Manual de laboratorio:
Redes de comunicación industrial

Erick Pérez P.
erickpatriciopp9@gmail.com

Este manual tiene como objetivo servir como guía para la implementación de redes de comunicación industrial. El documento contiene una introducción teórica a los protocolos más utilizadas en las industrias para formar una red de comunicación entre dispositivos de control y actuadores y/o sensores.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción teórica

1.1. Protocolo MODBUS

MODBUS es un protocolo de mensajería de capa de aplicación, ubicado en el nivel 7 del modelo OSI, que proporciona comunicación cliente/servidor entre dispositivos conectados en diferentes tipos de buses o redes. MODBUS es un protocolo de solicitud/respuesta y ofrece servicios especificados por códigos de función. Los códigos de función MODBUS son elementos de las PDU de solicitud/respuesta MODBUS. Las comunicaciones Modbus son de dos tipos:

- Consulta/respuesta (comunicaciones entre un maestro y un esclavo).
- Difusión (un maestro envía un comando a todos los esclavos).

Actualmente se implementa usando:

- TCP/IP sobre Ethernet.
- Transmisión en serie asíncrona a través de una variedad de medios (cable: EIA/-TIA -232-E, EIA-422, EIA/TIA-485-A; fibra, radio, etc.).
- MODBUS PLUS, una red de paso de tokens de alta velocidad (HLC - High level Data Link Control).

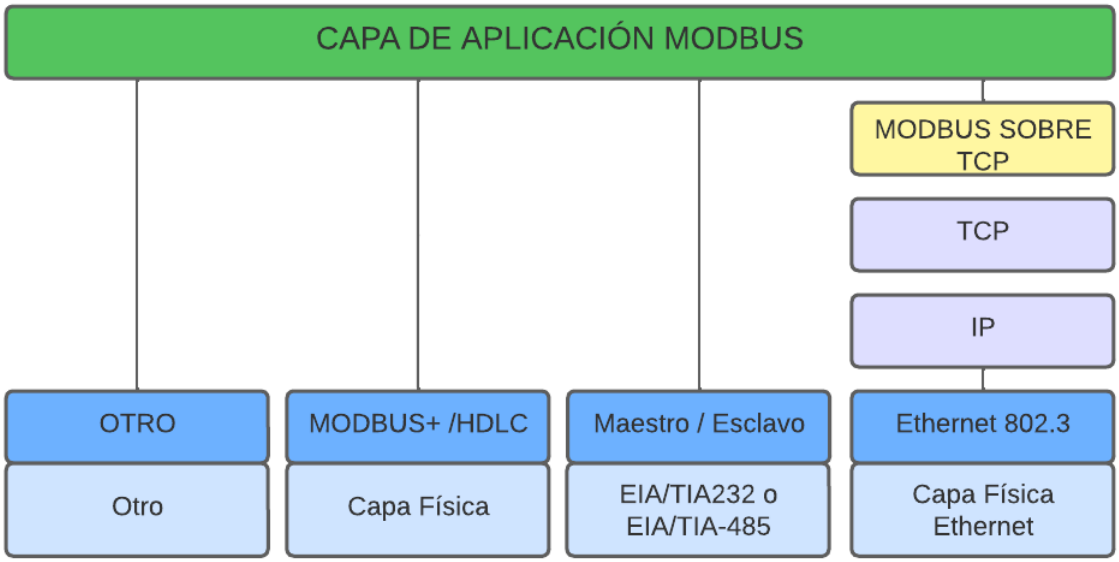


Figura 1.1: Pila de comunicación MODBUS.

1.1.1. Trama MODBUS

Una transacción Modbus comprende una única trama de consulta o respuesta, o una única trama de difusión.

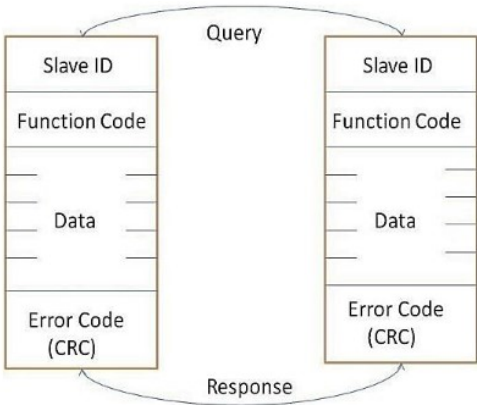


Figura 1.2: Comunicación master/esclavo MODBUS RTU.

Un mensaje de trama Modbus contiene la dirección del receptor previsto, el comando que el receptor debe ejecutar y los datos necesarios para ejecutar el comando. Tal y como se indica en la Figura 1.3

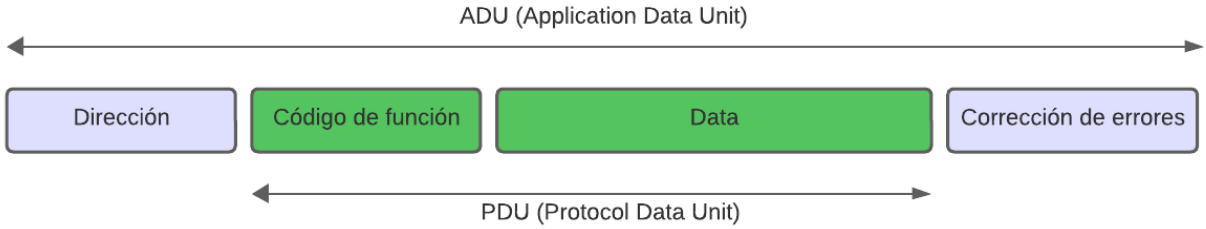


Figura 1.3: Trama MODBUS.

El protocolo MODBUS define una unidad de datos de protocolo (PDU) simple independiente de las capas de comunicación subyacentes. El mapeo del protocolo MODBUS en buses o redes específicas puede introducir algunos campos adicionales en la unidad de datos de la aplicación (ADU). La unidad de datos de la aplicación MODBUS la construye el cliente que inicia una transacción MODBUS.

El campo de código de función de una unidad de datos MODBUS está codificado en un byte. Los códigos válidos están en el rango de 1 a 255 decimales (el rango de 128 a 255 está reservado y se utiliza para respuestas de excepción). La función indica al servidor qué tipo de acción realizar.

El campo de datos de los mensajes contiene información adicional que el servidor utiliza para realizar la acción definida por el código de función. Esto puede incluir elementos como direcciones discretas y de registro, la cantidad de elementos que se manejarán y el recuento de bytes de datos reales en el campo. El campo de datos puede ser inexistente (de longitud cero) en ciertos tipos de solicitudes, ya que el código de función por sí solo especifica la acción.

El tamaño del PDU MODBUS está limitado por la restricción de tamaño heredada de la primera implementación MODBUS en la red de línea serie (máx. RS485 ADU = 256 bytes). Por lo tanto:

$$MODBUS\ \textbf{PDU}\ (com.\ serial) = 256 - Server\ address\ [1\ byte] - CRC\ [2\ bytes]$$

$$MODBUS\ \textbf{PDU}\ (com.\ serial) = \textbf{253 bytes}$$

Como consecuencia:

$$RS232/RS485\ \textbf{ADU} = \textbf{253 bytes} + Server\ address\ [1\ byte] + CRC\ [2\ bytes]$$

$$RS232/RS485\ \textbf{ADU} = \textbf{256 bytes}$$

Además,

$$TCP\ MODBUS\ \textbf{ADU} = \textbf{253 bytes} + MBAP\ [7\ bytes] = \textbf{260 bytes}$$

El protocolo MODBUS define tres PDU. Ellos son:

- MODBUS Request PDU
- MODBUS Response PDU
- MODBUS Exception Response PDU

Los PDUs de solicitud y respuesta se conforma por la función de código y su data. Estos campos depende del código de función y normalmente contiene información

como referencias de variables, recuentos de variables, compensaciones de datos, códigos de subfunción, etc. Su tamaño depende de la información que conlleve, es decir $n\ bytes$. Así mismo, el PDU de excepción contiene la función de código de 1 $byte$, pero en este caso se agrega la data solicitada (request data).

1.1.2. Características principales

Codificación de datos

MODBUS utiliza una representación 'big-Endian' para direcciones y elementos de datos. Esto significa que cuando se transmite una cantidad numérica mayor que un byte, el byte más significativo se envía primero. Así por ejemplo:

$$Tamaño\ de\ registro = 16\ bits$$

$$Valor = 0x1234$$

En este caso, el primer byte enviado en $0x12$ y luego $0x34$.

Modelo de datos MODBUS

MODBUS basa su modelo de datos en una serie de tablas que tienen características diferenciadoras. Las cuatro tablas principales son:

Tablas primarias	Tipo de objeto	Tipo	Descripción
Entradas discretas	1-bit	Lectura	Este tipo de datos puede ser proporcionado por un sistema de E/S.
Coils (bobinas)	1-bit	Escritura	Este tipo de datos puede ser alterado por un programa de aplicación.
Registros de entrada	palabra de 16-bits	Lectura	Este tipo de datos puede ser proporcionado por un sistema de E/S.
Registros de retención	palabra de 16-bits	Escritura	Este tipo de datos puede ser alterado por un programa de aplicación.

Tabla 1.1: Tablas primarias MODBUS.

Estos bancos de datos definen el tipo y los derechos de acceso a los datos contenidos y son identificados generalmente a través de un rango de direcciones: coils (0xxxx), entradas discretas (1xxxx), registros de entrada (3xxxx) y registros de retención (4xxxx). Para cada una de las tablas primarias, el protocolo permite la selección individual de 65536 elementos de datos, y las operaciones de lectura o escritura de esos elementos están diseñadas para abarcar múltiples elementos de datos consecutivos hasta un límite de tamaño de datos que depende del código de función de transacción.

MODBUS sobre TCP/IP

El protocolo Modbus se puede implementar sobre varias redes de comunicación diferentes, incluidas serie, TCP/IP y UDP. En la implementación de TCP/IP, el protocolo Modbus se envía como datos de la capa de aplicación. No hay autenticación, autorización ni cifrado del protocolo. El protocolo Modbus en sí tampoco tiene capacidad para manejar estas funciones. Por lo tanto, cualquier solicitud con el formato adecuado se considera válida y se responde a ella. El protocolo Modbus en sí se puede dividir en seis secciones:

1. **Identificador de transacción:** un campo de 2 bytes que se utiliza para correlacionar solicitudes y respuestas. Este campo suele ser fácilmente predecible debido a una mala aleatorización.
2. **Identificador de protocolo:** un campo de 2 bytes que siempre es 0 para Modbus.
3. **Longitud de campo:** un campo de 2 bytes que indica el número de bytes restantes en la carga útil de Modbus.
4. **Identificador de unidad:** un campo de 1 byte que identifica el esclavo específico en una dirección IP. Puede haber hasta 254 esclavos diferentes en una única IP.
5. **Código de función:** un campo de 1 byte que indica la acción solicitada por el maestro. Pueden ser bobinas de lectura y escritura, registros de entrada, registros de retención o entradas discretas.
6. **Datos:** un campo de longitud variable, los valores asociados con los distintos códigos de función.

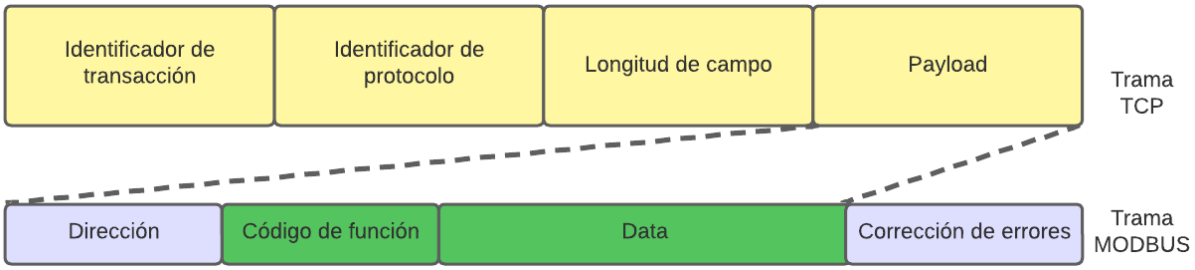


Figura 1.4: Trama MODBUS/TCP.

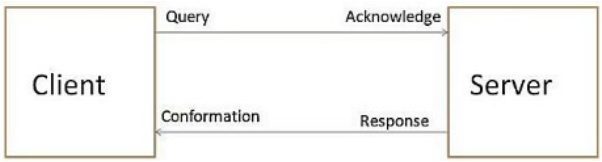


Figura 1.5: Comunicación master/esclavo MODBUS TCP.

RS-232

RS-232 (Recommended Standard 232), comúnmente conocido como RS-232 o EIA/TIA RS-232, se originó en la década de 1960 y representa un enfoque para la comunicación en serie de tipo asíncrono. En esta modalidad de comunicación, los dispositivos emplean una única conexión que contiene dos conjuntos de cables. En el marco de este protocolo, las señales de salida típicamente varían en el rango de $\pm 5V$ a $\pm 25V$. La interpretación por parte del dispositivo receptor es simple: cualquier voltaje por encima de +3 V se considera como un 0, mientras que cualquier voltaje por debajo de -3 V se interpreta como un 1, lo que permite una comunicación directa en formato binario.

Figura 1.6: Frame RS-232.

En una trama RS-232, el primer elemento es el bit de inicio, desempeñando la función crucial de informar al dispositivo receptor que se avecina la transmisión de datos. Este aspecto adquiere especial relevancia debido a la naturaleza asíncrona del protocolo RS-232. A continuación, siguen los bits de datos, que pueden variar en número de 5 a 9 bits, aunque la configuración más común emplea 8 bits. Luego se encuentra el bit de paridad, destinado a verificar la presencia de errores. El sistema detectará un error si detecta un número par de bits de datos. Por último, se halla el bit de parada, que especifica intervalos de 1, 1.5 o 2 bits antes de que sea posible transmitir el próximo bit de inicio.
Las señales utilizadas en este protocolo son:

- Request To Send (RTS)
- Clear To Send (CTS)
- DATA Terminal Ready (DTR)
- Data Set Ready (DSR)
- Receive Signal Line Detect (RSLD)
- Transmit Data (TD)
- Receive Data (RD)

RS-485

RS-485, también referido como EIA/TIA-485, es una interfaz estándar en la capa física de comunicación que ocupa un lugar primordial en el modelo OSI, diseñada con el propósito de mejorar las capacidades físicas de la interfaz RS-232. La conexión en serie utilizando EIA-485 se establece a través de un cable compuesto por dos o

tres conductores: uno destinado a la transmisión de datos, otro para la transmisión de datos invertidos y, en muchas ocasiones, un tercer conductor que desempeña la función de conexión a tierra (0 V). Esto habilita a los transmisores y receptores para intercambiar información a través de un cable de par trenzado conformado por hilos sólidos de calibre 22 o 24 AWG.

Uno de los cables transmite la señal original y el otro transporta su copia inversa. Este método de transmisión ofrece una gran resistencia a las interferencias en modo común. Este permite enviar datos a largas distancias y a velocidades relativamente altas, que pueden alcanzar **100 kbits/s a 1200 metros**. Además permite la comunicación sobre: Transmisión de datos bidireccional semidúplex, canal de comunicación simétrico, y comunicación multipunto.

Inicio	Dirección de dispositivo	Data	Paridad	Fin
1 char	2 char	n char	4 char	2 char
:	01 ... 31	comandos	****	\r\n

Figura 1.7: Estructura RS-485.

- El comienzo del comando se indica con dos puntos :.
- La dirección del dispositivo corresponde a la dirección necesaria para activar el sensor correcto en una red con varios sensores. La dirección del dispositivo 01 … 31 se puede programar en el sensor. Los sensores de la misma red no deben tener la misma dirección de dispositivo. La dirección estándar del dispositivo es 01.
- Hay 2 tipos diferentes de CARGA ÚTIL:
  - Codificación legible: desarrollada para controlar el sensor con un programa terminal
  - Codificación automática: desarrollada para garantizar una comunicación eficiente y confiable entre dispositivos
- El CHECKSUM se utiliza para comprobar la transmisión correcta. Consta de los valores INICIO, DIRECCIÓN DEL DISPOSITIVO y CARGA ÚTIL y siempre tiene 4 dígitos. El cálculo se realiza con: CRC16-ARC / CRC-IBM
- El final del frame o comando está marcado por la combinación de 4 dígitos \r\n. Importante: Este comando siempre debe enviarse como HEX

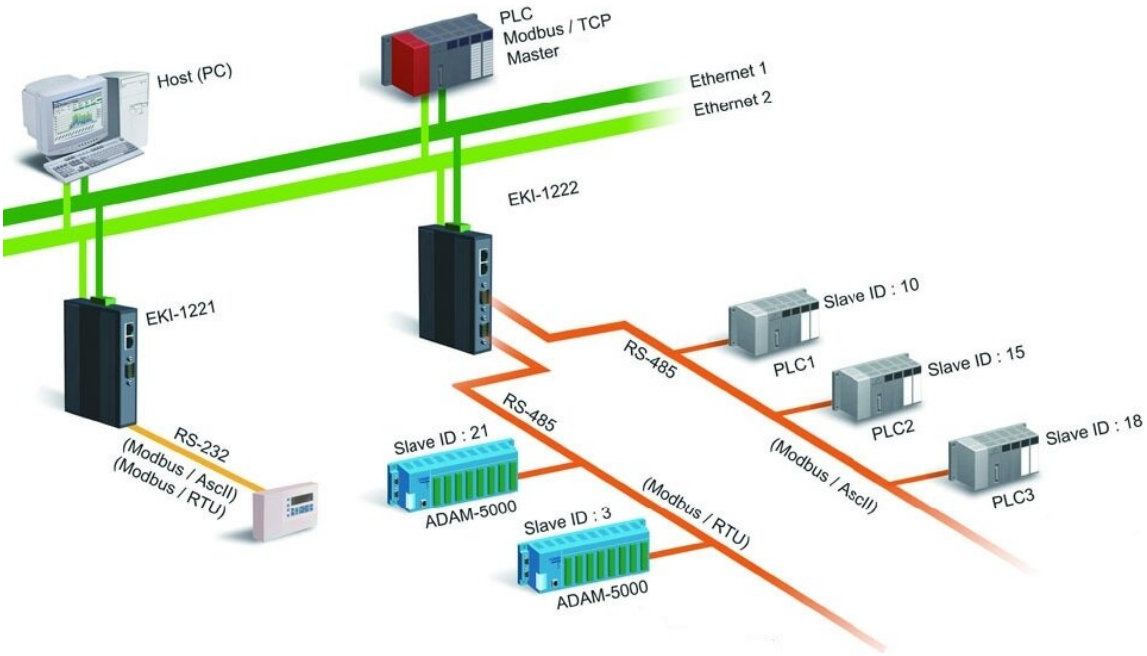


Figura 1.8: Ejemplo de red industrial con protocolo MODBUS.

1.2. HART

HART, un protocolo de comunicación diseñado para su aplicación en entornos industriales de medición y control, **es considerado un protocolo "híbrido" en virtud de su capacidad para facilitar tanto la comunicación analógica como la digital**. Este protocolo emplea una señal analógica de 4-20 mA para transmitir una variable específica, al mismo tiempo que transporta información adicional mediante la modulación de una señal digital de bajo nivel que se superpone de forma transparente a la señal analógica, sin que esto afecte la precisión de la medición, dado que dicha interferencia se puede eliminar mediante técnicas convencionales de filtrado.

1.2.1. Características principales

- **Comunicación Digital sobre Señales Analógicas:** permite que los dispositivos HART convivan con instrumentos analógicos tradicionales en el mismo bucle de control.
- **Comunicación en Dos Sentidos**: permite que los dispositivos de campo no solo pueden enviar datos medidos, sino también recibir comandos y configuraciones.
- **Modo Maestro-Esclavo:** los dispositivos maestros pueden solicitar información a los dispositivos esclavos de manera individual. Esto permite la gestión de múltiples dispositivos en una misma red.
- **Flexibilidad en la Configuración:** permite ajustar los parámetros de medición y realizar diagnósticos sin necesidad de acceder físicamente al dispositivo.

- **Mensajes Digitales y Analógicos:** HART puede transmitir tanto datos digitales como analógicos. Los datos digitales se utilizan para la configuración y el diagnóstico, mientras que los datos analógicos representan las mediciones reales.
- **Seguridad y Redundancia:** permiten una comunicación confiable en entornos industriales críticos.
- **Diagnóstico Avanzado:** que permite a los usuarios identificar y solucionar problemas en tiempo real y reducir el tiempo de inactividad.
- **Reducción de Costos de Cableado:** Al utilizar la comunicación digital, HART puede reducir la cantidad de cableado necesario en comparación con métodos analógicos.

1.2.2. Trama HART

HART es un protocolo de comunicación de naturaleza híbrida que combina tanto la comunicación analógica como la digital y ha sido especialmente diseñado para aplicaciones de medición en entornos industriales. La versión predominante y original de HART utiliza la modulación FSK (Frequency Shift Keyed). Este protocolo HART opera en el rango de frecuencias bajas (1200 y 2200 Hz), lo que limita su velocidad de transmisión a 1200 baudios. Además, se caracteriza como un protocolo Maestro-Esclavo, donde es posible tener hasta dos maestros HART y hasta 15 dispositivos HART conectados a un único par de cables en una configuración de conexión de tipo Punto Multipunto.

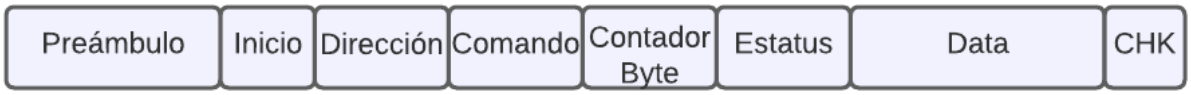


Figura 1.9: Frame HART

- **Preámbulo:** Consiste de entre cinco a veinte caracteres hexadecimales FF. Esto permite al receptor sincronizarse con la señal de frecuencia y la cadena de caracteres entrante. Su tamaño varía de 5 a 20 bytes.
- **Caracter de Inicio:** en un mensaje HART puede tener varios posibles valores, indicando cual formato de mensaje se está usando, la fuente del mensaje, y si el mensaje está en "modo burst".

Tipo de mensaje	**Formato corto**	Formato largo
Maestro a esclavo	02	82
Esclavo a maestro	06	86
Mensaje burst de esclavo	01	81

- **Dirección:** Este campo incluye tanto la dirección del maestro (un bit: 1 para maestro primario, 0 para maestro secundario) y la dirección del esclavo. En el formato corto, la dirección del esclavo es de 4 bits que contienen la "dirección de barrido" o "polling address " (0 a 15). En el formato largo, la dirección del

esclavo es de 38 bits que contienen el "identificador único" para ese dispositivo en particular. Su tamaño varía de 1 a 5 bytes.

- **Comando:** Este byte contiene el comando HART del mensaje. Los comandos Universales están en el rango de 0 a 30; los comandos de práctica común están en el rango de 32 a 126; y los comandos específicos del dispositivo están en el rango de 128 a 253.
- **Conteo de Bytes:** Contiene la cantidad de bytes que hay entre los bytes de Estatus y Data.
- **Estado:** Este campo solo está presente en la respuesta de un esclavo. Contiene información acerca de los errores de comunicación que ocurrieron en el mensaje, el estado del comando recibido, y el estado del dispositivo. Esta información se muestra en dos bytes.
- **Data:** No todos los comandos o respuestas contienen Data. La data puede venir en forma de enteros sin signo, números en punto flotante o cadena de caracteres ASCII. El número de bytes de data, y el formato usado en la data son específicos para cada comando.
- **Suma de Verificación (Checksum):** Esto se usa para detectar errores en la comunicación.

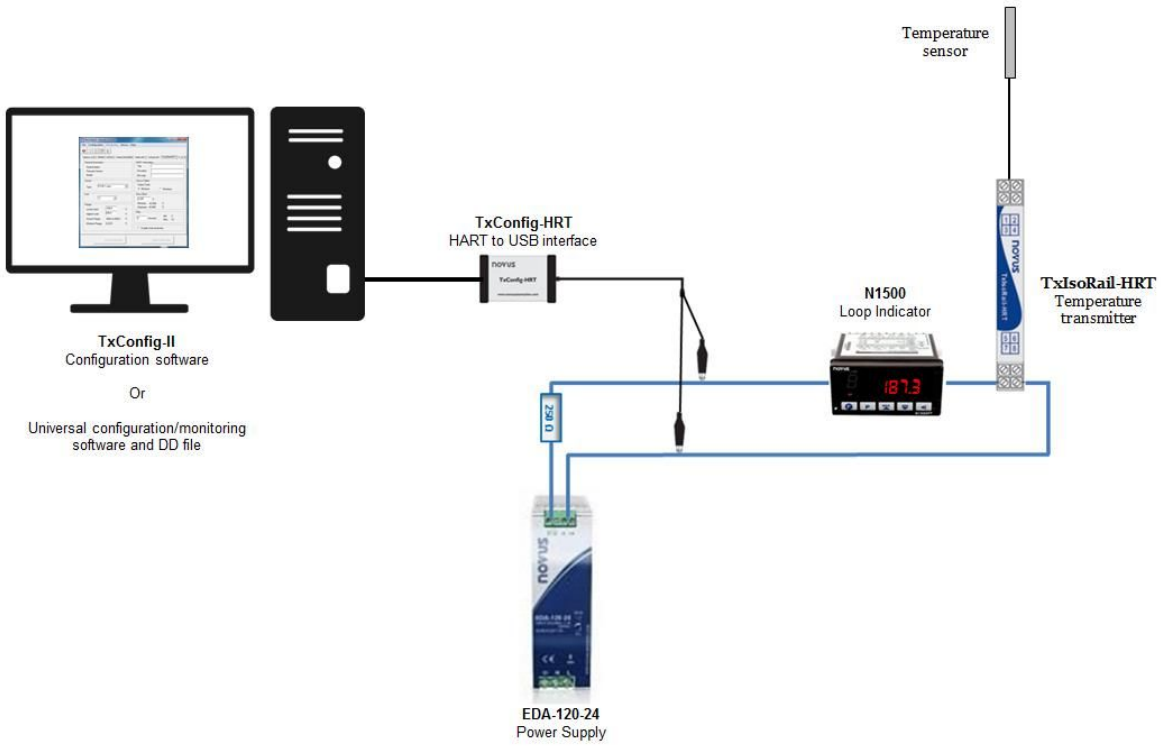


Figura 1.10: Ejemplo de red industrial con protocolo HART.

1.3. PROFIBUS

PROFIBUS se basa en la utilización de la interfaz RS-485, que es un estándar de comunicación serial. En una red PROFIBUS, se establece una distinción entre los componentes denominados maestros y los esclavos PROFIBUS. Los maestros pueden ser dispositivos como controladores lógicos programables (PLCs), controladores de automatización programable (PACs) o sistemas de control distribuido (DCS), entre otros. En cambio, los esclavos engloban una amplia variedad de dispositivos, que incluyen accionamientos, motores, módulos de entrada/salida, sensores, equipos de campo, robots, actuadores y otros dispositivos similares.

PROFIBUS se divide en dos variantes: PROFIBUS DP (Periféricos Descentralizados) y PROFIBUS PA (Automatización de Procesos). En términos generales, la idea central de PROFIBUS es **consolidar múltiples entradas y salidas de campo en un solo dispositivo de E/S local** y luego transmitir estos datos a través de un único cable hacia el dispositivo maestro.

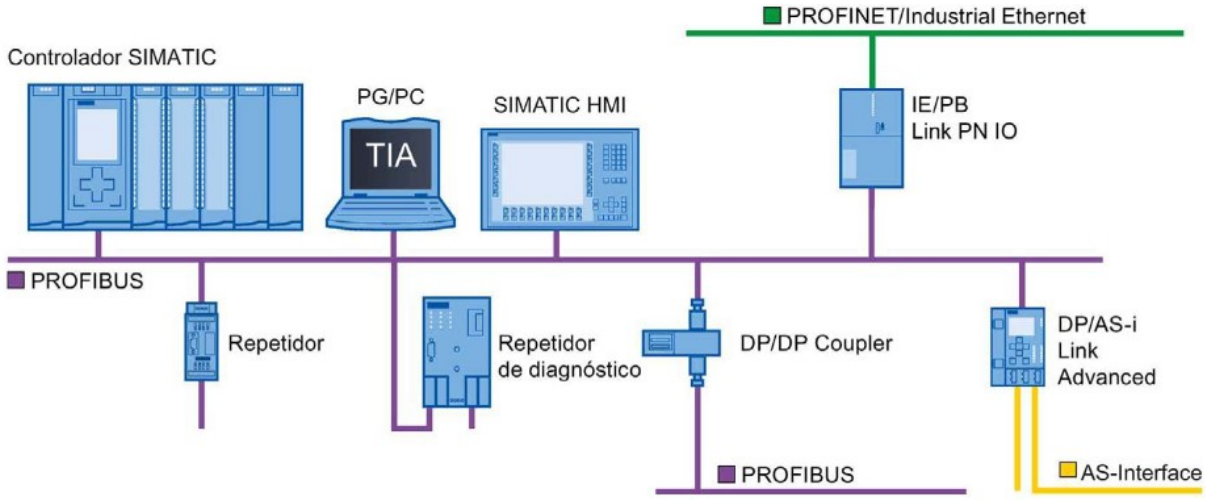


Figura 1.11: Ejemplo de red industrial con protocolo PROFIBUS.

Este enfoque contribuye al ahorro de costos al eliminar la necesidad de hardware y cableado adicional. Además, simplifica las tareas de ingeniería, facilitando la instalación, el mantenimiento y la resolución de problemas de la red.

PROFIBUS PA	- Diseñado para automatización de procesos. - Permite la conexión de sensores y actuadores a una línea de bus común incluso en áreas especialmente protegidas. - Permite la comunicación de datos y energía en el bus mediante el uso de 2 tecnologías (norma IEC 1158-2)
PROFIBUS DP	- Optimizado para alta velocidad. - Conexiones sencillas y baratas. - Diseñada especialmente para la comunicación entre los sistemas de control de automatismos y las entradas/salidas distribuidas.
PROFIBUS FMS	- Solución general para tareas de comunicación a nivel de célula. - Gran rango de aplicaciones y flexibilidad. - Posibilidad de uso en tareas de comunicación complejas y extensas.

Tabla 1.2: Variantes PROFIBUS.

1.3.1. Características principales

- **Variedad de Tipos:** PROFIBUS se presenta en dos tipos principales: PROFIBUS DP (Decentralized Peripherals) y PROFIBUS PA (Process Automation).
- **Comunicación en Tiempo Real:** PROFIBUS DP permite la comunicación en tiempo real entre dispositivos de campo, controladores lógicos programables (PLC) y otros dispositivos de control.
- **Topología de Bus:** los dispositivos se conectan en serie a un solo cable. Esto reduce la cantidad de cableado requerido y facilita la expansión de la red.
- **Detección de Errores y Diagnóstico**: incorpora funciones avanzadas de diagnóstico y detección de errores que permiten a los usuarios supervisar el estado de la red y los dispositivos de campo.
- **Flexibilidad de Configuración:** permite la asignación de direcciones a dispositivos de campo. Los dispositivos pueden ser configurados y reconfigurados de forma remota.
- **Velocidades Variables:** PROFIBUS DP permite ajustar la velocidad según las necesidades de la aplicación.
- **Comunicación en Serie y Paralelo:** PROFIBUS DP admite tanto la comunicación en serie (para datos de proceso) como la comunicación en paralelo (para datos acíclicos y de configuración).
- **Amplia Adopción:** ampliamente utilizado en diversas industrias, incluyendo la automotriz, manufacturera y de automatización de procesos.

1.3.2. Trama PROFIBUS

La trama PROFIBUS admite 3 tipos de formato: tramas de longitud fija sin datos, tramas de longitud fija con datos y tramas de longitud variable.

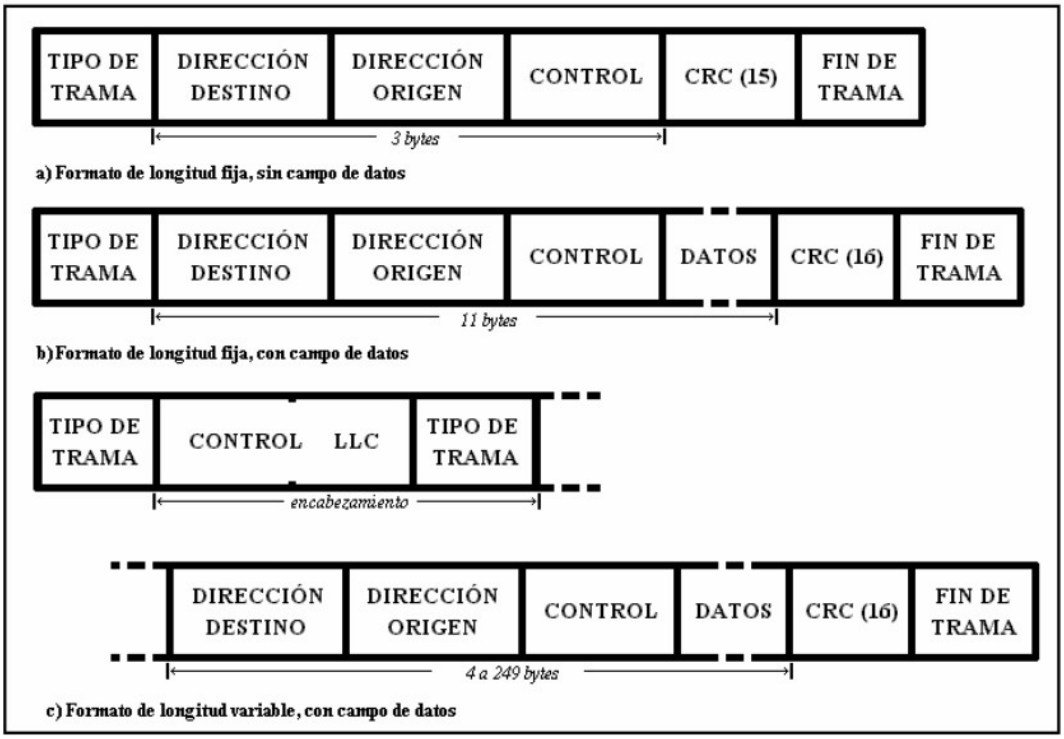


Figura 1.12: Tramas PROFIBUS.

1.4. PROFINET

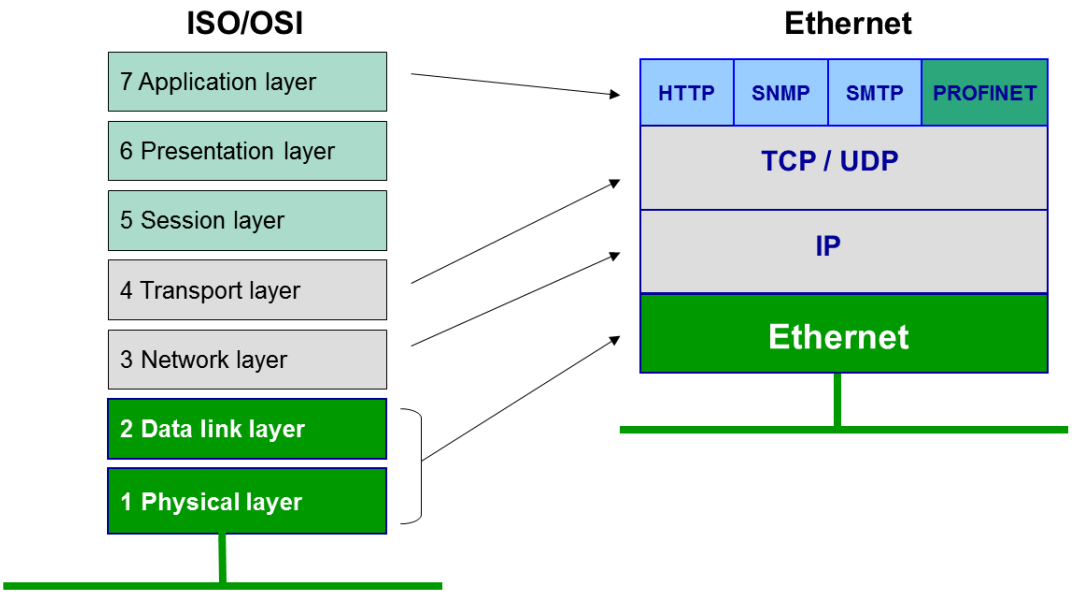


Figura 1.13: Bloques de construcción del sistema PROFINET

PROFINET se fundamenta en la tecnología estándar Ethernet. Aunque los cables Ethernet convencionales pueden ser utilizados en redes PROFINET, generalmente se prefieren cables específicos de PROFINET. Estos cables son esencialmente versiones reforzadas de cables Ethernet diseñados para soportar las condiciones desafiantes presentes en entornos industriales. PROFINET comprende una gama de controladores, como PLCs, PACs y DCS, así como sensores, actuadores, robots, lectores RFID y otros dispositivos de entrada/salida. En el contexto de PROFINET, estos elementos son referidos como controladores y dispositivos, respectivamente. PROFINET es compatible con tecnologías como WLAN y Bluetooth, según su especificación, lo que permite conexiones inalámbricas sin restricciones, incluso para la transmisión de mensajes de seguridad funcional (PROFIsafe).

1.4.1. Características principales

- **Ethernet Industrial:** se basa en Ethernet industrial y utiliza las ventajas de la tecnología Ethernet para la comunicación en tiempo real en aplicaciones industriales.
- **Determinismo:** es capaz de garantizar tiempos de ciclo constantes y predecibles.
- **Comunicación en Tiempo Real:** adecuado para aplicaciones donde se requiere una respuesta rápida y precisa.
- **Topologías Variadas:** admite una variedad de topologías, incluyendo la topología de estrella, la de anillo, la de línea, entre otras.
- **Integración de Datos:** permite la integración de datos de proceso y datos de diagnóstico en una única red.
- **Capacidades de Diagnóstico Avanzadas:** permite la supervisión del estado de los dispositivos y la identificación rápida de problemas.
- **Redes de Control y Automatización Integradas:** es compatible con redes de control y automatización de edificios.
- **Aplicaciones Diversas:** se utiliza en una amplia gama de aplicaciones industriales, incluyendo la automatización de fábricas, sistemas de control de procesos, robótica y maquinaria industrial.
- **Compatibilidad con PROFIBUS:** PROFINET permite la integración de dispositivos PROFIBUS, lo que facilita la migración de sistemas basados en PROFIBUS a PROFINET.

En las redes PROFINET se puede transportar flujos de datos en tiempo real y no en tiempo real. Estos flujos se dividen en dos clases: Clase 1 y Clase 2. La primera hace referencia a los flujos en tiempo real, mientras que la segunda es lo opuesto. Además, existe una evolución de los flujos de datos de en tiempo real y se denomina clase 3. La siguiente tabla describe las características principales de las clases de flujos de datos en PROFINET.

Característica	PROFINET Clase 1	PROFINET Clase 2	PROFINET Clase 3
Aplicaciones típicas	Control en tiempo real, automatización crítica.	Monitoreo y supervisión, aplicaciones no críticas en tiempo real.	Control de movimiento, aplicaciones de alta precisión en tiempo real.
Determinismo	Alto (tiempo real crítico)	Bajo a moderado (menos crítico en tiempo real)	Muy alto (alta precisión y determinismo)
Latencia	Muy baja	Puede variar más que Clase 1	Muy baja
Comunicación isócrona	No	No	Sí
Priorización de tráfico	Sí	No	Sí
Sincronización de dispositivos	Sí	Puede variar más que Clase 1	Sí
Redundancia de red	Posible	Posible	Posible
Tolerancia a fallos	Alta	Menos crítica que Clase 1	Alta
Aplicaciones comunes	PLC, controladores de lógica, E/S remotas.	Supervisión, HMI, adquisición de datos.	Control de movimiento, sistemas de visión.

Tabla 1.3: Clases de flujos de datos en PROFINET.

1.4.2. Trama PROFINET

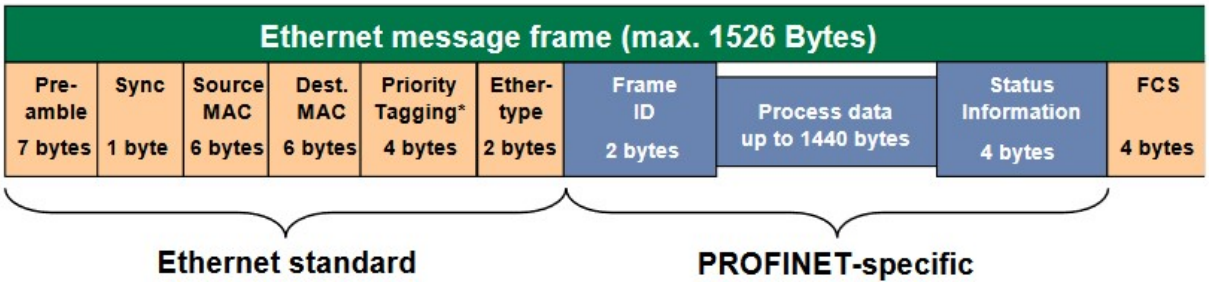


Figura 1.14: Trama PROFINET

PROFINET utiliza 3 servicios de comunicación:

- **Standard TCP/IP:** Este servicio se utiliza para funciones no deterministas, como parametrización, transmisiones de vídeo/audio y transferencia de datos a sistemas TI de nivel superior.
- **Real Time:** Las capas TCP/IP no son utilizadas para dar un rendimiento determinista a las aplicaciones de automatización, funcionando con unos tiempos de retardo en el rango 1-10ms. Este hecho representa una solución basada en software adecuada para aplicaciones típicas de E/S, incluyendo control de movimiento y requisitos de alto rendimiento.

- **Isochronous Real Time:** La priorización de señal y la conmutación programada proporcionan una sincronización de alta precisión para aplicaciones como el control de movimiento. Las velocidades de ciclo en rangos de sub-milisegundos son posibles, con jitter (variabilidad temporal durante el envío de señales digitales) en el rango de sub-microsegundos.

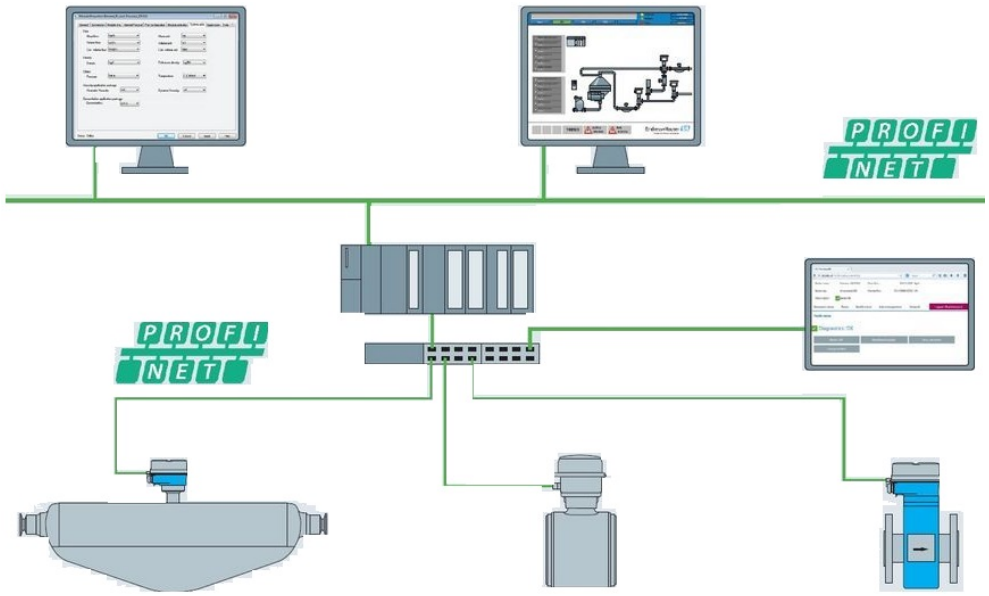


Figura 1.15: Ejemplo de red industrial con los protocolos PROFINET.

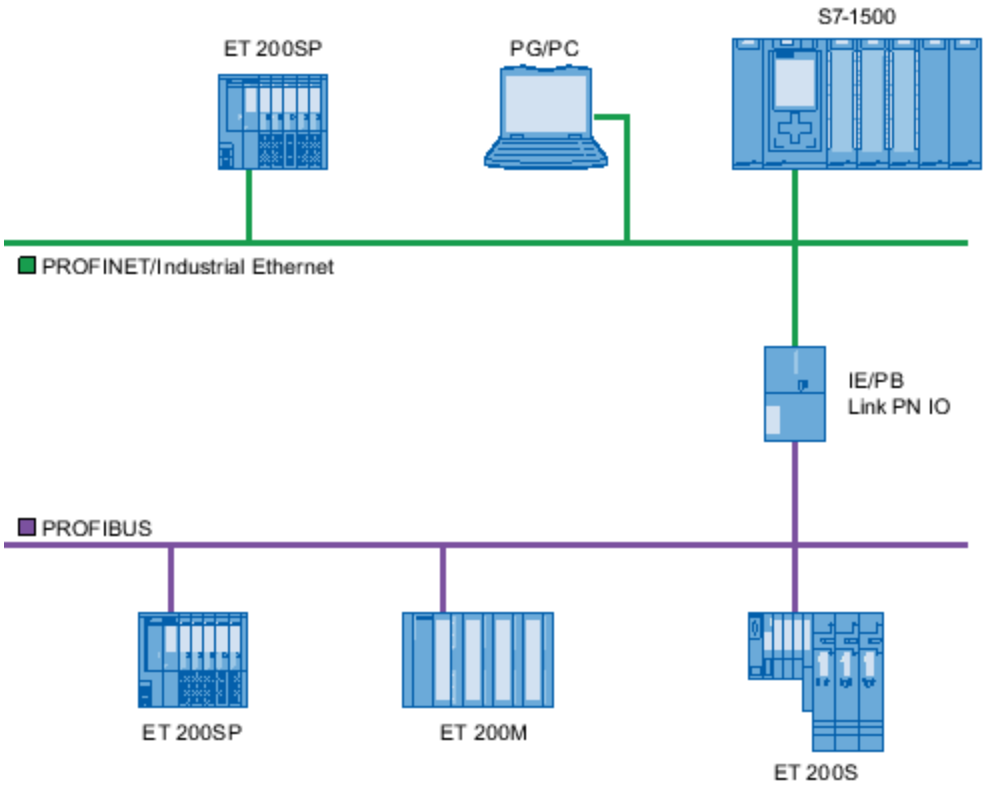


Figura 1.16: Ejemplo de red industrial con los protocolos PROFIBUS/PROFINET.

1.5. DeviceNet

DeviceNet es una de las redes que ha adoptado el concepto de productor/consumidor, lo que implica que los datos generados por un único emisor en la red se transmiten de forma simultánea a todos los posibles receptores, quienes tienen la autonomía de decidir si desean atender o no el mensaje que han recibido. Esta aproximación conlleva ventajas, tales como una **utilización más eficiente del ancho de banda** y una mejora en la velocidad de respuesta de la red.

Adicionalmente, DeviceNet se configura como una red de comunicación digital multipunto concebida para enlazar sensores, actuadores y sistemas de automatización industrial en distintos contextos. Su desarrollo se enfocó en conseguir una notable flexibilidad entre los dispositivos de campo y asegurar la interoperabilidad entre equipos procedentes de diversos fabricantes en la industria.

1.5.1. Características principales

- Puede albergar un máximo de 64 nodos por red, en topología de bus con derivaciones. Los nodos son direccionados de 0 a 63. Un nodo DeviceNet es modelado por un conjunto de objetos CIP, los cuales encapsulan datos y servicios y determinan así mismo su comportamiento.
- Distancia máxima: 100 m a 500 m. Puede alcanzar los 6 km con el uso de repetidores, alcanzando de 125, 250 y 500 Kbps.
- Emplea dos pares trenzados: control y alimentación.
- Transmisión basada en el modelo productor/consumidor con un empleo eficiente de ancho de banda y mensajes desde 1 byte.
- Reemplazo automático de nodos, no requiere de programación y elevado nivel de diagnósticos.

Tipos de datos:

Datos cíclicos	Datos provenientes de sensores y actuadores, directamente relacionados al control. Estos datos representan las actualizaciones regulares y programadas que se transmiten entre los dispositivos de campo. Además, los datos cíclicos son esenciales para el monitoreo en tiempo real y el control de los procesos industriales.
Datos no cíclicos	Datos indirectamente relacionados al control, como configuración y diagnóstico. Estos datos son mensajes de información intercambiados eventualmente durante la configuración o diagnóstico del equipo de campo.

Tabla 1.4: Tipos de datos en DeviceNet.

1.5.2. Trama DeviceNet

La trama transmitida por DeviceNet sigue una estructura específica que consta de varios campos. Incluye 1 bit de inicio de trama, 11 bits que representan el identificador del equipo receptor y la prioridad, 1 bit RTR que indica si se trata de una trama remota o de datos, 6 bits para el campo de control, que especifica el número de datos que se están transmitiendo (de 0 a 8 bytes de información), seguidos de 2 bytes destinados a la detección de errores de transmisión (CRC). Luego, se incluyen 2 bits de acuse de recibo (ACK), seguidos de 7 bits para marcar el final de la trama y, finalmente, 3 bits para indicar el espacio entre tramas. La Figura 1.17 muestra la disposición de estos elementos en la trama.

Inicio	Identificador	RTR	Campo de control	Data	CRC	ACK	Final	Espaciado
1 bit	11 bits	1 bit	6 bits	0-8 bytes	2 bytes	2 bits	7 bit	3 bits

Figura 1.17: Trama DeviceNet.

1.5.3. Capa Física

La capa física y de acceso a la red en DeviceNet se basa en la tecnología CAN (Controller Area Network), mientras que las capas superiores operan bajo el protocolo CIP (Common Industrial Protocol). La estructura de los datos sigue las especificaciones del estándar CAN. Antes de que un dispositivo transmisor envíe una trama, lleva a cabo una escucha activa para verificar que la red esté desocupada, evitando de esta manera colisiones con otros dispositivos. Además, DeviceNet incluye detección de colisiones, lo que significa que si dos dispositivos intentan enviar una trama simultáneamente, ambos detienen la transmisión y el que tiene prioridad retransmite la trama primero. La trama transmitida por DeviceNet utiliza el protocolo CIP, lo que le confiere independencia con respecto a la capa física utilizada.

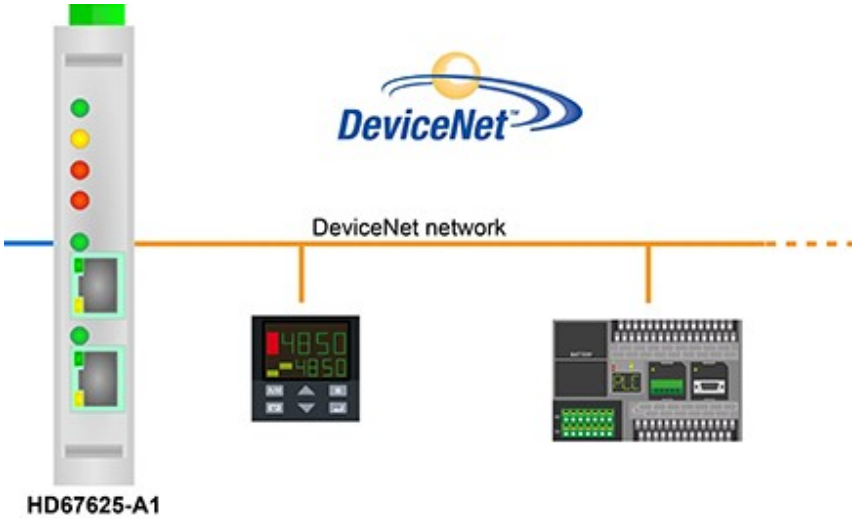


Figura 1.18: Ejemplo de red industrial con el protocolo DeviceNet.

1.6. Ethernet Industrial

Ethernet, conocida también como IEEE 802.3, es uno de los estándares más ampliamente aceptados en las comunicaciones de Red de Área Local (LAN). Este estándar permite la interconexión de dispositivos ubicados en proximidad geográfica a través de una red, lo que habilita la conexión de una cantidad que puede oscilar entre 100 y 1000 usuarios, con velocidades de transmisión que pueden variar desde 10 Mbps hasta 10 Gbps, dependiendo de la tecnología de transmisión empleada.

Este protocolo utiliza el método de transmisión conocido como CSMA (Carrier Sense Multiple Access) o acceso múltiple con detección de portadora y colisiones. Su funcionamiento inicia con la escucha y la comprobación de que la red se encuentre libre antes de transmitir una trama. Si la red está desocupada, el dispositivo procede a enviar la trama, y otros dispositivos en la red la reciben, si bien solo el destinatario designado examina la información contenida en la trama. En caso de que dos dispositivos intenten transmitir tramas simultáneamente, lo que provoca una colisión, ambos dispositivos interrumpen la transmisión y aguardan un período de tiempo aleatorio antes de intentar nuevamente la transmisión de la trama, lo que contribuye a evitar conflictos continuos.

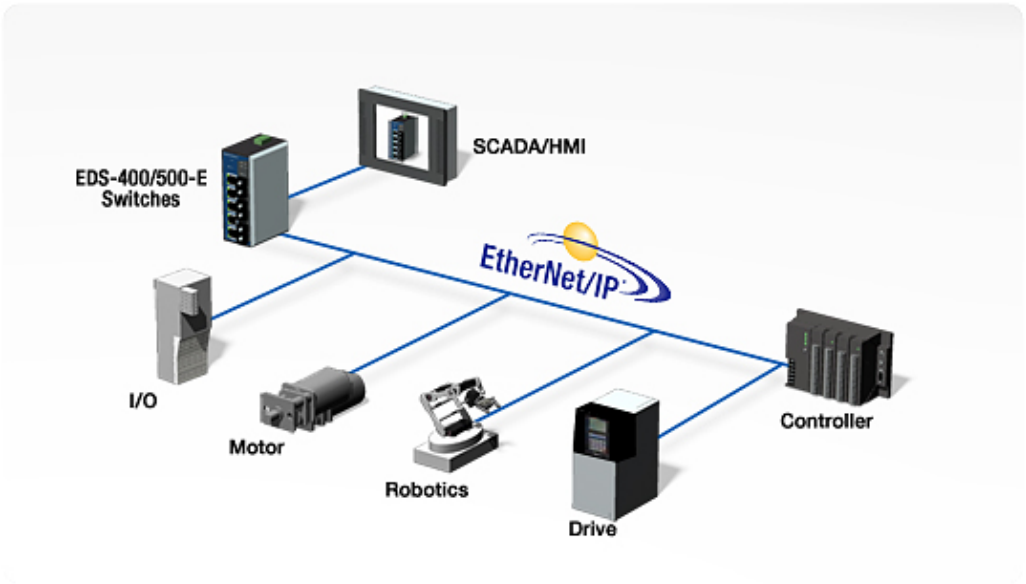


Figura 1.19: Ejemplo de red industrial con el protocolo Ethernet.

1.6.1. Características principales

- **Robustez y Durabilidad:** Ethernet industrial es resistente a las vibraciones, variaciones de temperatura, humedad y polvo.
- **Conectividad en Tiempo Real:** admite comunicaciones en tiempo real que son esenciales en aplicaciones de automatización industrial, donde se requiere una respuesta inmediata.
- **Redundancia:** garantiza la disponibilidad y la confiabilidad de la red.

- **Cableado Robusto:** utiliza cables y conectores industriales resistentes para garantizar una conexión estable y duradera.
- **Protocolos de Comunicación Específicos:** además de Ethernet IP, PROFINET y otros protocolos de Ethernet industrial, se utilizan para adaptarse a aplicaciones específicas en la automatización industrial.
- **Seguridad y Protección:** incorpora medidas de seguridad, como autenticación y cifrado.
- **Integración de Sistemas:** permite la integración de sistemas de control, dispositivos de campo, sensores y actuadores.

1.6.2. Trama Ethernet

La trama Ethernet consta de la dirección del equipo receptor, la dirección del equipo transmisor y el mensaje a transmitir. La longitud del mensaje puede variar en un rango de 64 a 1500 bytes, lo que resulta en un tiempo de transmisión que oscila entre 50 y 1200 microsegundos. Además, la trama incluye una sección de preámbulo al inicio de la transmisión, que está compuesta por 64 bits y ayuda a sincronizar con el receptor previsto. También incorpora una zona de redundancia cíclica o CRC de 32 bits que verifica la integridad de la trama para garantizar su corrección. La estructura de la trama Ethernet se puede visualizar en la Figura 1.20.

Adicionalmente, la trama Ethernet puede incluir una sección de "tipo de trama"que tiene como función identificar el tipo de datos que se está transmitiendo en el mensaje, lo que permite a las tramas autodeterminarse. El receptor de la trama utiliza esta información para determinar qué protocolo debe utilizar para procesar la trama. Esto habilita a un dispositivo a emplear varios protocolos en una misma red sin generar interferencias ni conflictos, lo que incrementa la flexibilidad y versatilidad de la comunicación en la red Ethernet.

Preámbulo	Dirección destino	Dirección origen	Tipo	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Figura 1.20: Trama Ethernet.

1.6.3. Capa Física

Estándar Ethernet	Denominación	Velocidad de datos	Tecnología de cables
802.3	10Base5	10 MB/s	Cable coaxial
802.3a	10Base2	10 MB/s	Cable coaxial
802.3i	10Base-T	10 MB/s	Cable de par trenzado
802.3j	10Base-FL	10 MB/s	Cable de fibra óptica
802.3u	100Base-TX 100Base-FX 100Base-SX	100 MB/s	Cable de par trenzado, cable de fibra óptica
802.3z	1000Base-SX 1000Base-LX	1 GB/s	Cable de fibra óptica
802.3ab	1000Base-T	1 GB/s	Cable de par trenzado
802.3ae	10GBase-SR 10GBase-SW 10GBase-LR 10GBase-LW 10GBase-ER 10GBase-EW 10GBase-LX4	10 GB/s	Cable de fibra óptica
802.an	10GBase-T	10 GB/s	Cable de par trenzado

Tabla 1.5: Estándares de Ethernet

Los elementos físicos de una red Ethernet, como los cables de red y las tarjetas de interfaz de red, son los componentes fundamentales que posibilitan el flujo de datos codificados de un nodo de la red a otro. En cuanto al cableado, existen cuatro tipos principales utilizados en las redes Ethernet: coaxial delgado, coaxial grueso, UTP (par trenzado sin blindaje) de categoría 5 y fibra óptica. La Tabla 1.5 resume las especificaciones para cada tipo de medio de transmisión, incluyendo la longitud máxima admitida para un segmento particular de ese medio. Además, la topología física de la red está estrechamente relacionada con el tipo de medio de transmisión empleado.

1.7. AS-interface

AS-i es una abreviatura de Actuator Sensor Interface o Interfaz de Sensores y Actuadores. El bus AS-Interface es un sistema de interconexión electromagnética de bajo costo que simplifica la conexión entre sensores, actuadores y sistemas integrados utilizando un cable de dos conductores estándar. Su propósito principal no es funcionar como un bus de campo universal para todas las aplicaciones de automatización, sino, en cambio, como un sistema económico adecuado para el nivel más básico de la jerarquía de la automatización.

En este bus, la señal es robusta, equilibrada y cuenta con redundancia de paridad, lo que hace que el cableado sea simple. Un segmento de señal se puede distribuir de

diversas maneras, ya sea en configuración de estrella, árbol o bus, sin restricciones en la cantidad de dispositivos conectados. El único requisito es que la longitud total del cableado en un segmento de señal no exceda los 100 metros. Además, no se requieren resistencias terminales en la red. AS-interface no tiene la gloria de Ethernet ni la sofisticación de DeviceNet ni la velocidad de ProfibusDP, pero hace el trabajo para muchas aplicaciones y por menos dinero. Puede que no sea la red industrial principal de todas las plantas, pero debería considerarse como una primera alternativa.

El bus AS-Interface está específicamente diseñado para conectar dispositivos de E/S (Entrada/Salida) de campo simples, como actuadores, sensores, codificadores rotatorios, entradas y salidas analógicas, pulsadores y sensores de posición de válvulas, en aplicaciones de procesos y fabricación discreta. Este sistema utiliza dos únicos cables conductores para lograr estas conexiones de manera eficiente y económica. El sistema AS-I es configurado y controlado por un maestro, el cual programa a la interfaz entre un controlador y el sistema AS-I. Este intercambia información continuamente con todos los sensores y actuadores conectados al bus AS-I de forma predeterminada y cíclica.

1.7.1. Características principales

- **Compatibilidad:** Sensores y Actuadores de diferentes fabricantes pueden ser conectados a una interfaz digital serial estandarizada;
- **Control de acceso al medio:** Sistema con solo un maestro y sondeo cíclico;
- **Direccionamiento:** Esclavos reciben un direccionamiento permanente del maestro o a través de hand-held.
- **Topología:** Sin restricciones (lineal, anillo, estrella o árbol).
- **Medio de transferencia:** Dos cables no-trenzados y sin blindaje para datos y energía (24 VDC), típicamente hasta 200 mA por esclavo, y hasta 8A por bus.
- **Longitud del cable:** Máximo de 100 m o hasta 300 m con el uso de repetidores.
- **Número de esclavos:** Hasta 62 esclavos por red (versión 2.1).
- **Telegramas:** Telegrama del maestro contenido el direccionamiento, respuesta directa del esclavo.
- **Datos:** 4 entradas y 4 salidas para cada esclavo y en el caso de más de 31 esclavos tiene, solo 3 salidas; (máximo de 248 entradas y salidas binarias por red).
- **Carga útil:** Transmite 4 bits/esclavo/mensaje. Todos los esclavos son llamados secuencialmente por el maestro y reciben 4 bits de datos. Cada esclavo responde inmediatamente con 4 bits de datos.
- **Tiempo de ciclo:** 10 ms para la versión 2.1.

- **Detección de error:** Detección eficiente y retransmisión de telegramas incorrectos.
- **Chip AS-Interface:** 4 E/S configurables para datos, 4 parámetros de salidas y 2 salidas de control.
- **Confiabilidad:** Alto nivel de contabilidad operacional en ambientes industriales agresivos.
- **Estándar abierto:** Elaborado por diversos fabricantes, afiliados a la Asociación Internacional AS-I, cuyo protocolo de transmisión es normalizado.

Componentes de AS-Interface

Maestro AS-i	En la parte superior de la red se encuentra el AS-i Master, que desempeña un papel central. El AS-Interface Master establece la conexión con el sistema de control de nivel superior y se encarga de la gestión de todo el tráfico de datos en la línea. Además, asume responsabilidades importantes como la parametrización, el diagnóstico y la supervisión de los dispositivos conectados a la red AS-i.
Cable AS-i	Hay dos cables necesarios en un sistema de AS-Interface: - Un cable para llevar la energía y los datos a los sensores que suele ser de color amarillo. - Un cable para llevar 24 voltios a los actuadores que suele ser de color negro.
Fuente de alimentación	Proporciona una corriente continua constante y regulada de 30 V para suministrar energía a los dispositivos maestro y esclavo. También funciona como desacoplador de datos.
AS-i de Seguridad	Todos los dispositivos de seguridad conocidos pueden conectarse directamente al segmento AS-i mediante módulos o como solución integral

Tabla 1.6: Componentes de AS-i.

Interfaces

Interfaz 1	Sensores y actuadores	En este nivel se encuentran los esclavos que utilizan chips AS-i.Estos chips habilitan a los esclavos para conectarse a la red AS-i, transmitir datos al maestro y recibir instrucciones de vuelta.
Interfaz 2	Sistema de transmisión	En este nivel, se facilita el intercambio de datos entre los esclavos de la red. La Interfaz 2 establece cómo se accede a la Interfaz 1, gestionando la transferencia de datos eléctricos, abordando problemas de comunicación y controlando el tiempo de cada transacción en la red.

Interfaz 3	Elemento de control (maestro)	Establece la conexión entre el controlador (host) y los sensores y actuadores en la red. Actúa como intermediario en la comunicación entre estos dispositivos y el controlador, el maestro puede gestionar el tráfico de datos de manera autónoma. También es capaz de realizar la configuración inicial de los dispositivos y llevar a cabo diagnósticos para garantizar un funcionamiento óptimo de la red.

Tabla 1.7: Interfaces de AS-i.

1.7.2. Trama AS-i

- AS-i es una red maestro/esclavo que funciona mediante polling cíclico, es decir, hay un único maestro que direcciona uno a uno a los esclavos y realiza la comunicación con ellos.
- La red es de difusión, por lo que en cada trama se ha de indicar la dirección del esclavo con el que se establecerá la comunicación.
- Los esclavos de AS-Interface deben tener asignada una dirección:
  - De fábrica la dirección 0.
  - Se asigna mediante un terminal de direccionamiento o a través del maestro de la red.
  - Ha de ser única, y debe estar comprendida entre 1 y 31(A/B).
  - Dirección en una memoria no volátil (EEPROM).
  - Cada esclavo tiene 1 byte de datos, de forma que pueden conectarse 4 dispositivos de entrada binarios y 4 de salida por esclavo.[A/B 4I/3O]
  - Si un esclavo se conecta directamente a la red, ocupará la dirección completa.

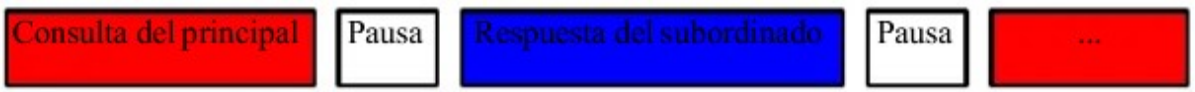
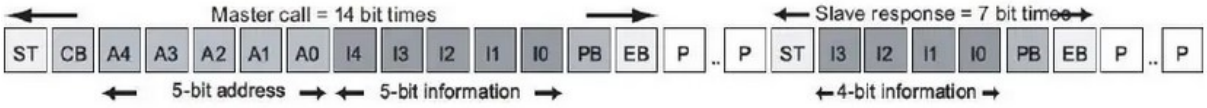


Figura 1.21: Estructura general de un intercambio de mensajes en AS-i



An AS-Interface message comprises the following elements:

- Master call: each master call comprises exactly **14** bit times
- Master interval: at least 2 bit times, max. 10 bit times
- Slave response: each slave response comprises exactly 7 bit times
- Slave interval:
  - under normal circumstances with synchronized slave: 1.5 to 2 bit times
  - During startup with non-synchronized slave: 4 bit times

Figura 1.22: Estructura de mensajes en AS-i

1.7.3. Capa Física

Puede emplearse cualquier cable bifilar de $2 \times 1{,}5\ mm^2$ sin apantallamiento ni trenzado, sin embargo, se recomienda utilizar el Cable Amarillo (de fábrica del dispositivo).

- Conectable por perforación de asilamiento.
- Codificación mecánica para evitar los cambios de polaridad, es decir, el perfil del cable es asimétrico, lo que impide que sea conectado de forma inadecuada a los restantes dispositivos de la red.
- Grado de protección IP65/67.
- Autocicatrizante, lo que permite la desconexión segura de los esclavos manteniendo el grado de protección IP65/67.
- Existen módulo sin electrónica integrada que adaptan el cable AS-i a otros normalizados, como el cable redondo con conector M12.

1.8. BACnet

BACnet (Building Automation and Control Networks) es un protocolo de comunicación de datos creado con el propósito de simplificar la interacción entre los diversos dispositivos electrónicos que se encuentran en edificios modernos. Estos dispositivos pueden abarcar sistemas de alarma, sensores de movimiento, sistemas de climatización, calefacción y otros equipos relacionados con la automatización y el control de edificaciones.

El protocolo BACnet establece una serie de servicios que se emplean para posibilitar la comunicación entre dispositivos en un edificio. Estos servicios incluyen funciones como "Who-Is" (¿Quién es?), "I-am" (Soy yo), "Who-Has" (¿Quién tiene?) e "I-Have" (Tengo), que se utilizan para la detección de objetos y dispositivos. Además, otros servicios como "Read-Property" (Leer Propiedad) y "Write-Property" (Escribir Propiedad) se emplean para leer o escribir datos. BACnet posibilita el control centralizado de

todos los dispositivos en un edificio de gran envergadura desde una ubicación central.

1.8.1. Trama BACnet

La arquitectura de protocolo de BACnet consta de cuatro capas que corresponden a la capa física, de enlace de datos, de red y de aplicación del modelo ISO/OSI. Aunque BACnet especifica la capa de red y aplicación, no define una capa física y de enlace de datos en particular. En principio, cualquier combinación de capas físicas y/o de enlace de datos podría utilizarse para la comunicación de mensajes BACnet. Sin embargo, con el fin de mejorar la interoperabilidad entre dispositivos BACnet, se han definido cinco opciones de red diferentes, cada una con características de velocidad y rendimiento específicas. Estas cinco opciones de red son:

- Ethernet
- ARCNET
- Master-Slave/Token-Passing (MS/TP)
- Point-to-Point (PTP)
- LonTalk

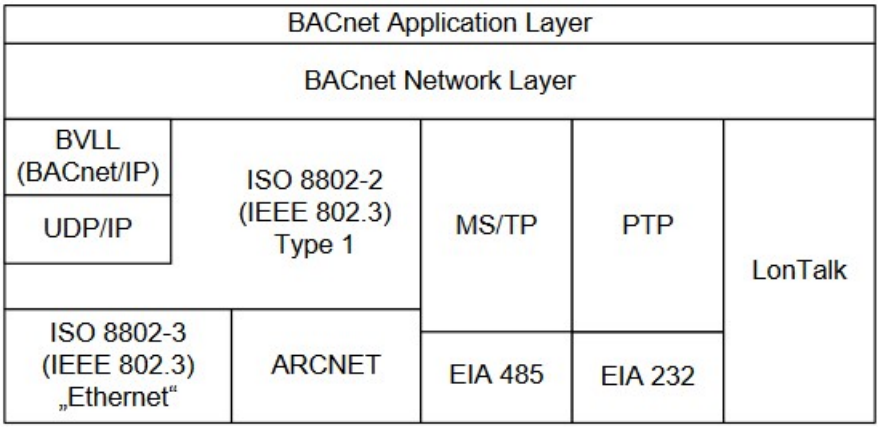


Figura 1.23: Stack BACnet.

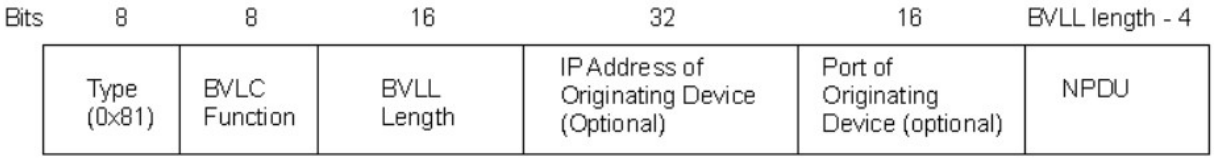


Figura 1.24: BACnet UDP/IP.

Control octet:

Bit 7:	1 ... Message is a network layer message 0 ... Message contains a BACnet APDU
Bit 6:	Reserved
Bit 5:	0 ... DNET, DLEN, DADR, hop count absent 1 ... DNET, DLEN, DADR, hop count present
Bit 4:	Reserved
Bit 3:	0 ... SNET, SLEN, SADR absent 1 ... SNET, SLEN, SADR present
Bit 2:	Corresponds to *data_expecting_reply* parameter
Bit 1,0:	11 ... Life safety message 10 ... Critical equipment message 01 ... Urgent message 00 ... Normal message

1	1	2	1	d	2	1	s	1	1	2	n
Version	Control	DNET	DLEN = d	DADR	SNET	SLEN = s	SADR	Hop Count	Message Typ	Vendor ID	APDU

Figura 1.25: BACnet NPDU.

Las opciones de red convencionales, BACnet/IP permite la utilización de comunicación BACnet a través de redes IP. Para establecer conexiones de túneles, se emplea un dispositivo específico denominado BACnet/Internet Protocol Packet-Assembler-Disassembler (B/IP PAD), el cual encapsula el mensaje BACnet en un paquete UDP. Este paquete se transmite al destino B/IP PAD, donde se desempaqueta de nuevo como un mensaje BACnet. Otra alternativa para aprovechar las redes IP es utilizar el protocolo UDP como la capa de enlace de datos nativa. Para habilitar esta funcionalidad, se ha definido la Capa de Enlace Virtual BACnet (BVLL). En el caso de comunicaciones de difusión que abarcan múltiples subredes IP, se necesita un dispositivo especial llamado BACnet Broadcast Management Device (BBMD).

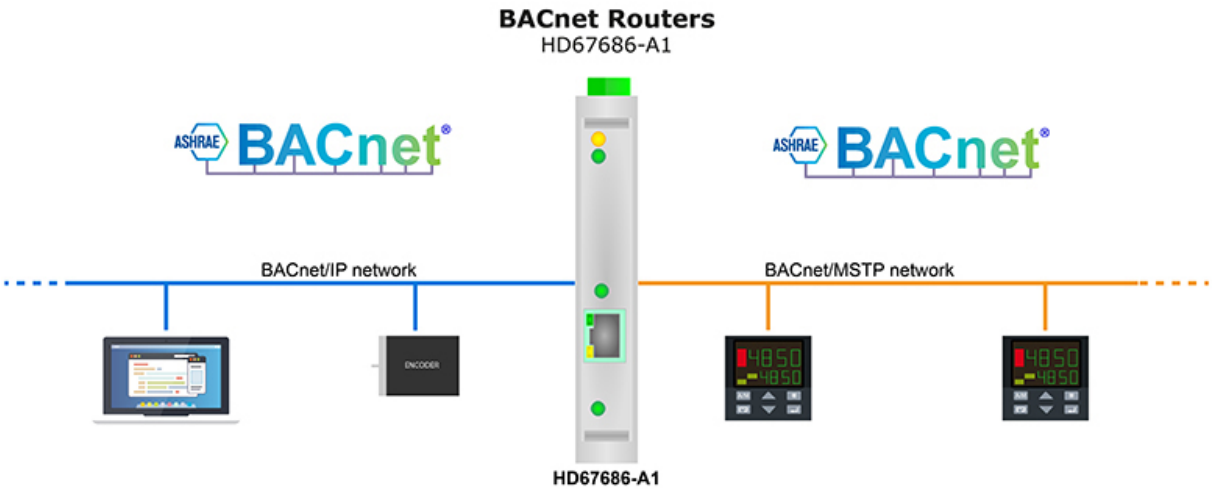


Figura 1.26: Ejemplo de red industrial con el protocolo BACnet

1.9. SMS

Un dispositivo cliente GSM cuenta con la capacidad de realizar una variedad de actividades relacionadas con la transmisión de datos. Estas actividades abarcan el envío y recepción de mensajes de correo electrónico, faxes, navegación por Internet y otras funciones de transmisión de datos digitales. Además, el cliente GSM puede aprovechar servicios como los mensajes cortos (SMS) o mensajes de texto para lograr una comunicación rápida y eficiente. En conjunto, estas capacidades amplían las opciones de comunicación y conectividad disponibles a través de la red móvil GSM.

1.9.1. Características principales

- **Mensajes de Texto Cortos**: El SMS permite el envío y recepción de mensajes de texto que suelen ser cortos, generalmente limitados a 160 caracteres por mensaje.
- **Comunicación Asíncrona:** significa que el remitente y el destinatario no necesitan estar conectados simultáneamente para enviar o recibir mensajes.
- **Ubicuidad:** SMS es ampliamente compatible y se encuentra en la mayoría de los teléfonos móviles y dispositivos móviles.
- **Entrega Confiable:** depende de la calidad de la red móvil y la configuración del servicio.
- **Compatibilidad Multiplataforma:** Los mensajes SMS pueden enviarse y recibirse entre diferentes dispositivos y sistemas operativos.
- **Limitación de Longitud:** Los mensajes SMS tienen una longitud limitada.
- **Amplias Aplicaciones:** El SMS se utiliza en una variedad de aplicaciones, incluyendo mensajería personal, notificaciones de servicios, marketing y autenticación de dos factores (2FA), telemetría médica, etc.

1.9.2. Trama SMS

Un mensaje SMS (Short Message Service) es una cadena alfanumérica que puede contener hasta 140 caracteres o 1602 caracteres de 7 bits. Este mensaje se encapsula con una serie de parámetros. En su forma básica, los SMS se utilizan para enviar y recibir mensajes de texto simples. Sin embargo, existen extensiones del protocolo que permiten incluir otros tipos de contenido, dar formato a los mensajes o encadenar varios mensajes de texto para permitir una longitud mayor.

SMS-DELIVER (Mobile Terminated)

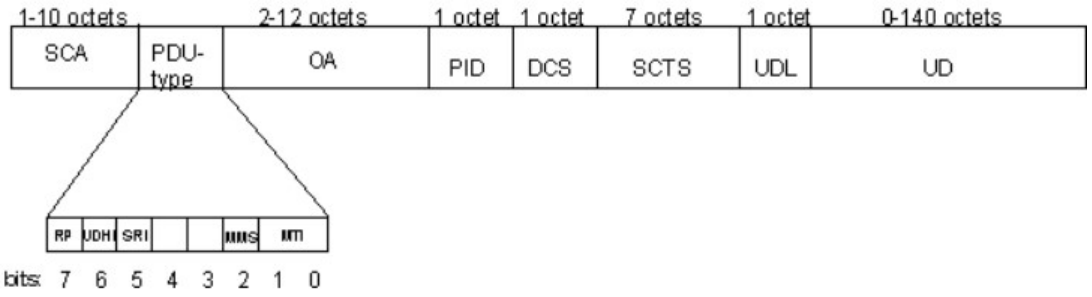


Figura 1.27: Frame SMS-DELIVER

SMS-SUBMIT (Mobile Originated)

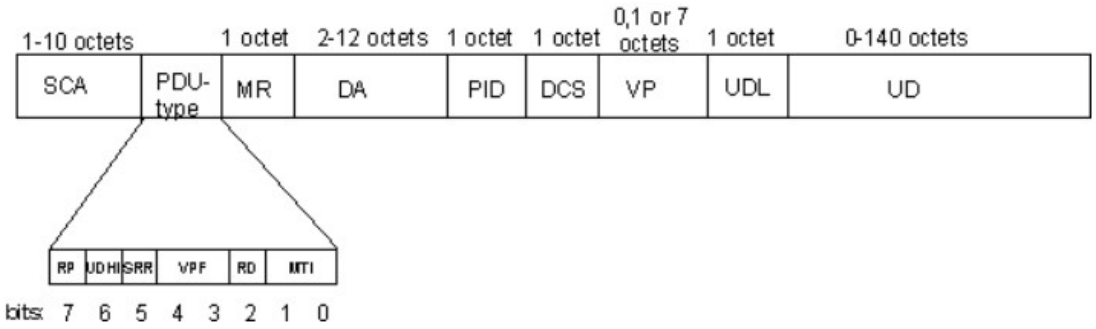


Figura 1.28: Frame SMS-SUBMIT

Mensaje		Descripción
SCA	Service Centre Address	Número de teléfono del Centro de Servicio
PDU Type	Protocol Data Unit Type	
MR	Message Reference	Número sucesivo (0..255) de todas las tramas de envío de SMS establecidas por el M20
OA	Originator Address	Dirección de la PYME de origen
DA	Destination Address	Dirección de la PYME de destino
PID	Protocol Identifier	Parámetro que muestra al SMSC cómo procesar el SM (como FAX, voz, etc.)
DCS	Data Coding Scheme	Parámetro que identifica el esquema de codificación dentro de los Datos de Usuario (UD)
SCTS	Service Centre Time Stamp	Parámetro que identifica la hora en que el SMSC recibió el mensaje
VP	Validity Period	Parámetro que identifica la hora a partir de la cual el mensaje deja de ser válido en el SMSC
UDL	User Data Length	Parámetro que indica la longitud del campo UD
UD	User Data	Datos del SM
RP	Reply Path	Parámetro que indica que existe ruta de respuesta
UDHI	User Data Header Indicator	Parámetro que indica que el campo UD contiene un encabezado
SRI	Status Report Indication	Parámetro que indica si la Pyme ha solicitado un informe de estado
SRR	Status Report Request	Parámetro que indica si el MS ha solicitado un informe de estado
VPF	Validity Period Format	Parámetro que indica si el campo VP está presente o no
MMS	More Messages to Send	Parámetro que indica si hay o no más mensajes para enviar
RD	Reject Duplicate	

MTI	Message Type Indicator	Parámetro que describe el tipo de mensaje 00 significa ENTREGAR SMS 01 significa ENVIAR SMS

Tabla 1.8: Tipo de mensajes SMS.

1.9.3. Aplicación en telemetría médica

En la actualidad, el término telemedicina se refiere al empleo de dispositivos biomédicos y tecnologías de telecomunicaciones avanzadas con el propósito de mejorar la atención al paciente y facilitar diagnósticos médicos. A medida que aumenta la demanda de transporte de pacientes a hospitales en el mundo actual, se destaca la importancia de la monitorización continua de los signos vitales o fisiológicos en situaciones de cuidados críticos. Estos signos comprenden la frecuencia cardíaca (FC), la saturación de oxígeno (SpO2), la temperatura corporal, entre otros. Gracias a los avances en las ciencias biomédicas, la informática y las tecnologías de telecomunicaciones, es factible diseñar sistemas capaces de detectar, monitorizar, mostrar y transmitir estas señales biomédicas desde pacientes ubicados en lugares remotos a profesionales de la salud mediante servicios GSM.

Estos sensores también pueden emplearse en el hogar u otras ubicaciones remotas para llevar a cabo el seguimiento de pacientes que no requieren cuidados críticos. Sin embargo, es importante destacar que, a pesar de que los sensores y las estaciones base posibilitan el monitoreo externo de un paciente, esto no implica que el paciente tenga total movilidad, ya que sigue estando conectado a la estación base y a la infraestructura de comunicaciones. No obstante, en ciertos escenarios, podría haber sido factible controlar a los pacientes de manera remota si se hubiera contado con los sensores adecuados y una infraestructura de comunicaciones que permitiera verificar de manera periódica su estado de salud.

Este enfoque ha demostrado ser beneficioso para los profesionales médicos, ya que les posibilita supervisar a pacientes que están en sus hogares o ingresados en el hospital de forma constante. Esto adquiere una importancia fundamental, dado que los pacientes a menudo necesitan decisiones médicas precisas y continuas para garantizar que reciban el tratamiento adecuado y se puedan salvar vidas.

1.10. DNP 3

DNP3 (acrónimo de Distributed Network Protocol, versión 3) es un protocolo industrial creado con la finalidad de mejorar las comunicaciones entre dispositivos inteligentes conocidos como IED (Intelligent Electronic Devices) y estaciones de control. Este protocolo tiene una amplia aplicación en sistemas SCADA (Supervisory Control and Data Acquisition) y cumple una función esencial en la supervisión y el control de procesos industriales, infraestructuras críticas y sistemas de automatización en diversos sectores industriales.

El protocolo DNP3 es versátil y admite varias configuraciones de red. Tres de las configuraciones más comunes son las siguientes:

- **Configuración Uno a Uno:** En esta configuración, un dispositivo maestro se conecta a un dispositivo externo a través de una conexión dedicada, como una línea telefónica de acceso telefónico. Esta configuración se utiliza cuando se necesita una comunicación directa y exclusiva entre un maestro y un dispositivo remoto.

- **Configuración Multipunto:** La configuración multipunto es muy popular y se utiliza cuando un dispositivo maestro necesita comunicarse con múltiples estaciones remotas. En esta configuración, el maestro envía solicitudes a todas las estaciones remotas, pero cada estación remota solo responde a los mensajes que están destinados específicamente a ella. Es eficiente para sistemas con múltiples dispositivos remotos que deben ser monitoreados y controlados centralmente.

- **Configuración Jerárquica:** En una configuración jerárquica, un dispositivo desempeña un papel dual: actúa como estación remota en un segmento de la red y como maestro en otro segmento. Este dispositivo de doble función se conoce como "submaestro". Esta configuración se utiliza cuando se necesita una estructura de red en la que ciertos dispositivos pueden actuar como maestros para una parte de la red y como estaciones remotas para otra parte, permitiendo así una jerarquía de control.

1.10.1. Características principales

La Comisión Electrotécnica Internacional (IEC) inicialmente propuso el estándar IEC 870 con el objetivo de facilitar la transmisión de datos de telemetría en sistemas SCADA que se basaban en el modelo de Interconexión de Sistemas Abiertos (OSI). Para mejorar el rendimiento, se desarrolló una arquitectura de tres capas conocida como arquitectura de rendimiento mejorado (EPA). Esta arquitectura eliminó capas innecesarias del modelo OSI de siete capas. Sin embargo, la EPA tenía una limitación: no permitía el envío de mensajes de la capa de aplicación que fueran más largos que la longitud máxima admitida en una trama de enlace de datos. DNP3 abordó este problema al incorporar una capa de pseudotransporte que permitía la fragmentación de mensajes, lo que se ilustra en la Figura 1.29. Esto permitió que DNP3 gestionara mensajes de aplicación más extensos y superara la limitación de longitud de trama de enlace de datos que existía en la EPA.

A continuación, se listan algunas de las principales características que tiene este protocolo de comunicación industrial:

- **Estándar Abierto:** su especificación es pública y está disponible para su uso por parte de diversos fabricantes y organizaciones.

- **Comunicación Maestro-Esclavo:** un dispositivo maestro (como un sistema de control) solicita datos a dispositivos esclavos (como sensores y dispositivos de campo).
- **Comunicación en Tiempo Real:** DNP3 admite la comunicación en tiempo real y la transmisión de datos en función de eventos.
- **Redundancia:** implementa redundancia para garantizar la disponibilidad y la integridad de la comunicación en sistemas críticos.
- **Integración de Datos:** integra datos analógicos y digitales en una red.
- **Capacidades de Diagnóstico:** permite a los usuarios supervisar el estado de los dispositivos y realizar un seguimiento de problemas y eventos.
- **Seguridad:** implementa autenticación, cifrado y firmas digitales, para proteger la comunicación y los datos transmitidos.
- **Compatibilidad con Protocolos Serie y Ethernet:** DNP3 puede funcionar en redes serie (por ejemplo, RS-232/RS-485) o en redes Ethernet, lo que lo hace versátil en términos de infraestructura de red.
- **Amplio Uso en Energía:** es ampliamente utilizado en la supervisión y el control de sistemas eléctricos, subestaciones, medidores y sistemas de generación de energía.

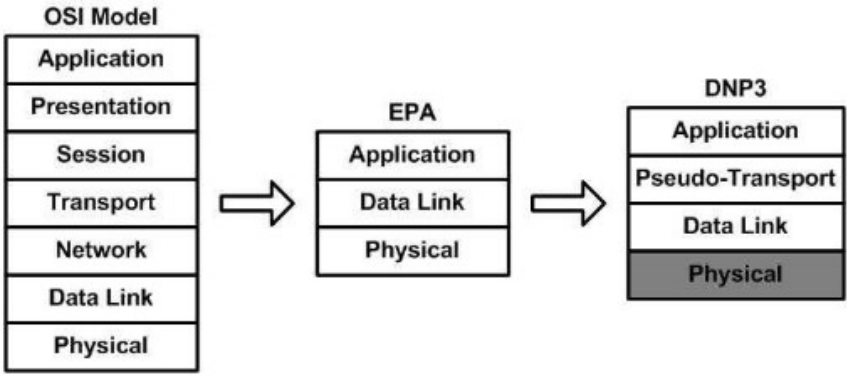


Figura 1.29: Stack DNP3.

1.10.2. Trama DNP3

Una trama de capa de enlace de datos consta de los siguientes elementos:

- Encabezado de tamaño fijo de 10 bytes.
- Sección de datos o çarga útilçon una longitud máxima de 250 bytes (que incluye campos CRC de 16 bits por cada 16 bytes de datos), lo que da como resultado una longitud máxima de trama de enlace de datos de 292 bytes.
- El campo Inicio siempre contiene los valores de dos bytes 0x0564, lo que permite al receptor identificar el inicio de la trama.

- El campo Longitud indica el número de bytes en el resto de la trama (excluyendo los CRC).
- El campo Control de enlace contiene datos para gestionar el flujo de mensajes, secuenciarlos y definir la función de la trama. Incluye un código de función de cuatro bits que especifica el propósito del mensaje y dos indicadores para sincronización y control de flujo.
- La dirección de destino de 16 bits en el encabezado del enlace de datos identifica al destinatario, mientras que la dirección de origen de 16 bits indica al emisor.
- Un CRC de 16 bits se incluye en el encabezado para verificar la integridad de la transmisión.

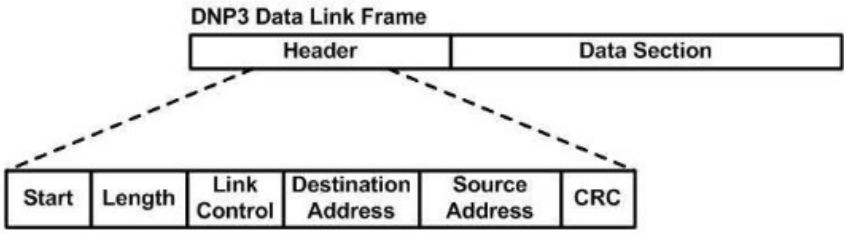


Figura 1.30: Trama DNP3

DNP3 se destaca por su flexibilidad y un conjunto de funcionalidades que van más allá de los protocolos de comunicación convencionales. Algunas de sus características notables incluyen opciones de salida, la capacidad de realizar transferencias seguras de archivos, la habilidad para direccionar y gestionar más de 65.000 dispositivos en un solo enlace de comunicación, sincronización precisa de tiempos y eventos de marca de tiempo, confirmación de la integridad de los datos transmitidos y otras capacidades avanzadas. Estas características hacen que DNP3 sea una elección sólida para sistemas de control y supervisión que requieren un alto grado de flexibilidad y confiabilidad en entornos industriales y de automatización.

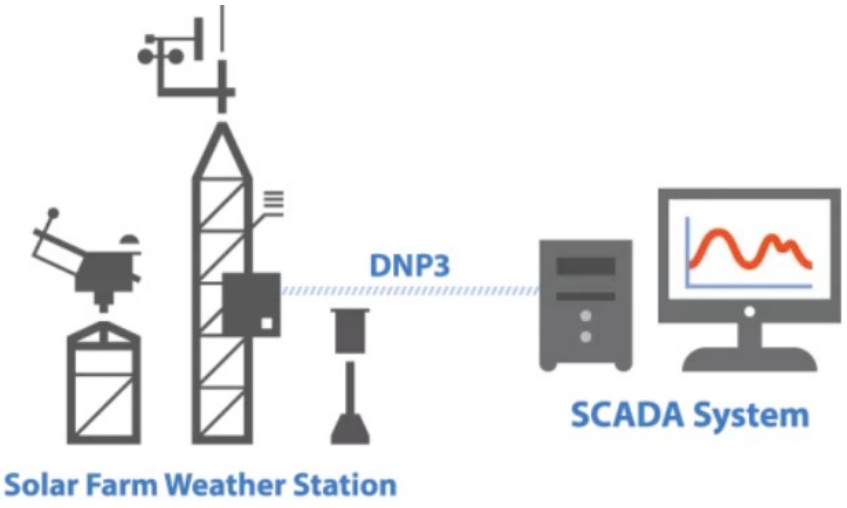


Figura 1.31: Ejemplo de red industrial con el protocolo DNP3.

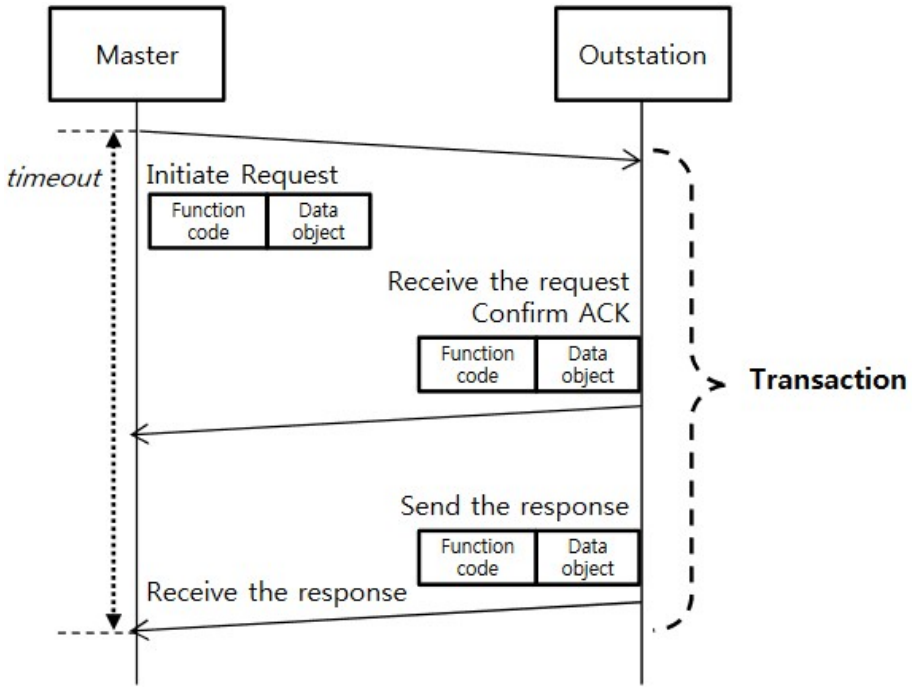


Figura 1.32: Intercambio de mensajes en DNP3.

1.10.3. Capa Física

La especificación de la capa física determina la configuración eléctrica, el voltaje y la sincronización, junto con otras propiedades necesarias para enviar señales entre dispositivos. La capa física proporciona cinco servicios: (i) enviar datos, (ii) recibir datos, (iii) conectar, (iv) desconectar y (v) actualizar el estado. La capa física no está especificada en el estándar DNP3. DNP3 puede transportarse a través de una variedad de medios físicos, incluidos enlaces en serie antiguos.

1.11. IEC 61850

En su nivel más fundamental, DNP3 se orienta hacia el transporte seguro y eficiente de datos simples para la comunicación a distancia. Por otro lado, IEC 61850 se centra principalmente en la comunicación entre activos, como la protección de equipos, dispositivos electrónicos inteligentes (IED) o sistemas HMI/SCADA locales dentro de las instalaciones a nivel local. Una diferencia clave entre DNP3 y IEC 61850 es que la norma IEC se enfoca en el contexto de los datos. Mientras DNP3 se enfoca en los datos en sí y deja gran parte de la contextualización en manos de los ingenieros, IEC 61850 integra el contexto en el sistema asignando datos a nodos lógicos con nombres contextuales predefinidos. Esto asegura que el contexto nunca se pierda durante la recopilación de datos, lo que simplifica la interpretación y el uso de la información en el entorno de la automatización.

1.11.1. Características principales

IEC 61850 destaca por su extenso conjunto de capacidades de modelado de datos, respaldado por información de autodescripción y un sistema independiente de proveedores que promueve la interoperabilidad. Los protocolos de comunicación en IEC 61850 abarcan modelos cliente-servidor y de publicación-suscripción. Algunos de los protocolos de comunicación admitidos incluyen el Evento de Estado de Subestación Genérico, MMS basado en un modelo cliente-servidor, SV (para transferencia de valores muestreados) y GOOSE (para eventos de subestación). SV y GOOSE se utilizan para transmitir datos en tiempo crítico mediante comunicación asincrónica y multicast, lo que permite a los editores enviar una única copia de los datos a la red para su distribución eficiente a múltiples suscriptores. Esto mejora el rendimiento y reduce la latencia y el tráfico en la red.

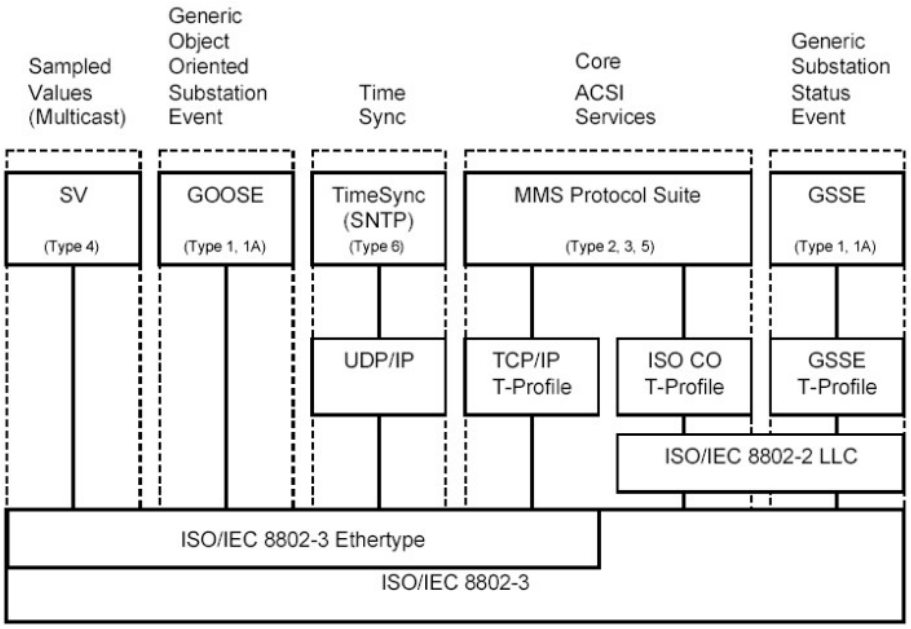


Figura 1.33: Descripción general de la funcionalidad IEC 61850 y perfiles de comunicación asociados

1.11.2. Trama IEC 61850

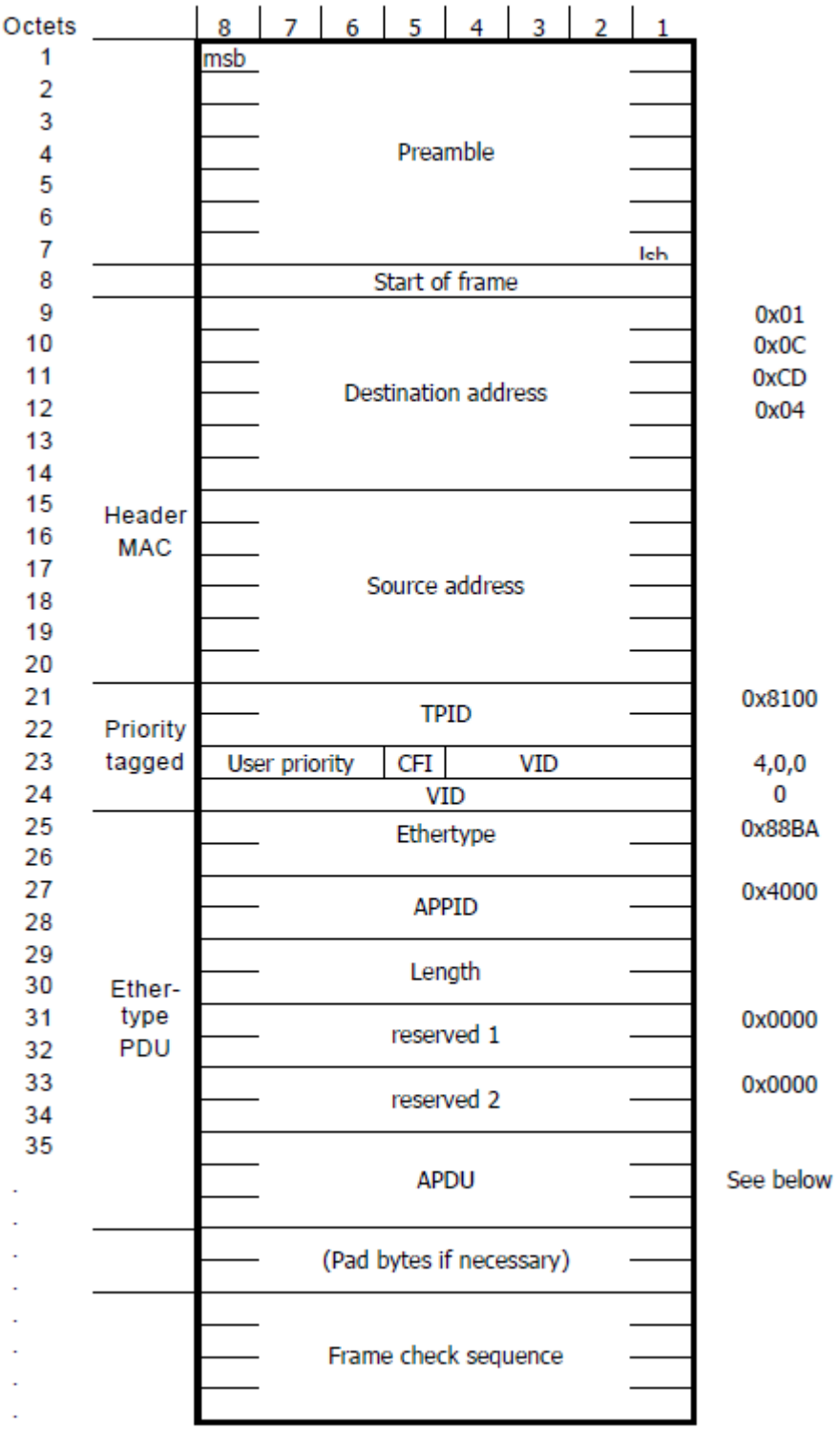


Figura 1.34: Trama IEC

1.12. Comparación general de los protocolos de comunicación industrial

Protocolo	Tipo de Comunicación	Velocidad de Comunicación	Topología de Red	Aplicaciones Principales
Modbus	Serie	9600 bps a 115200 bps	RS-485, TCP/IP	Automatización industrial, PLC, Control de Procesos
HART	Serie	Variable (1200 baudios)	Varios	Instrumentación de campo, medición y control
Profibus	Serie	Hasta 12 Mbps	RS-485	Automatización industrial, sensores y actuadores
ProfiNet	Ethernet	Hasta 1000 Mbps	Ethernet	Automatización industrial, tiempo real
DeviceNet	Serie	Hasta 500 kbps	CAN	Automatización industrial, dispositivos de campo
Red de Control	Variable	Variable	Variable	Control de procesos y sistemas de automatización
Ethernet/IP	Ethernet	Hasta 1 Gbps	Ethernet	Automatización industrial, integración de sistemas
Interfaz Actuador-Sensor (AS-i)	Serie	Hasta 167 kbps	Serie	Automatización industrial, sensores y actuadores
BACNet	Serie/Ethernet	Variable	Variable	Automatización de edificios, sistemas HVAC
SMS para elemetría Médica	SMS	Variable	Variable	Telemetría médica y salud
DNP 3	Serie/Ethernet	Variable	Variable	Sistemas de control y automatización eléctrica
IEC 61850	Ethernet	Variable	Ethernet	Sistemas eléctricos, subestaciones eléctricas

Tabla 1.9: Comparación general de los protocolos de comunicación industrial.

1.13. I2C

El protocolo I2C proporciona una comunicación sencilla sin pérdida de datos. I2C utiliza solo dos cables para la comunicación. es ligero, económico y omnipresente. También aumenta la tasa de transferencia de datos. El objetivo al desarrollar el protocolo es lograr una comunicación de alta velocidad y controlar los registros dentro de los dispositivos, así como los datos que se pueden guardar en los registros, a través de esto podemos controlar varios parámetros. I2C se utiliza en la vigilancia de datos para mayor precisión y eficiencia. El método de diseño está desarrollado en VHDL, simulado en MODELSIM o Xilinx y puede implementarse en placa FPGA.

Hay muchas razones para utilizar el diseño de interfaz en serie y muchas aplicaciones más importantes incluyen la comunicación en serie, como la comunicación de sensores con una computadora personal. Muchos periféricos comunes de sistemas integrados, como convertidores analógicos a digitales y digitales a analógicos, pantallas LCD y sensores de temperatura, admiten interfaces en serie. La interfaz serie permite que los procesadores se comuniquen sin la necesidad de memoria compartida y los problemas que pueden crear. Existen protocolos de comunicación en serie como UART, CAN, USB, SPI, Inter IC. USB, SPI y UARTS son todos de un solo tipo de protocolo de tipo punto. USB utiliza multiplexor para comunicarse con otros dispositivos. Sólo los protocolos I2C y CAN utilizan direccionamiento por software. Pero sólo I2C es muy sencillo de diseñar y fácil de mantener.

	UART	CAN	USB	SPI	I2C
PROS	Bien conocida, Simple	Seguro, rápido	Seguro, rápido, plug and play	Rápido, bajo costo, universal	Simple, plug and play, rentable, universal
CONTRAS	Funcionalidad limitada, punto a punto	Complejo, orientado a la automoción	Se requiere un maestro potente, no plug and play, controladores adicionales	No plug and play, estándar no fijado	Limitado número de componentes

Tabla 1.10: Comparaciones de diferentes protocolos de comunicación serial.

1.13.1. Características principales

El tamaño físico y los requisitos de energía de los circuitos integrados se reducen con el paso de los años. La razón principal de esto es que se puede integrar una mayor cantidad de transistores en tamaños más pequeños y es posible una menor cantidad de cables de interconexión presentes entre los circuitos integrados. El circuito real del IC es mucho más pequeño que el empaque del IC, pero requiere un área más grande para cubrirlo debido al cable de interconexión presente entre los IC.

Estos requisitos de cables se pueden reducir utilizando I2C, es decir, un bus de circuito interintegrado. Esta comunicación tiene asignado un protocolo especial que

es el protocolo I2C. El bus I2C consta físicamente de dos cables activos y una conexión a tierra. Los dos cables activos son Serial Clock[SCL] y Serial Data[SDA]. Estos cables son de naturaleza semidúplex bidireccional y transportan información entre los dispositivos conectados al bus. Cada dispositivo se reconoce mediante una dirección única, ya sea un microcontrolador, un controlador LCD, una memoria o una interfaz de teclado, y puede funcionar como transmisor o receptor, según la función del dispositivo. En el bus I2C, los dispositivos se pueden agregar o quitar fácilmente, lo cual es muy útil para aplicaciones de control y bajo mantenimiento en sistemas integrados.

Componentes de I2C

- La parte superior maestra I2C se compone de registro de preescala, registro de comando, registro de estado, registro de transmisión y registro de recepción. El registro de preescala se utiliza para reducir la señal eléctrica de alta frecuencia a una frecuencia más baja mediante división de números enteros. Los datos llegan inicialmente al registro de estado y, dependiendo de ello, el registro de comandos emite los comandos. El registro de transmisión y recepción decide si transmitir o recibir los datos y estos datos se transmiten en paralelo al registro de E/S de datos.
- El controlador de bytes maestro I^2C es el controlador de comando de bytes y el registro de desplazamiento de E/S de datos. El controlador de comando de bytes es el corazón del tráfico de comunicación I^2C a nivel de bytes y es una máquina de estado que genera diferentes estados de operaciones de bytes I^2C en función de los bits del registro de comando. El registro de desplazamiento de E/S de datos es un componente que contiene y trata los datos asociados con las transacciones de escritura y lectura I^2C actuales.
- El controlador de bits I^2C Master implica un generador de reloj y un controlador de comando de bits. Durante la transmisión, los datos se transfieren bit a bit al controlador de bits de comando y desde allí se transfieren al SDA. Durante la recepción, los datos llegan al SDA y luego al controlador de bits.

Funcionamiento

1. **Condiciones de inicio y detención:**
   Antes de cualquier transacción, se debe emitir una condición de INICIO en el bus. La condición de inicio actúa como una señal para todos los circuitos integrados conectados de que algo está a punto de transmitirse. Una vez completado un mensaje, se envía una condición de DETENER. Esta es la señal para todos los dispositivos del bus de que el bus vuelve a estar disponible (inactivo). Si se accedió a un chip y recibió datos durante la última transacción, ahora procesará esta información (si aún no se procesó durante la recepción del mensaje).

2. **Transmitir un byte a un dispositivo esclavo:**
   Una vez enviada la condición de inicio, el maestro puede transmitir un byte a

un esclavo. Este primer byte después de una condición de inicio identificará el esclavo en el bus (dirección) y seleccionará el modo de operación. El significado de todos los bytes siguientes depende del esclavo.

Figura 1.35: Transmisión de un byte a un dispositivo esclavo.

3. **Recibir un byte de un dispositivo esclavo:**
Una vez que el esclavo ha sido direccionado y el esclavo ha reconocido esto, se puede recibir un byte del esclavo si el bit R/W en la dirección se configuró en READ (establecido en '1').

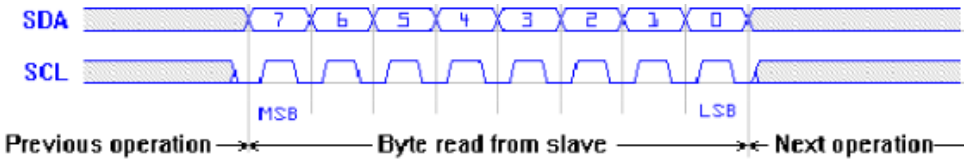


Figura 1.36: Transmisión de un byte a un dispositivo esclavo.

4. **Obtener reconocimiento (ACK) de un dispositivo esclavo:**
Cuando se ha transmitido una dirección o un byte de datos al bus, los esclavos deben confirmarlo. En el caso de una dirección, si la dirección coincide con la suya, entonces ese esclavo y solo ese esclavo responderá a la dirección con un ACK. En caso de que un byte se transmita a un esclavo ya direccionado, el esclavo también responderá con un ACK.

5. **Dar reconocimiento (ACK) desde un dispositivo esclavo:**
Al recibir un byte de un esclavo, el maestro debe acusarlo al dispositivo esclavo. Si no quedan datos para recibir, el maestro enviará una señal de no reconocimiento (NACK) y detendrá la transacción de datos.

Características generales DE I2C:

- Es un bus de computadora con terminal serie multimaestro.
- I2C tiene un bus serie bidireccional de dos cables
- Es un método simple y eficiente de intercambio de datos.
- El protocolo I2C tiene un ancho de banda bajo.
- Es un protocolo de distancia corta.

Vnetajas DE I2C:

- Se utiliza para aplicaciones sensibles a la seguridad, como conexiones de sensores, RFID, dispositivos biométricos, etc.
- Estándares de comunicación comunes entre microcontroladores y sensores.
- Cada dispositivo se reconoce por su dirección única y puede funcionar como transmisor o receptor, dependiendo de la función del dispositivo.
- Proporciona un sistema de seguridad mejorado

1.14. Redes de malla inalámbricas (WSM)

Las redes de malla inalámbricas (WMN - Wireless Mesh Networks) son redes de comunicación que comprenden nodos de radio, en los que los nodos están dispuestos en una topología de malla. La topología de malla es una interconexión de todos los nodos conectados con todos los demás nodos de la red. La red incluye dispositivos como nodos, clientes, enrutadores, puertas de enlace, etc. Como los nodos están completamente conectados, las redes de malla suelen ser menos móviles, ya que el redireccionamiento es menos difícil de predecir y provoca un retraso en la transmisión de datos. Los clientes Mesh pueden ser cualquier dispositivo inalámbrico como teléfonos celulares, computadoras portátiles, etc. Las puertas de enlace que actúan como nodos de reenvío no pueden estar conectadas a Internet. Como diferentes dispositivos se encuentran bajo una única red, también se la conoce como nube en malla. WMN es autocurable. Funciona mejor con varias redes diferentes que incluyen redes celulares y también IEEE 802.11, 802.15 y 802.16. WMN es flexible para trabajar con más de un protocolo.

1.14.1. Características principales

La red de malla inalámbrica basada en infraestructura es una red descentralizada sin una gestión centralizada o sin un servidor centralizado, lo que es más caro. Estos métodos son más confiables y eficientes ya que cada nodo tiene que transmitir al siguiente nodo. Aquí, los nodos actúan como enrutadores para transmitir los datos a sus pares que se encuentran lejos incluso en un solo salto. La red inalámbrica en malla debe ser estable, es decir, no debe haber mucha movilidad. Si se produce una falla del nodo debido a algún problema de hardware o cualquier otro, el nodo vecino realizará el redireccionamiento con la ayuda de protocolos de enrutamiento.

La red de malla puede estar compuesta por dispositivos móviles o dispositivos estacionarios. Algunas de las aplicaciones de las redes malladas que ameritan comunicación son:

- Vigilancia del campo de batalla
- Túneles
- Aplicaciones de vídeo móviles

- Situaciones de emergencia
- Carreras de coches en tiempo real, etc.
- Industria de agricutura de precisión

Arquitectura Wireless Mesh:

La red de malla inalámbrica es la arquitectura que proporciona menos movilidad con bajo costo dentro de un rango de radio. WMN es una infraestructura que es una red de enrutadores menos cableado entre los nodos. Consta de nodos de radio que no necesitan estar conectados a un puerto cableado como los puntos de acceso inalámbricos convencionales. Se predice que los saltos más cortos transmitirán los datos a grandes distancias. Los nodos entre el origen y el destino actúan como un nodo de reenvío que trabaja de manera cooperativa para tomar decisiones en la predicción de rutas basadas en la topología y el reenvío de datos. La red de malla inalámbrica proporciona estabilidad en comparación con el resto de topologías de red en lugar de agregar o eliminar nodos en la red. En la red de infraestructura en malla, el envío y la recepción de datos se realizan a través de una puerta de enlace, mientras que en el resto de la red se realiza a través de un par de nodos.

Las redes de malla inalámbrica se clasifican en tres tipos según la funcionalidad de los nodos de la red:

- **Arquitectura de malla de infraestructura:** Los enrutadores de malla actúan juntos como una columna vertebral inalámbrica para la arquitectura de malla de infraestructura. El nodo cliente es pasivo en la infraestructura de malla a través de enlaces Ethernet; Los clientes convencionales con interfaces Ethernet se pueden conectar a enrutadores de malla.

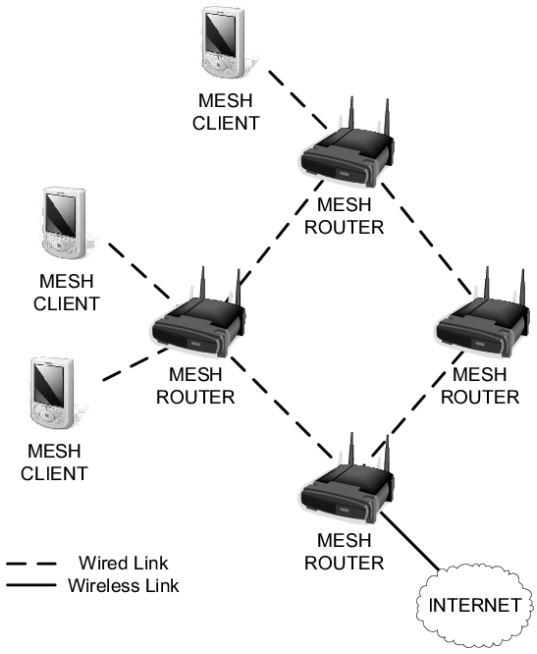


Figura 1.37: Arquitectura de malla de infraestructura.

- **Arquitectura mallada basada en clientes:** La arquitectura de malla basada en el cliente es aquella en la que los nodos del cliente están conectados de igual a igual. Cada nodo puede actuar como un nodo de enrutamiento para transferir los datos. Aquí, el cliente desempeña el papel de enrutamiento de malla actuando en el reenvío de los paquetes de datos.

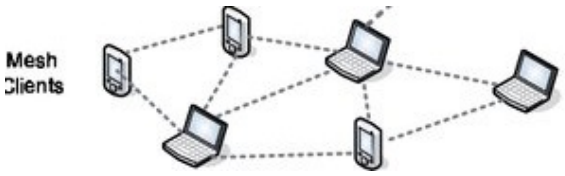


Figura 1.38: Arquitectura mallada basada en clientes.

- **Arquitectura de malla híbrida:** En la arquitectura de malla híbrida, normalmente los nodos de malla/enrutador actúan como la columna vertebral de toda la operación de la red. Con la ayuda del enrutador de malla de red, realiza el enrutamiento y reenvío de paquetes de datos hacia su destino.

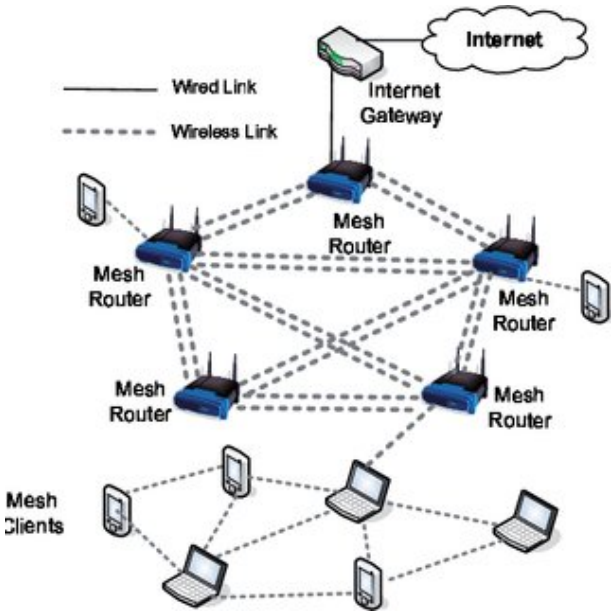


Figura 1.39: Arquitectura de malla híbrida.

1.15. MQTT

MQTT es un protocolo de comunicación estandarizado por OASIS, diseñado para aplicaciones en Internet de las cosas (IoT). Su enfoque principal es proporcionar una manera altamente eficiente de intercambiar mensajes a través de un sistema de publicación y suscripción, lo que lo hace especialmente adecuado para conectar dispositivos remotos. MQTT se distingue por su ligereza en términos de recursos, lo que lo convierte en una elección ideal para aplicaciones que requieren un código compacto y un consumo mínimo de ancho de banda de red. En la actualidad, MQTT se ha convertido en una tecnología ampliamente adoptada en diversas industrias, que van

desde la automotriz y la manufactura hasta las de telecomunicaciones y petróleo y gas, entre otras.

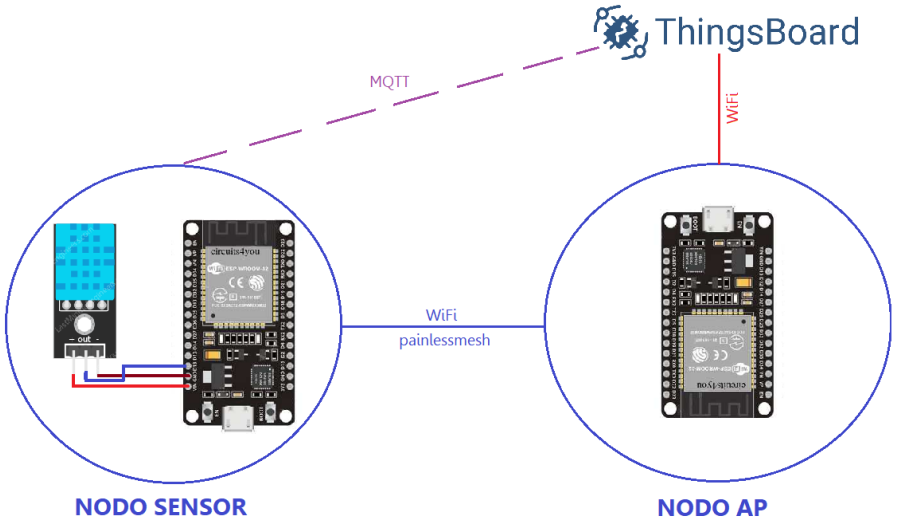


Figura 1.40: Ejemplo de red usando comunicación MQTT.

1.15.1. Características principales

Conceptos básicos de MQTT:

Publish/subscribe	En el protocolo MQTT, el editor publica mensajes y los usuarios se suscriben a temas que comúnmente se consideran un modelo de Publicación/Suscripción. El suscriptor se suscribe a temas particulares que se relacionan con él y al recibir todos los mensajes que se publican sobre esos temas. Por otro lado, los clientes pueden publicar mensajes por temas, de tal manera que permitan a todos los suscriptores acceder a los mensajes de esos temas.
Tópicos y subscripciones	En MQTT, el editor publica mensajes sobre temas que pueden considerarse como asunto del mensaje. El suscriptor, por lo tanto, se suscribe a temas para recibir mensajes específicos. Las suscripciones de temas pueden ser expresas, lo que restringe los datos que se recopilan al tema en particular.
Niveles de calidad de servicio	Este protocolo describe los niveles de calidad de servicio (QoS) que son un acuerdo entre dos partes de un mensaje con respecto a la garantía de distribución de datos. Permite 3 niveles de QoS.
Mensajes retenidos	En MQTT, los mensajes se retienen en el broker después de distribuirlos a todos los clientes presentes. Cuando se obtiene otra membresía para el mismo tema, los mensajes retenidos de esos temas se transmiten al nuevo cliente.

Sesiones limpias y conexiones confiables	En el momento en que un suscriptor se asocia con el broker, la asociación de sesión limpia se considera permanente, si su valor es falso. En esta tarea, los mensajes consecutivos que salen con una asignación de QoS más alta se reservan para su entrega cuando se reanude la asociación. El uso de estas banderas es opcional.
Wills (voluntad)	Un cliente puede informar al corredor que contiene un wills (mensaje) que debe distribuirse a un tema o temas en particular en caso de una separación imprevista. Esta voluntad es especialmente valiosa en el sistema, como la configuración de seguridad o alarma, donde los administradores notifican instantáneamente justo cuando un sensor ha extinguido la conexión con el sistema.

Tabla 1.11: Conceptos básicos de MQTT.

Arquitectura MQTT:

Componente	Descripción	Acciones
Cliente	Puede ser un Publicador o Suscriptor y siempre establece la conexión de red con el Servidor (Broker).	- Publicar mensajes para los usuarios interesados. - Suscribirse en el asunto de interés para recibir - Darse de baja para extraer de los asuntos suscritos. - Desvincularse del Broker
Broker	Controla la distribución de la información y es el principal responsable de recibir todos los mensajes del editor, filtrarlos, decidir quién está interesado en ellos y luego enviar los mensajes a todos los clientes suscritos.	- Aceptar solicitudes de Clientes. - Recibe mensajes publicados por los usuarios. - Procesa diferentes solicitudes como suscripción y cancelación de suscripción de los usuarios. - Después de recibir mensajes del editor los envía a los usuarios interesados

Tabla 1.12: Arquitectura MQTT.

1.15.2. Trama MQTT

Estructura de un mensaje MQTT:

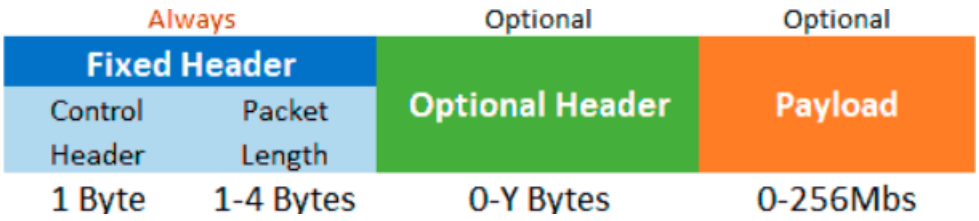


Figura 1.41: Estructura de un mensaje MQTT

- La cabecera fija es esencial y ocupa de 2 a 5 bytes, siendo obligatoria. Incluye un código de control para identificar el tipo de mensaje y la longitud del mensaje. La longitud se codifica en 1 a 4 bytes, utilizando los primeros 7 bits, y el último bit indica la continuidad.
- Por otro lado, la cabecera variable es opcional y proporciona información adicional necesaria en determinados mensajes o situaciones.
- El contenido (payload) constituye el contenido real del mensaje y puede alcanzar un máximo de 256 Mb, aunque en implementaciones prácticas, el límite suele situarse entre 2 y 4 kB.

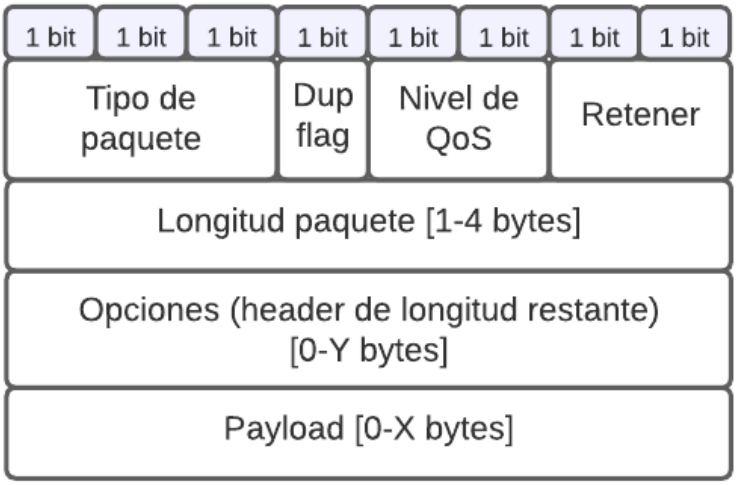


Figura 1.42: Trama MQTT.

El campo Tipo de mensaje tiene una longitud de 1 octeto y especifica el tipo de mensaje. Se establecerá en uno de los valores que se muestran a continuación.

MsgType Field Value	MsgType	MsgType Field Value	MsgType
0x00	ADVERTISE	0x01	SEARCHGW
0x02	GWINFO	0x03	reserved
0x04	CONNECT	0x05	CONNACK
0x06	WILLTOPICREQ	0x07	WILLTOPIC
0x08	WILLMSGREQ	0x09	WILLMSG
0x0A	REGISTER	0x0B	REGACK
0x0C	PUBLISH	0x0D	PUBACK
0x0E	PUBCOMP	0x0F	PUBREC
0x10	PUBREL	0x11	reserved
0x12	SUBSCRIBE	0x13	SUBACK
0x14	UNSUBSCRIBE	0x15	UNSUBACK
0x16	PINGREQ	0x17	PINGRESP
0x18	DISCONNECT	0x19	reserved
0x1A	WILLTOPICUPD	0x1B	WILLTOPICRESP
0x1C	WILLMSGUPD	0x1D	WILLMSGRESP
0x1E-0xFD	reserved	0xFE	Encapsulated message
0xFF	reserved		

Figura 1.43: Tipos de mensajes MQTT.

El contenido de la parte variable del mensaje depende del tipo de mensaje. Los siguientes campos están definidos para la parte variable del mensaje:

- **ClientId** Al igual que con MQTT, el campo ClientId tiene una longitud variable y contiene una cadena de 1 a 23 caracteres que identifica de forma única al cliente ante el servidor.
- **Data** El campo Datos corresponde a la carga útil de un mensaje MQTT PUBLISH. Tiene una longitud variable y contiene los datos de la aplicación que se va publicando.
- **Duración** El campo Duración tiene una longitud de 2 octetos y especifica la duración de un período de tiempo en segundos. El valor máximo que se puede codificar es de aproximadamente 18 horas.
- **Flags** El campo Banderas tiene 1 octeto y contiene las siguientes banderas:
  - **DUP** Mismo significado que con MQTT, es decir, establecido en "0"si el mensaje se envía por primera vez; establecer en "1" si se retransmite (solo relevante dentro de los mensajes PUBLICAR);
  - **QoS** Como con MQTT para los niveles de QoS 0, 1 y 2; establecido en "0b00" para el nivel de QoS 0, "0b01" para el nivel de QoS 1, "0b10" para el nivel de QoS 2 y "0b11" para el nuevo nivel de QoS -1 (solo relevante dentro de los mensajes PUBLICAR enviados por un cliente);
  - **Retain** mismo significado que con MQTT (solo relevante dentro de los mensajes PUBLISH);
  - **Will** si está configurado, indica que el cliente está solicitando el tema Will y el mensaje Will (solo relevante dentro del mensaje CONNECT);
  - **CleanSession** mismo significado que con MQTT, aunque extendido para el tema Will y el mensaje Will (solo relevante dentro del mensaje CONNECT);

  - **TopicIdType** indica si el campo TopicId o TopicName incluido en este mensaje contiene una identificación de tema normal (establecida en "0b00"), una identificación de tema predefinida (establecida en "0b01") o un nombre de tema corto (establecido en "0b10") . El valor "0b11" está reservado. Consulte las secciones 3 y 6.7 para conocer la definición de los distintos tipos de identificadores de tema.

- **GwAdd** El campo GwAdd tiene una longitud variable y contiene la dirección de un GW. Depende de la red sobre la que opera MQTT-SN y se indica en el primer octeto de este campo. Por ejemplo, en una red ZigBee, la dirección de red tiene una longitud de 2 octetos.

- **GwId** El campo GwId tiene una longitud de 1 octeto e identifica de forma exclusiva una puerta de enlace.

- **MsgId** El campo MsgId tiene una longitud de 2 octetos y corresponde al parámetro 'ID de mensaje' de MQTT. Permite al remitente hacer coincidir un mensaje con su correspondiente acuse de recibo.

- **ProtocolId** El ProtocolId tiene una longitud de 1 octeto. Solo está presente en un mensaje CONNECT y corresponde al 'nombre de protocolo' y la 'versión de protocolo' de MQTT. Está codificado 0x01. Los demás valores están reservados

- **Radius** El campo Radio tiene una longitud de 1 octeto e indica el valor del radio de transmisión. El valor 0x00 significa "transmitir a todos los nodos de la red".

- **ReturnCode** El valor y significado del campo ReturnCode de 1 octeto de longitud.

  - 0x00 Aceptado
  - 0x01 Rechazado: congestión
  - 0x02 Rechazado: ID de tema no válido
  - 0x03 Rechazado: no compatible
  - 0x04 - 0xFF reservado

- **TopicId** El campo TopicId tiene una longitud de 2 octetos y contiene el valor de la identificación del tema. Los valores "0x0000" y "0xFFFF" están reservados y por lo tanto no deben usarse.

- **TopicName** El campo TopicName tiene una longitud variable y contiene una cadena codificada en UTF8 que especifica el nombre del tema.

- **WillMsg** El campo WillMsg tiene una longitud variable y contiene el mensaje Will.

- **WillTopic** El campo WillTopic tiene una longitud variable y contiene el nombre del TopicName.

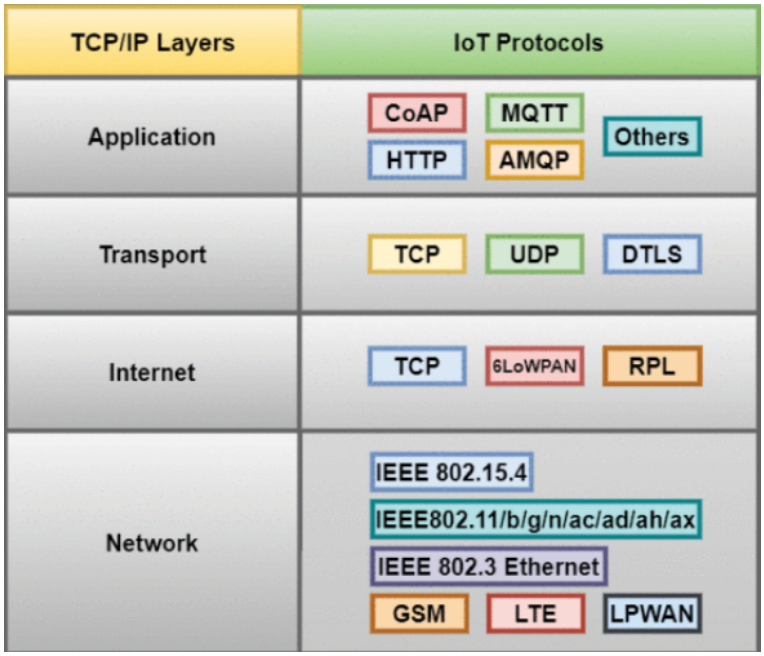


Figura 1.44: Modelo OSI (MQTT en la capa de aplicación).

La Figura 1.45 ilustra el intercambio de mensajes que se da en una comunicación MQTT entre un MQTT publisher y un MQTT Broker. Donde, los usuarios establecen una conexión TCP/IP con el broker, el cual gestiona un registro de los usuarios conectados. Esta conexión permanece activa hasta que el usuario la cierra. De manera predeterminada, MQTT utiliza el puerto 1883 y el 8883 cuando opera a través de TLS. En este proceso, el cliente envía un mensaje CONNECT que incluye información esencial (nombre de usuario, contraseña, client-id, entre otros). A esto, el broker responde con un mensaje CONNACK, proporcionando el resultado de la conexión (ya sea aceptada, rechazada, etc.).

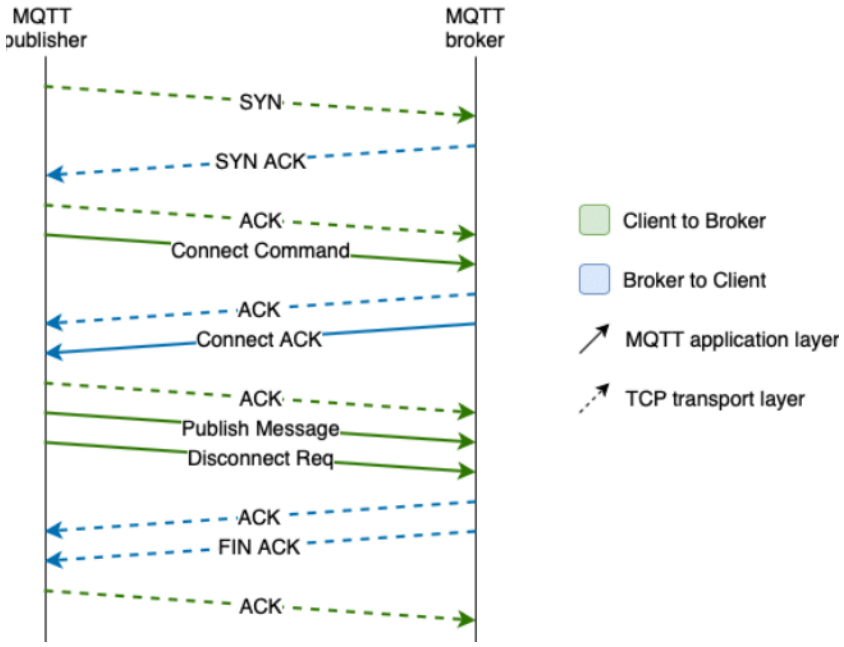


Figura 1.45: Intercambio de mensajes MQTT).

Para transmitir mensajes, el cliente utiliza mensajes PUBLISH, los cuales incluyen el tema (topic) y la carga útil (payload).

Para registrar y cancelar la suscripción, se utilizan mensajes SUBSCRIBE y UNSUBSCRIBE, respectivamente, a los cuales el servidor responde con SUBACK y UNSUBACK.

Por otro lado, para asegurar que la conexión está activa los clientes mandan periódicamente un mensaje PINGREQ que es respondido por el servidor con un PINGRESP. Finalmente, el cliente se desconecta enviando un mensaje de DISCONNECT.

1.16. Biografía

Erick Pérez P.

Nació en Cuenca-Ecuador el 05 de noviembre de 1999. Obtuvo su título de Técnico en Aplicaciones Informáticas en la Unidad Educativa Técnico Salesiano en el año 2017. Obtuvo su título de Ingeniero en Telecomunicaciones en la Facultad de Ingeniería de la Universidad de Cuenca en el año 2023.