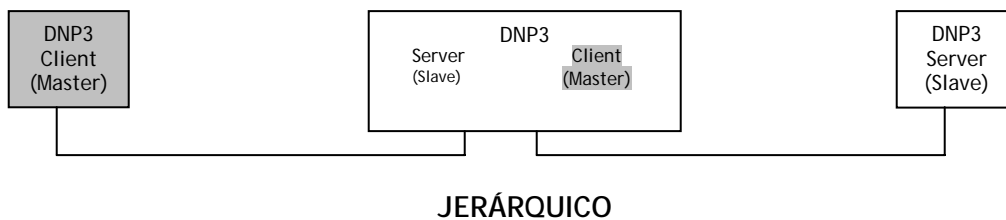
#### V.4.2.2 Diseño Multidrop

Un maestro se comunica con múltiples dispositivos esclavos, las "conversaciones" entre ellos son entre un cliente y un maestro al mismo tiempo. El maestro le hace una petición de datos al primer esclavo, luego se mueve al segundo esclavo por sus peticiones y así continúa interrogando a cada esclavo en una ronda. Los medios de comunicación son una línea telefónica multidrop, cable de fibra óptica o radio. Cada esclavo puede oír los mensajes del maestro y solo está permitido responder los mensajes de su dirección. Los esclavos pueden o no ser capaces de escucharse entre sí.



#### V.4.2.3 Jerárquico

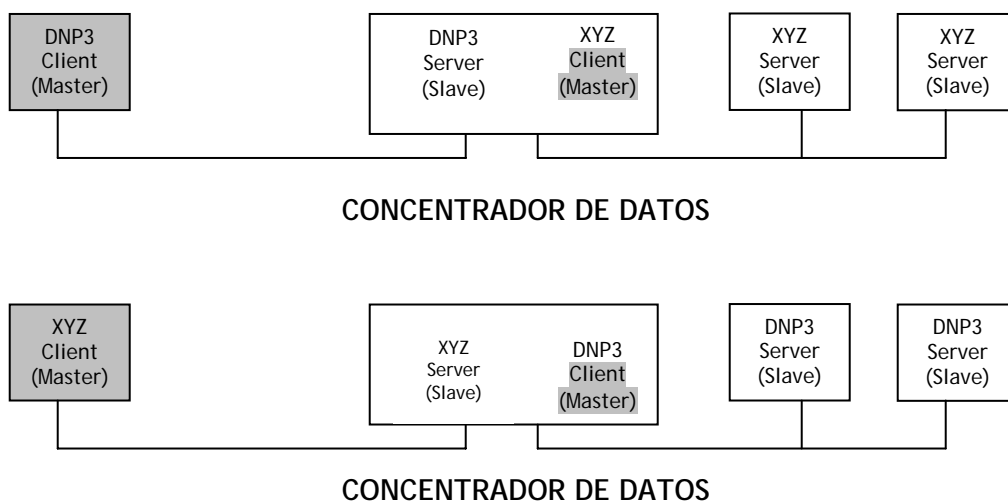
En este tipo de arquitectura donde los dispositivos del centro son un servidor del cliente de la izquierda y un cliente con respecto al servidor de la derecha. En dispositivo central es generalmente llamado submaestro.



#### V.4.2.4 Concentrador de datos

Las siguientes dos figuras muestran el concentrador de aplicaciones y el convertidor de protocolo.

Un dispositivo puede recopilar datos de los servidores múltiples en el derecho y almacenar estos datos en su base de datos donde están recuperables por un cliente de la estación principal en el lado izquierdo. Este diseño se considera a menudo en las subestaciones donde el concentrador de datos recoge la información de los dispositivos inteligentes locales para su transmisión a la estación principal



El software DNP3 se encuentra en capas para proveer una transmisión confiable y para tener un efecto cercano a la organización de la transmisión de datos y comandos.

El conector de capas tiene la responsabilidad de hacer confiable la conexión física. Lo anterior lo logra proveyendo la detección de errores y la de duplicado de tramas (o *frames*). El conector de capas envía y recibe paquetes, los cuales en tecnología DNP3 son llamados tramas. En algunas ocasiones la transmisión de más de una trama es necesaria para transportar toda la información de un dispositivo a otro.

#### V.4.3 LA TRAMA DNP3

Una trama DNP3 consiste en un encabezado y una sección de datos. El encabezado especifica el tamaño de la trama, cuál estación debe recibir esta trama, qué dispositivo envía la trama y la información de control de la

transmisión de datos. La sección de datos es comúnmente llamada carga útil y contiene los datos que han pasado a través de las capas antes mencionadas.

Trama DNP3

Encabezado	Datos
------------	-------

Encabezado

Sincronización	Longitud	Control de conexión	Dirección de destino	Dirección de origen	CRC
----------------	----------	---------------------	----------------------	---------------------	-----

Todas las tramas comienzan con dos bytes de **sincronización** que ayudan al receptor a determinar donde comienza la trama. La **longitud** especifica el número de octetos remanentes de la trama, sin incluir los octetos de verificación CRC. El octeto de **control de conexión** es utilizado entre las capas de conexión de la fuente y del receptor para coordinar sus actividades.

La **Dirección de Destino** especifica que dispositivo DNP3 deberá procesar los datos, y la **Dirección de Origen** identifica que dispositivo DNP3 envía el mensaje. Teniendo ambas direcciones, de destino y origen, se satisface al menos un requerimiento para una comunicación punto a punto, porque el receptor sabe a donde dirigir sus respuestas. 65520 direcciones individuales están disponibles. Cada dispositivo DNP3 debe tener una dirección única dentro de la colección de dispositivos para el envío o recepción de mensajes de uno a otro. Tres direcciones de destino están reservadas por el DNP3 para designar un mensaje llamado a todos (*all-call*); esto es, cuando la trama debe ser procesada por todos los dispositivos DNP3. Trece direcciones son reservadas para futuras necesidades específicas.

Los datos de la carga útil en el *frame* de conexión contienen un par de octetos CRC por cada 16 octetos de datos. Esto provee un alto grado de aseguramiento de que los errores de comunicación puedan ser detectados. El número máximo de octetos en los datos de la carga útil es de 250, sin incluir los octetos CRC. (El *frame* más largo de capa de conexión es de 292 octetos, si todos los octetos del CRC y del encabezado son contados.)

Usualmente oímos el término “confirmación de capa de conexión” cuando se habla del DNP3. Una característica de las capas de conexión DNP3 es la habilidad del transmisor de la trama para solicitar la confirmación al receptor de que la trama haya llegado. El uso de esta característica es opcional y usualmente no es empleada. Este provee un grado extra para el aseguramiento de la confiabilidad de las comunicaciones. Si una confirmación no es recibida, la capa de conexión puede reintentar la transmisión. Algunas desventajas son el tiempo extra requerido para la confirmación de mensajes y la espera en múltiples pausas cuando los reintentos son configurados.



La capa de transporte es responsable de romper largos mensajes en tramas más pequeñas para su transmisión en la capa de conexión o, en caso de que se esté recibiendo, rearmar las tramas para formar el largo mensaje original. Esta capa de transporte requiere de sólo un octeto dentro del mensaje para realizar su trabajo. Por ello, siendo que la capa de conexión puede manejar sólo 250 octetos de datos y uno de ellos es usado para la función de transporte, entonces cada trama de la capa de conexión puede manejar no más de 249 octetos por capa de aplicación.

La fragmentación de mensajes es la responsabilidad de la capa de aplicación. Los mensajes en esta capa se "rompen" en fragmentos; el tamaño de los fragmentos se determina por el tamaño del buffer del dispositivo de recepción, normalmente es entre 2048 y 4096 bytes. Un mensaje que es más largo que un fragmento requiere de múltiples fragmentos.

Nótese que un fragmento de la capa de aplicación de 2048 bytes de tamaño se rompe en 9 tramas para la capa de transporte, y un fragmento de 4096 bytes requiere de 17 tramas. Es interesante como se ha aprendido por la experiencia, que las comunicaciones son algunas veces más exitosas para los sistemas operativos que funcionan en altos ambientes de ruido si los tamaños de los fragmentos son significativamente reducidos.

La capa de aplicación trabaja junto con las capas de transporte y de conexión para permitir una comunicación confiable. Provee funciones estandarizadas y el formateo de los datos con los cuales puede interactuar la capa de usuario.

En DNP3, el término **estático** es utilizado con datos y se refiere al valor actual, así el dato de entrada binaria estática hace referencia al estado presente, encendido o apagado, de un dispositivo biestado. El dato de entrada analógica estática contiene el valor de un análogo en el instante en que es transmitido. Una posibilidad dentro del DNP3 es que permite requerir alguno o todos los datos estáticos de un dispositivo esclavo.

Los eventos DNP3 están asociados con algún suceso significativo. Algunos ejemplos son los cambios de estado, valores excediendo algún umbral, tomas de datos variando, datos transitorios y información disponible recientemente. Un evento ocurre cuando una entra binaria cambia de un estado encendido a apagado o cuando un valor analógico cambia por más de lo que está configurado su límite. DNP3 provee la habilidad de reportar eventos con o sin registro de tiempo, por lo que el cliente puede generar reportes de la secuencia del tiempo.

La capa de usuario puede solicitar directamente eventos al DNP3. Usualmente un cliente se actualiza más rápidamente si sondea eventos desde el servidor y sólo ocasionalmente pregunta por datos estáticos como una medida de integridad. La

razón por la que el cliente se actualiza más rápidamente es porque el número de eventos generados entre las preguntas de los servidores es menor y, entonces, menos datos deben regresar al cliente.

El DNP3 va más allá clasificando eventos en tres clases: cuando DNP3 fue concebido el evento clase 1 fue considerado como de prioridad más alta que los eventos de clase 2, y los eventos clase 2 más que los eventos clase 3. Debido a que el esquema puede ser configurado, algunos usuarios de DNP3 han desarrollado otras estrategias más favorables para su operación para la asignación de eventos en las clases. La capa de usuario puede requerir a la capa de aplicación que sondee por eventos de clase 1, 2 o 3 o cualquier combinación de ellos.

DNP3 cuenta con suministros para la representación de datos en diferentes formatos. La examinación de formatos de datos analógicos es útil para entender la flexibilidad del DNP3. Estático, valor actual, datos analógicos pueden ser representados por números variables como los que siguen:

1. Un valor entero de 32-bits con bandera,
2. Un valor entero de 16-bits con bandera,
3. Un valor entero de 32-bits,
4. Un valor entero de 16-bits,
5. Un valor flotante de 32-bits con bandera y
6. Un valor flotante de 16-bits con bandera.

La bandera es un octeto sencillo con un campo de bits indicando si la fuente está en línea, o si el valor contiene un valor de reinicio, si las comunicaciones están perdidas con la fuente, si el valor es forzado o si el valor está sobre el rango.

No todos los dispositivos DNP3 pueden transmitir o interpretar las seis variantes; los dispositivos DNP3 deben permitir la transmisión de las más simples variaciones de tal forma que cualquier receptor pueda interpretar el contenido.

Los eventos de datos analógicos pueden ser representados en estas variantes:

1. Un valor entero de 32-bits con bandera,
2. Un valor entero de 16-bits con bandera,
3. Un valor entero de 32-bits con bandera y tiempo de evento,
4. Un valor entero de 16-bits con bandera y tiempo de evento,
5. Un valor flotante de 32-bits con bandera,
6. Un valor flotante de 64-bits con bandera,
7. Un valor flotante de 32-bits con bandera y tiempo de evento y
8. Un valor flotante de 64-bits con bandera y tiempo de evento.

La bandera tiene el mismo campo de bits que para las variantes estáticas.

Esto parece que una variación de uno o dos eventos análogos de valores no pueden ser diferenciados de una o dos variaciones estáticas análogos, este problema se puede resolver asignando números a objetos; los valores estáticos análogos son asignados como objetos 30 y valores de eventos análogos son asignados como objetos 32.

Cuando el servidor DNP3 transmite un mensaje conteniendo los datos de respuesta, el mensaje identifica el número de objeto y la variación de cada valor dentro del mensaje. Los objetos y los números de variación son asignados por los contadores, entradas binarias y salidas análogas, de hecho, todos los formatos válidos de los tipos de datos son identificados por objetos y números de variación, así se asegura la interoperatividad entre los dispositivos.

La capa del usuario del cliente formula su petición de datos al servidor, diciéndole a la capa de aplicación qué función debe realizar como leer y especificar cuales objetos requiere del servidor. La petición puede especificar cuantos objetos quiere o puede especificar objetos definidos o un rango de ellos mediante un índice x hasta el y; entonces la capa de aplicación pasa la petición abajo con la capa de transporte a la capa de acoplamiento, que alternadamente, envía el mensaje al servidor.

La transmisión de mensajes no solicitados. Este es un modo de operación donde el servidor transmite una respuesta de manera espontánea, conteniendo posiblemente datos sin haber recibido una petición específica de datos; es útil cuando el sistema tiene muchos esclavos y el maestro requiere notificaciones tan pronto sea posible después de que ha ocurrido un cambio. Para configurar el sistema de mensajes no solicitados, hay que hacer unas consideraciones básicas: primero, las transmisiones espontáneas deben ocurrir generalmente de forma poco frecuente, si no, demasiada contención puede ocurrir y los medios que controlan tienen acceso vía la interrogación de la estación principal serían mejores; segundo, es que el servidor debe tener alguna manera de saber si puede transmitir sin cambiar en algún mensaje en progreso.

#### V.4.4 BENEFICIOS

Los usuarios tendrán beneficios de corto plazo a partir del uso del DNP3:

- Interoperabilidad entre equipos de diferentes proveedores
- Menor cantidad de protocolos que soportar en éste campo
- Menores costos de software
- No se requieren traductores de protocolos
- Menores tiempos de entrega
- Menor cantidad de ensayos, mantenimiento y entrenamiento

- Mejor documentación
- Ensayos de cumplimiento independientes
- Soporte del grupo de usuarios independientes y terceras partes (ej. sets de ensayo, código base).

Los beneficios a largo plazo del uso del DNP3 incluyen:

- Fácil expansión del sistema
- Producto de larga vida
- Productos con mayor valor agregado
- Adopción más rápida de nuevas tecnologías
- Importantes ahorros en las operaciones

## Capítulo VI. NORMAS

Los estándares surgen como una necesidad para proteger a los clientes y para fomentar tecnologías de interconexión de computadoras. En tanto que los estándares de red proporcionan la base para la transmisión de datos, para la fabricación de los equipos de red compatibles y para el diseño de sistemas operativos que se utilizan en una red; éstos definen el tipo máximo que un paquete debe tardar en viajar de un nodo a otro antes de determinar que el paquete no ha encontrado su destino, entre otras características.

Ahora bien, una norma o estándar es un procedimiento que se ajusta a un trabajo, a la industria, etcétera; es un patrón o un modelo al que se aspira, lo cual implica que ese procedimiento se aplique principalmente a la manera de hacer algo.

Las organizaciones más importantes que realizan los estándares para interconectar ordenadores son:

- ISO; *International Standards Organization* (Organización Internacional de Normas)
- IEEE; *The Institute of Electrical and Electronics Engineers* (Instituto de Ingenieros Electrónicos y Eléctricos), mismo que se encarga de fijar los estándares de los elementos físicos de una red, cables, conectores, etcétera.
- EIA/TIA- *Electronics Industries Association/Telecommunications Industry Association* (Asociaciones de las Industrias de Electrónica y Telecomunicación de Estados Unidos)
- CSA- *Canadian Standards Association* (Asociación Canadiense de Normas)
- ANSI- *American National Standards Institute* (Instituto Nacional Americano de Normalización)

Es importante mencionar que algunas de las normas que definen el cableado estructurado para los sistemas de telecomunicaciones son las siguientes:

- EIA/TIA-568. Estandariza los requerimientos de los sistemas de cableado de telecomunicaciones de redes de edificios con servicios de voz, datos, imagen y video.
- EIA/TIA TSB-36 Especificaciones adicionales para cables UTP.
- EIA/TIA TSB-40 Especificaciones adicionales de transmisión para cables UTP.

- EIA/TIA-569. Estandariza las prácticas de diseño y construcción dentro y entre los edificios.
- EIA/TIA-606. Guía para la administración de la infraestructura de telecomunicaciones en edificios.
- EIA/TIA-607. Provee los estándares para aislar y aterrizar el equipo de telecomunicaciones y sus datos.
- ANSI X3T9.5 FDDI. Define los estándares para redes locales de 100 Mbps basadas en fibra óptica o UTP.

Por su parte, uno de los encargados en establecer los estándares a nivel mundial en lo referente a computadoras es el IEEE en su división 802 y se clasifican en 16 categorías, abordando específicamente lo relativo a los sistemas de red.

Las categorías de las especificaciones 802 son:

Especificación	Descripción
802.1	Establece los estándares de interconexión relacionados con la gestión de redes.
802.2	Define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: los niveles LLC y MAC. El nivel MAC varía en función de los diferentes tipos de red y está definido por el estándar IEEE 802.3.
802.3	Define el nivel MAC para redes de bus que utilizan acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD, <i>Carrier-Sense Multiple Access with Collision Detection</i> ). Éste es el estándar Ethernet.
802.4	Define el nivel MAC para redes de bus que utilizan un mecanismo de paso de testigo (red de área local Token Bus).
802.5	Define el nivel MAC para redes <i>Token Ring</i> (red de área local <i>Token Ring</i> ).
802.6	Establece estándares para redes de área metropolitana (MAN, <i>Metropolitan Area Networks</i> ), que son redes de datos diseñadas para poblaciones o ciudades. En términos de extensión geográfica, las redes de área metropolitana (MAN) son más grandes que las redes de área local (LAN), pero más pequeñas que las redes de área global (WAN). Las redes de área metropolitana (MAN) se caracterizan, normalmente, por

	conexiones de muy alta velocidad utilizando cables de fibra óptica u otro medio digital.
802.7	Utilizada por el grupo asesor técnico de banda ancha ( <i>Broadband Technical Advisory Group</i> ).
802.8	Utilizada por el grupo asesor técnico de fibra óptica ( <i>Fiber-Optic Technical Advisory Group</i> ).
802.9	Define las redes integradas de voz y datos.
802.10	Define la seguridad de las redes.
802.11	Define los estándares de redes sin cable.
802.12	Define el acceso con prioridad por demanda ( <i>Demand Priority Access</i> ) a una LAN, 100BaseVG-AnyLAN.
802.13	No utilizada.
802.14	Define los estándares de módem por cable.
802.15	Define las redes de área personal sin cable (WPAN, <i>Wireless Personal Area Networks</i> ).
802.16	Define los estándares sin cable de banda ancha.

Fundado en 1884, el Instituto de Ingenieros en Electricidad y Electrónica, Inc. (IEEE) se ha dedicado a ayudar a que más de 320,000 profesionales y estudiantes de Ingeniería desarrollen su potencial en campos de la ingeniería eléctrica, así la mejor manera de proteger la posición de una empresa es participando en la elaboración de normas técnicas.

A continuación se hará mención de algunas de las normas o estándares más importantes para la transmisión de datos, terminología informática, comunicaciones entre dispositivos. Una de las normas que especifica la transmisión de datos es el estándar **IEEE 1379-2000** que consiste en descripciones e información tabular para la implantación de funciones comunes de comunicación entre dispositivos electrónicos inteligentes (IED's) en aplicaciones de subestaciones eléctricas. Éste presenta un informe de las pautas para las comunicaciones entre unidades de terminales remotas (RTU's) y dispositivos electrónicos inteligentes, las definiciones de los datos y la estructura del mensaje pueden ser usados por desarrolladores de producto o ambos, IED y RTU, para crear interfaces de comunicaciones no propietarias. También se puede utilizar como interfaz de comunicaciones entre RTU's y las estaciones principales de supervisión del control y de adquisición de datos (SCADA).

En esta norma, se recomiendan dos protocolos con muchas similitudes; cada uno intenta satisfacer los requerimientos de la comunicación entre RTU e IED y contiene un marco adecuado para la mayoría de las aplicaciones del sistema.

Ambos protocolos son especificados completamente y hacen una referencia cruzada de modo que los usuarios y los desarrolladores puedan elegir uno o el otro, basado en los requisitos del uso del sistema o del producto<sup>13</sup>.

Otro de estos estándares para la transmisión de datos es el **IEEE 999-1992** que se aplica solamente para el uso de la transmisión serial digital por medio de los sistemas, teniendo terminales dispersas geográficamente. Estos tipos de sistemas utilizan típicamente los canales de comunicaciones dedicados, tales como canales de microonda privados o líneas telefónicas arrendadas, que se limitan a los índices de datos de menos de 10 000 b/s.

En esta norma están excluidas las redes locales de banda ancha usadas para la adquisición de datos y funciones de control de alta velocidad. Además abarca los canales de comunicaciones, las interfaces de canales, el formato del mensaje, el uso del campo de información, y la gerencia de la comunicación. Define generalmente un protocolo estándar de mensaje al nivel del octeto en lugar de a nivel de bit, la mayoría de los detalles de nivel de bit son dejados para que los defina e implemente el fabricante de los equipos SCADA<sup>14</sup>.

Por otro lado, dentro de las normas de IEEE se encuentra la **IEEE Std. C37.1-1994** la cual aplica y provee las bases para la definición, la especificación, el análisis del funcionamiento y la aplicación de los sistemas usados para el control de supervisión; la adquisición de datos o control automático, o ambos, en subestaciones eléctricas atendidas o desatendidas, incluyendo las asociadas a estaciones generadoras e instalaciones de utilización y conversión de energía<sup>15</sup>.

También existen normas que definen la terminología utilizada en las aplicaciones informáticas, uno de ellos es el **ANSI/IEEE Std. 610.2-1987** donde se definen los términos en el campo informático, los tópicos cubiertos incluyen los procesos automatizados de lenguaje, indexamiento automático, informática del negocio, reconocimiento de caracteres, aplicaciones médicas, investigación de operaciones, aplicaciones científicas, de ingeniería y de telecomunicaciones, entre otras<sup>16</sup>.

Uno más de los glosarios de términos para las aplicaciones computacionales es **IEEE Std. 610.7-1995**, en él se definen los términos que pertenecen a las comunicaciones de datos y establecimiento de una red, en particular de las siguientes áreas: transmisión de datos, comunicaciones generales, redes

---

<sup>13</sup> *Apud* IEEE Recommended Practice for Data Communications between Remote Terminal Units and Intelligent Electronic Devices in a Substation. IEEE-SA Standards Boards. Septiembre 2000.

<sup>14</sup> *Apud* IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications. IEEE-SA Standards Boards. Junio 1992.

<sup>15</sup> *Apud* IEEE Standard Definition, specification and Analysis of Systems Used for Supervisory Control, Data Acquisition and Automatic Control. IEEE-SA Standards Boards. Marzo 1994.

<sup>16</sup> *Apud* IEEE Standard Glossary of Computer Applications Terminology. IEEE-SA Standards Boards. Mayo 1987.



generales, redes de área local, seguridad de comunicaciones de la red, errores de la red, hardware del establecimiento de una red, dirección de la red, nodos de red, arquitectura de sistema, protocolos, estándares y telefonía. El glosario es sobre todo una compilación de los términos definidos en los estándares individuales de IEEE, pero también incluye un número de términos comunes<sup>17</sup>.

En lo referente a la evaluación de las comunicaciones, la IEEE cuenta con el estándar **IEEE Std. C37.115-2003**, este estándar se aplica a los sistemas usados para comunicarse entre los dispositivos electrónicos inteligentes (IED's) para la protección, el control y la adquisición de datos integrados en las subestaciones. Los requisitos de este estándar están además contenidos en los estándares para los dispositivos individuales (por ejemplo, relevadores, dispositivo de distribución).

Esta norma define el modelo de comunicación estándar, la terminología, los criterios de la evaluación y las medidas de funcionamiento para los escenarios de prueba, los cuales especifican que mensajes se intercambiarán entre las subestaciones de corriente eléctrica y los dispositivos electrónicos inteligentes (IED's). También definen las transacciones del mensaje entre las aplicaciones dentro de la subestación, los IED's y entre las aplicaciones localizadas remotamente. Sin embargo, los panoramas no especifican el protocolo de comunicación requerido para poner las transacciones en ejecución. Este estándar se aplica a una tecnología que cambia rápidamente y es recomendable que tenga revisiones frecuentes<sup>18</sup>.

Por último, se recomienda la norma **IEEE Std. 1379-1997** para la comunicación entre RTU's e IED's. Esta norma recomendada presenta un conjunto uniforme de pautas para las comunicaciones y la interoperación de IED's y de las unidades del terminales remotas RTU's en una subestación eléctrica. Ésta no establece un estándar de comunicación, en su lugar, proporciona un subconjunto limitado y específico de dos protocolos de comunicación existentes para entender y alentar el uso oportuno<sup>19</sup>.

---

<sup>17</sup> *Apud* IEEE Standard Glossary of Computer Networking Terminology. IEEE-SA Standards Boards. Junio 1995.

<sup>18</sup> *Apud* IEEE Std C37.115-2003, IEEE Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System. IEEE-SA Standards Boards. Noviembre 2003.

<sup>19</sup> *Apud* IEEE Trial-Use Recommended Practice for Data Communications between Intelligent Electronic Devices and Remote Terminal Units in a Substation. IEEE-SA Standards Boards. Septiembre 1997.

## Capítulo VII. RECOMENDACIONES DE IMPLANTACIÓN

El tipo de aplicaciones industriales se caracteriza por el gran número de señales de proceso que se controlan y/o monitorizan. Muchas de ellas son señales binarias que se utilizan para conducir la operación secuencial de IOs diferentes subsistemas que conforman la aplicación. Por ello, el dispositivo de control más comúnmente utilizado es el Controlador Lógico Programable (PLC), equipo que nació para procesar cíclicamente la lógica de control de la aplicación. Cuando la aplicación lo requiere las entradas / salidas se distribuyen utilizando, como sistemas de comunicación, los llamados buses de campo que transmiten gran cantidad de mensajes a frecuencias relativamente altas pero de pequeña longitud, y PLCs como elementos de control.<sup>20</sup>

En la actualidad, se requieren de sistemas abiertos que se puedan integrar tanto en células de producción como en sistemas computacionales de un nivel superior en la pirámide de automatización. Así mismo, la aplicación de estándares también tiene un gran impacto en el rápido crecimiento del mercado de la instrumentación y control de procesos industriales. En este sentido, la *International Electrotechnical Commission* (IEC) ha publicado varios estándares promoviendo sistemas abiertos e intercambiables. En particular, el estándar IEC 61131-3 proporciona lenguajes y métodos estandarizados que permiten resolver un amplio rango de problemas tecnológicos como los que se derivan del software propietario.

El lenguaje de modelado industrialmente estandarizado es UML (*Unified Modeling Language*) y se trata de un lenguaje de modelado de propósito general, evolucionado a partir de varios métodos orientados a objetos de segunda generación, soportado por distintas herramientas CASE, abierto y totalmente extensible. Uno de los inconvenientes de uso de este lenguaje de modelado, viene derivado de su potencialidad. La gran variabilidad de diagramas y elementos que permiten modelar cualquier tipo de aplicación y situación hace que sea lo suficientemente completo para ser utilizado en entornos industriales.

Con la finalidad de acotar los diagramas así como elementos UML, surgen los llamados Perfiles de UML que son muy útiles para añadir las características

---

<sup>20</sup> *Apud* E. Estévez I. Torre, U. Gangoiti, M. Marcos, J. Portillo, D. Orive, N. Iriondo, I. Cabanes, I. Sarachaga, F. Artaza. "Modelado Basado en Componentes de Sistemas Distribuidos de Control Industrial" Escuela Superior de Ingenieros de Bilbao (Universidad del País Vasco)

necesarias y en este caso limitarlas a las particularidades de las aplicaciones a modelar.

### VII.1.1 REQUISITOS DE LAS APLICACIONES A MODELAR

Una parte importante del sistema de control corresponde a los dispositivos que controlan los componentes mecánicos básicos que forman la planta, además habrán módulos de comunicaciones entre estos dispositivos y los controladores existentes en la misma. Estas comunicaciones se realizan normalmente mediante buses de campo o redes de planta.

En lo referente a la arquitectura hardware se realiza con equipamiento de control específico y la mayoría de las aplicaciones instaladas utilizan controladores propietarios y por tanto las características y configuración del equipamiento hardware es dependiente del fabricante. Los fabricantes ofrecen diferentes tipos de producto desde gamas bajas, para controlar aplicaciones simples, a producto de altas gamas que son mucho más potentes y ofrecen mayor funcionalidad. Si la aplicación es distribuida, el sistema de control se extiende con segmentos de red o segmentos de bus de campo. Esto requiere introducir tarjetas de comunicación en PLC que le permitan comunicarse con los sensores, actuadores de la planta o con otros controladores.

Por tanto, se pueden resumir como principales requisitos de las aplicaciones de interés los siguientes:

- Especificación modular y jerárquica de la funcionalidad del sistema de control.
- Especificación de la implantación en términos del modelo software del estándar IEC 61131-3.
- Especificación del hardware en función de fabricante y gama de producto.

### VII.1.2 METODOLOGÍA DE MODELADO

Para la definición del sistema de control distribuido se propone basar el modelado en la metodología MDA, metodología que ha sido propuesta por el *Object Management Group*, y define una aproximación para la especificación de sistemas cuyo principio es la separación de la funcionalidad del sistema de los aspectos dependientes de la plataforma destino. Es decir, separar el cómo implementar la aplicación de su funcionalidad.

Siguiendo esta metodología, el modelo de una aplicación está formado por tres partes:

- *Platform Independent Model, PIM* (Modelo de Plataforma Independiente): corresponde a una especificación funcional independiente de la plataforma, es decir, en esta fase se define qué es lo que tiene que hacer, en el caso de las aplicaciones de control industrial corresponde con una especificación jerárquica funcional.
- *Platform Specific Model, PSM* (Modelo de Plataforma Específica): contempla la implantación de la especificación funcional en cuanto a una arquitectura hardware y software; por ejemplo, define cómo implementar la especificación funcional definida en el PIM. La arquitectura software se hará siguiendo el modelo software propuesto por el estándar IEC 61131-3 (que es independiente de las características de los fabricantes), y la arquitectura hardware incluye los PLCs de diferentes fabricantes, PLCs abiertos, redes industriales, así como nodos entrada / salida.
- La última fase consiste en una extensión de la implantación o PSM, con el objeto de la generación de código para los equipos. Esta fase concluye con la generación del proyecto de automatización para una herramienta propietaria de programación de PLCs. Por tanto, en esta fase también son necesarias una serie de transformaciones para adaptar el código IEC 61131-3 al que realmente siga la herramienta, debido a que actualmente ninguna herramienta sigue este estándar al cien por ciento.

Una vez identificados y caracterizados las diferentes partes a modelar, el siguiente paso consiste en la definición de una metodología que guíe el modelado del sistema siguiendo además la separación de conceptos, propuesta por la metodología MDA. Los elementos básicos usados para modelar el sistema son los componentes y conectores. Por tanto, el modelo de cada parte de la aplicación se compone de un conjunto de elementos relacionados a través de conectores. El modelado por partes (funcionalidad e implantación) se completa teniendo en cuenta que ambas representan el mismo sistema y que por lo tanto están relacionadas tal y como se ilustra en la Figura 30.

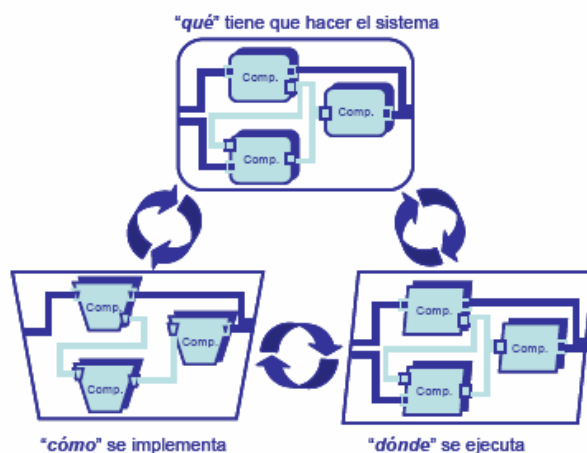


Figura 30: Vista de dominio de las aplicaciones

La utilización del modelado basado en componentes permite realizar diseños reutilizando aplicaciones o parte de ellas diseñadas previamente. Por otro lado, también garantiza el mantenimiento y mejora a través de reemplazar y personalizar los componentes que la definen.

### VII.1.3 ESPECIFICACIÓN FUNCIONAL

La especificación de la funcionalidad debe corresponder a una descripción jerárquica de alto nivel del sistema de control y está modelada a través de conexiones y conectores.

Las conexiones representan dos tipos de información. Por un lado se utilizan para definir la información procedente o con destino al proceso (sensores y actuadores), Interfaz Hombre Máquina (HMI), también se pueden usar con objeto de comunicar componentes del mismo nivel jerárquico.

El número de señales de campo involucradas en las aplicaciones de control industrial varía de decenas a cientos. Se han definido dos nuevos elementos para modelar la especificación funcional; estos son los conectores y los puertos.

Los **conectores** permiten agrupar un conjunto de conexiones que vienen o van al mismo componente. Todo conector debe contener al menos una conexión. Los conectores actúan como canales que agrupan conexiones.

Los **puertos** representan el punto donde los conectores se relacionan con los componentes; un componente al menos tiene un puerto de entrada y otro de salida. De la misma forma, un puerto contiene al menos un conector.

La Figura 31 presenta los elementos que caracterizan a un componente funcional.

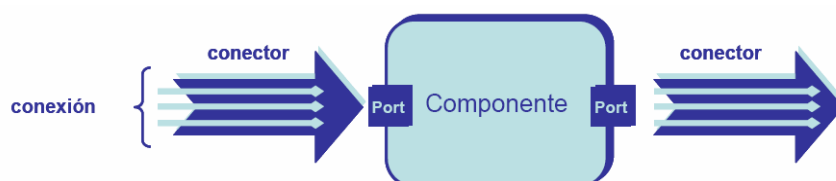


Figura 31: Elementos en el componente de especificación funcional

Con objeto de distinguir las conexiones heredadas (diseño *top-down* o *bottom-up*) de aquellas correspondientes a la comunicación entre componentes del mismo nivel, se han considerado necesarios dos tipos de puertos: vertical y horizontal.

El primero de ellos se usa para aquellos conectores que contienen conexiones heredadas y el segundo, para aquellos que contienen conexiones que comunican diferentes componentes del mismo nivel jerárquico.

Esta definición permite modelar una especificación jerárquica con suficiente detalle y de la misma manera permite representar gráficamente la especificación funcional independientemente del número de componentes y conexiones presentes en la aplicación.

La siguiente figura (Fig. 32) ilustra un ejemplo.

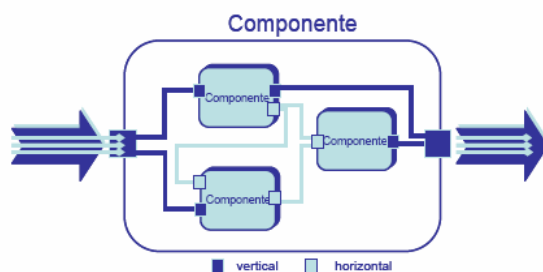


Figura 32: puertos verticales y horizontales de los componentes funcionales

#### VII.1.4 IMPLANTACIÓN DE LOS SISTEMAS DISTRIBUIDOS DE CONTROL INDUSTRIAL

El estándar IEC 61131 permite diseñar aplicaciones de control de forma jerárquica utilizando los elementos básicos de programación conocidos como *Program Organisation Units* (POUs, Unidades de Organización Programada). Estos elementos se caracterizan porque su uso es independiente de fabricante.

El modelo software está compuesto por los elementos que aparecen en la siguiente figura (Fig. 33):

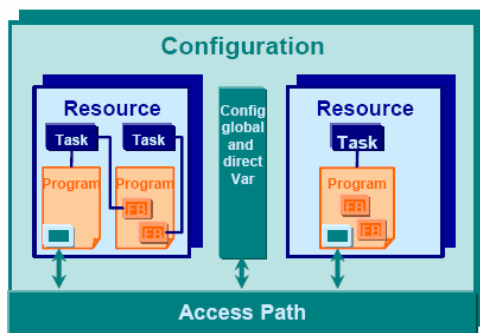


Figura 33: Modelo software IEC 61131-3

Como se aprecia en la figura anterior está compuesta por los elementos:

- **Configuration** (Configuración): Identifica cada uno de los nodos (PLC, Controladores abiertos) del sistema distribuido.
- **Resource** (Recurso): Identifica cada CPU o máquina virtual de una configuración.
- **Task** (Tarea): Identifica la unidad mínima de planificación dentro de un recurso. Las tareas se asocian con un recurso particular y se considera que se ejecutarán bajo el control de ese recurso. A cada tarea se le asigna una prioridad y un periodo de ejecución. El estándar IEC 61131 permite asignar los programas y bloques funcionales diseñados a diferentes tareas para ajustar los periodos de su ejecución.
- **POU**: Elemento principal de reutilización de código ya que se diseña una vez y puede ser utilizado tantas veces como sea necesario y además en diferentes aplicaciones. Existen tres tipos: *Function*, *Function Block* y *Program*. El más utilizado para asegurar la reutilización del software es el *Function Block*
- **Variables**: que se definen por su visibilidad. Se pueden tener por tanto, variables globales a nivel de configuración y/o recurso y de la misma manera variables locales del programa. En el caso de tener aplicaciones de control distribuidas, también se pueden tener variables de tipo Access que contienen la información intercambiable entre las diferentes configuraciones que componen la aplicación. Estas variables se caracterizan de la misma forma que las variables de los lenguajes de programación del alto nivel, tipo y valor.

Por tanto, en lo referente al modelado de la arquitectura software los componentes se corresponden a instancias de los POU's y las conexiones son las variables IEC 61131-3.

La arquitectura hardware se define por medio de un conjunto de componentes (nodos de procesamiento, controladores y dispositivos entrada / salida) que son conectados por medio de segmentos de red. Por tanto se pueden distinguir dos tipos de componentes: nodos de procesamiento y nodos I/O.

Finalmente, como ambas arquitecturas modelan el mismo sistema de control es claro que existe una relación entre ambas. Se tiene que indicar en qué nodo de procesamiento se descargará el software que es asociado a cada elemento IEC 61131-3. De la misma forma, también es necesario establecer la relación entre variables globales con dirección física y el dispositivo I/O de la arquitectura hardware.

**CONCLUSIONES**

El desarrollo de las comunicaciones, y su aplicación a la industria, ha permitido la implantación de redes industriales que facilitan la comunicación entre los dispositivos automáticos y la información que se requiere para la toma de decisiones, aumentando el rendimiento y las posibilidades en el control.

Por otro lado, a nivel industrial se está dando un cambio, en él no solo se pretende trabajar con los instrumentos específicos para cada proceso y con el control automático, sino que existe la necesidad de mantener históricamente información de todos los procesos, además que esta información esté también en tiempo real y que sirva para la toma de decisiones y se pueda así mejorar la calidad de los procesos.

Así, estas características definen algunas de las principales diferencias de una red industrial con una red convencional, las más importantes son:

	<b>RED INDUSTRIAL</b>	<b>RED DE OFICINA</b>
<b>SERVICIOS</b>	Predeterminado	Adaptado al usuario
<b>TRÁFICO</b>	Determinístico	Aleatorio
<b>USUARIO</b>	Procesos	Personas
<b>SIMULTANEIDAD</b>	Predeterminada	Todos los usuarios
<b>TIEMPO DE RESPUESTA</b>	Crítico	No crítico
<b>MÉTODO DE COMUNICACIÓN</b>	Según aplicación	Generales

Una vez establecidas las diferencias entre las redes industriales y las redes convencionales, podemos decir que ambas siguen los mismos patrones para su construcción: deben tener una topología, un bus para la interconexión de los dispositivos y un protocolo de comunicación; todo esto apoyado por las normas que nos dan una guía para poder realizarlo.

De este modo, en primera instancia, habrá que reconocer que actualmente las tecnologías que triunfan en el mercado son aquellas que ofrecen las mejores ventajas a los clientes y a los usuarios, dado que se busca un sistema abierto, compatible y funcional. Por ello y dadas las condiciones



extremas a nivel industrial, se requieren de equipos capaces de soportar altas temperaturas, ruido excesivo, polvo, humedad y demás condiciones adversas, ya que son éstas las que se encuentran en el ambiente y que definen también las principales diferencias con una red convencional. Así queda finalmente, cubierto el objetivo primordial de esta tesis.

Entre las innumerables ventajas del empleo de redes industriales, podemos destacar las siguientes:

- ✓ Visualización y supervisión de todo el proceso productivo.
- ✓ Mayor velocidad en la toma de datos.
- ✓ Disponibilidad de información en tiempo real.
- ✓ Mejora del rendimiento del proceso al realizar el control en su conjunto.
- ✓ Posibilidad de intercambio de datos entre diferentes sectores del proceso y departamentos.
- ✓ Posibilidad de programación y control a distancia sin tener que estar en campo.

Finalmente, el último capítulo de este trabajo trata de dar una guía para la implantación de una red industrial, de las consideraciones que se deben tener para que los buses sean compatibles con los protocolos y de qué protocolo cubre mejor las necesidades.

Al respecto resulta indispensable señalar que en muchos casos los dispositivos deben trabajar con el software que proporciona el mismo vendedor, condicionando de esta manera la adaptación de programas del usuario con los dispositivos que se adquieren, por lo que la implantación del sistema está sujeta a esas características y no a las de tipo técnico funcional.

Consecuentemente, se han tratado de estandarizar en la medida de lo posible los sistemas operativos y los programas que utilizan los dispositivos de control, pero aun está lejano el día en que se logre en su totalidad, porque eso depende mucho de los propios distribuidores y de los recursos mismos de cada planta.

---

## BIBLIOGRAFÍA

### LIBROS

- 📖 Solar, Iván; Pérez, Ricardo. Control Automático de Procesos Químicos. Ediciones Universidad Católica de Chile, 1993, Capítulo 3.
- 📖 Lawrence, T. Amy. Automation Systems for Control and Data Acquisition. ISA, 1992. Capítulo 1 y 3.
- 📖 Considine, M. Douglas. Process Instruments and Controls Handbook. McGraw Hill, 1984. Capítulo 18.
- 📖 Cassell, Douglas A. Microcomputers and modern control engineering. Prentice Hall, 1983. Capítulo 2.

### PUBLICACIONES

- 📖 Sirgo, J.A. y González, Rafael. "Redes Locales en entornos Industriales. Buses de Campo". Tema 9. Universidad de Oviedo, Departamento de Eléctrica, Electrónica, de Computadores y de Sistemas. 2003. página 1.
- 📖 "IEEE Recommended Practice for Data Communications between Remote Terminal Units and Intelligent Electronic Devices in a Substation". IEEE-SA Standards Boards. Septiembre 2000.
- 📖 "IEEE Recommended Practice for Mater/Remote Supervisory Control and Data Acquisition (SCADA) Communications". IEEE-SA Standards Boards. Junio 1992.
- 📖 "IEEE Standard Definition, specification and Analysis of Systems Used for Supervisory Control, Data Acquisition and Automatic Control". IEEE-SA Standards Boards. Marzo 1994.
- 📖 "IEEE Standard Glossary of Computer Applications Terminology". IEEE-SA Standards Boards. Mayo 1987.
- 📖 "IEEE Standard Glossary of Computer Networking Terminology". IEEE-SA Standards Boards. Junio 1995.
- 📖 "IEEE Std C37.115-2003, IEEE Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System". IEEE-SA Standards Boards. Noviembre 2003.

- 📖 "IEEE Trial-Use Recommended Practice for Data Communications between Intelligent Electronic Devices and Remote Terminal Units in a Substation". IEEE-SA Standards Boards. Septiembre 1997.

## APUNTES

- 📖 Garibay Jiménez, Ricardo. Especialización en Mantenimiento a Equipo de Instrumentación y Control en Plataformas Marinas. Unidad 1. paginas 7-9.
- 📖 DNP3 Users Group. A DNP3 Protocol Primer. Marzo 20, 2005. Página 1.
- 📖 E. Estévez I. Torre, U. Gangoiti, M. Marcos, J. Portillo, D. Orive, N. Iriondo, I. Cabanes, I. Sarachaga, F. Artaza. "Modelado Basado en Componentes de Sistemas Distribuidos de Control Industrial" Escuela Superior de Ingenieros de Bilbao (Universidad del País Vasco)

## PÁGINAS EN INTERNET

<http://www.euskalnet.net/m.ubiria/ARTICULOS.htm>  
<http://www.can-cia.de/can/protocol/>  
<http://www.mjschofield.com/index.htm>  
<http://www.datanetprotocols.com/products.html>  
[http://www.instrucontrol.com/protocolos\\_digitales/sld004.htm](http://www.instrucontrol.com/protocolos_digitales/sld004.htm)  
[http://pomelo.ivia.es/mecanizacion/www/Manual\\_Electronica/redes1.htm](http://pomelo.ivia.es/mecanizacion/www/Manual_Electronica/redes1.htm)  
<http://www.anybus.com/>  
[http://claymore.engineer.gvsu.edu/~jackh/books/plcs/chapters/plc\\_intro.pdf](http://claymore.engineer.gvsu.edu/~jackh/books/plcs/chapters/plc_intro.pdf)  
[http://www.bairesrobotics.com.ar/data/Sistemas\\_Comunicaciones\\_R3\\_Silica.pdf](http://www.bairesrobotics.com.ar/data/Sistemas_Comunicaciones_R3_Silica.pdf)  
[http://www.ditel.es/pub/downloads/reguladores/Modbus\\_Akros\\_Cas.pdf](http://www.ditel.es/pub/downloads/reguladores/Modbus_Akros_Cas.pdf)  
[http://www.dte.upct.es/personal/manuel.jimenez/docencia/GD6\\_Comunic\\_Ind/pdfs/Tema%206.pdf](http://www.dte.upct.es/personal/manuel.jimenez/docencia/GD6_Comunic_Ind/pdfs/Tema%206.pdf)  
[http://www.dte.upct.es/personal/manuel.jimenez/docencia/GD6\\_Comunic\\_Ind/pdfs/Tema%207.pdf](http://www.dte.upct.es/personal/manuel.jimenez/docencia/GD6_Comunic_Ind/pdfs/Tema%207.pdf)  
<http://www.isa.uma.es/personal/jafma/docencia/sdca19992000/transp1.pdf>  
<http://www.isa.uniovi.es/docencia/redes/tema9.pdf>  
[http://www.uv.es/~rosado/sid/Capitulo3\\_rev0.pdf](http://www.uv.es/~rosado/sid/Capitulo3_rev0.pdf)  
<http://www.knowthebus.org/fieldbustech/profibus.asp>  
[http://www.nwfusion.com/archive/2000/101451\\_07-10-2000.html](http://www.nwfusion.com/archive/2000/101451_07-10-2000.html)  
[http://www.automatas.org/modbus/intr7.html#BM0\\_2\\_\\_QCQPYD\\_MGAZ6D\\_D1](http://www.automatas.org/modbus/intr7.html#BM0_2__QCQPYD_MGAZ6D_D1)  
<http://neutron.ing.ucv.ve/revista-e/No4/RCI.html>  
<http://www.isa.uniovi.es/docencia/redes/>  
[http://www.serck-controls.com/Technology/ThirdParty/DNP3\\_Capabilities.asp](http://www.serck-controls.com/Technology/ThirdParty/DNP3_Capabilities.asp)  
<http://www.kvaser.com/can/protocol/index.htm>