ARQUITECTURA Y CONECTIVIDAD

Profesor: Jorge Morales

Integrantes

- Fernando Gimenez Coria - FerCbr
- Nicolás Barrionuevo - NicolasB-27
- Macarena Aylen Carballo - MacarenaAC
- Raul Jara - r-j28
- Diego Ezequiel Ares - diegote7
- Juan Diego Gonzaléz Antoniazzi - JDGA1997

Módulo II: Arquitectura en Redes IoT

Informe trabajo práctico #5

Índice

1. ¿Qué es un protocolo COAP?, ¿Para qué se usa? Ejemplifique.

El protocolo COAP (Constrained Application Protocol) es un protocolo de aplicación diseñado específicamente para su uso en dispositivos de Internet de las Cosas (IoT) con limitaciones de recursos, tales como aquellos con capacidad de procesamiento limitada, memoria limitada y baja energía. Se considera un protocolo web utilizado para correr en dispositivos con recursos limitados y está apuntado a correr en dispositivos simples, permitiendo que puedan comunicarse sobre internet.

COAP tiene una fuerte semejanza con el protocolo HTTP y utiliza el modelo de solicitudes-respuesta similar al HTTP. Sin embargo, COAP está optimizado para redes con restricciones de ancho de banda y energía y utiliza un encabezado más compacto y un conjunto de métodos más liviano en comparación con HTTP

Algunas de sus características clave incluyen:

- Encabezado comprimido, formato de paquete simple y mensajes muy cortos. El mensaje COAP más pequeño tiene solo cuatro bytes.

- Utiliza el protocolo UDP como capa de transporte para reducir los gastos generales de la red.

- Admite intercambio de mensajes asincrónicos.

- Posee una baja sobrecarga de datos asociados a cada paquete.

- Es simple de analizar con distintas herramientas.

- Es posible diseñar sus recursos de manera análoga a HTTP, tiene compatibilidad con la definición unificada de recursos (URI) y puede manejar distintos tipos de contenido.

- Comparte capacidades de proxy y caché con HTTP.

- Tiene la capacidad de observar si ocurrieron cambios en algún recurso en particular de manera nativa.

- Es capaz de detectar si nuevos dispositivos se unieron a la red.

- Incluye otras características como multicast.

- Para compensar la falta de fiabilidad de UDP, tiene un mecanismo de retransmisión de mensajes.

- No admite la conexión persistente y no tiene mensajes de heartbeat.

- El dispositivo debe activarse antes de realizar los servicios, lo que puede resultar en un rendimiento deficiente en tiempo real

¿Para qué se usa?

COAP se utiliza para facilitar la comunicación entre dispositivos en redes de IoT y permite la transferencia de datos de manera eficiente y confiable. El objetivo principal es proporcionar un protocolo liviano y eficiente para dispositivos con restricciones.

Algunos casos de uso comunes para COAP incluyen:

- **Monitoreo y Control de Sensores**: Para la comunicación entre dispositivos de sensores y sistemas de monitoreo centralizados. Por ejemplo, un sensor de temperatura podría enviar datos a un servidor central a través de COAP. En un entorno industrial, sensores monitoreando parámetros pueden enviar datos a un servidor en la nube y recibir comandos de control. También se ejemplifica con redes de sensores ambientales en una ciudad.

- **Automatización del Hogar**: Para controlar dispositivos domésticos inteligentes como luces, termostatos y electrodomésticos, permitiendo la comunicación entre sí y con un controlador central.

- **Gestión de Energía**: Para monitorear y controlar el consumo de energía en edificios o sistemas de energía renovable. Un sistema de paneles solares puede informar su producción de

energía a un sistema de gestión centralizado usando COAP. También se menciona el uso en medidores de electricidad inteligentes.

- **Seguimiento de Activos**: En aplicaciones donde los dispositivos de seguimiento pueden comunicar su ubicación y estado a una plataforma centralizada. Esto es útil en logística y gestión de flotas.

- En general, es adecuado para dispositivos que requieren el mecanismo de suspensión / activación en escenarios de IoT, ahorrando energía de la batería.

- Permite la observación de recursos, donde un cliente puede recibir actualizaciones sobre un determinado recurso cuando cambia su estado, siendo útil para sensores de puerta o temperatura.

- Es conveniente usar COAP cuando el hardware no puede ejecutar HTTP debido a limitaciones de memoria, tamaño del programa o capacidad de procesamiento.

- También es útil para optimizar el consumo de energía en dispositivos remotos alimentados por baterías, ya que UDP ahorra ancho de banda.

Ejemplifique.

1. **Red de sensores ambientales**: Sensores desplegados en una ciudad envían información sobre la calidad del aire, temperatura y humedad a una plataforma centralizada utilizando COAP para su procesamiento y toma de decisiones.

2. **Control de iluminación inteligente**: Un teléfono móvil envía solicitudes COAP (PUT method) para encender o apagar luces específicas (identificadas por URIs como "coap://192.168.1.100/light") en un sistema de iluminación inteligente, incluyendo información como {"state": "on"} o {"state": "off"} en el cuerpo del mensaje.

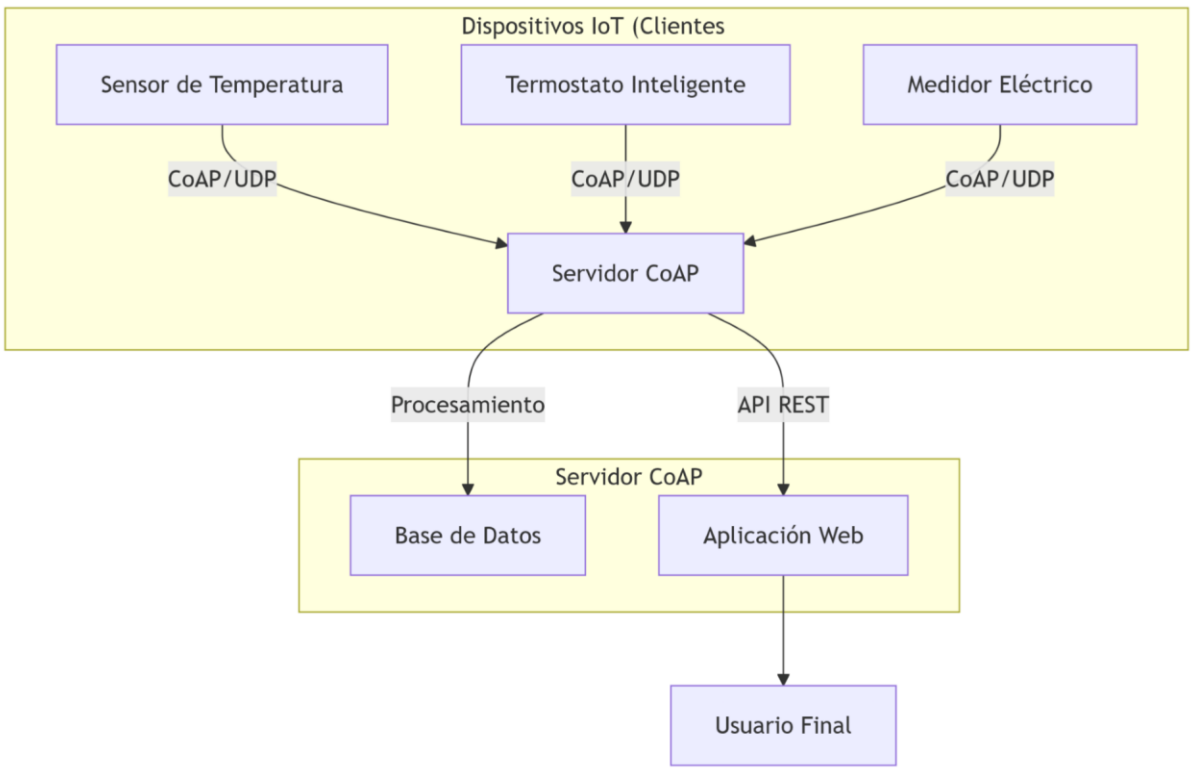
3. **Obtención de la temperatura de un sensor**: Un cliente con dirección IP 192.168.1.100 envía una solicitud GET a coap://192.168.1.200:5683/sensor/temperature a un servidor COAP. El servidor responde con un código 2.05 Content y un cuerpo que contiene la temperatura en formato JSON, por ejemplo, {"temperature": 25.5}.

4. **Control de una red de sensores industriales**: Sensores que monitorean temperatura y humedad envían datos a un servidor en la nube a través de COAP y reciben comandos para ajustar su configuración.

5. Soluciones en medidores de agua y electricidad inteligentes, agricultura inteligente, y estacionamiento inteligente utilizan el protocolo COAP para la comunicación de datos.

Diagramas

Diagrama de Arquitectura General de CoAP



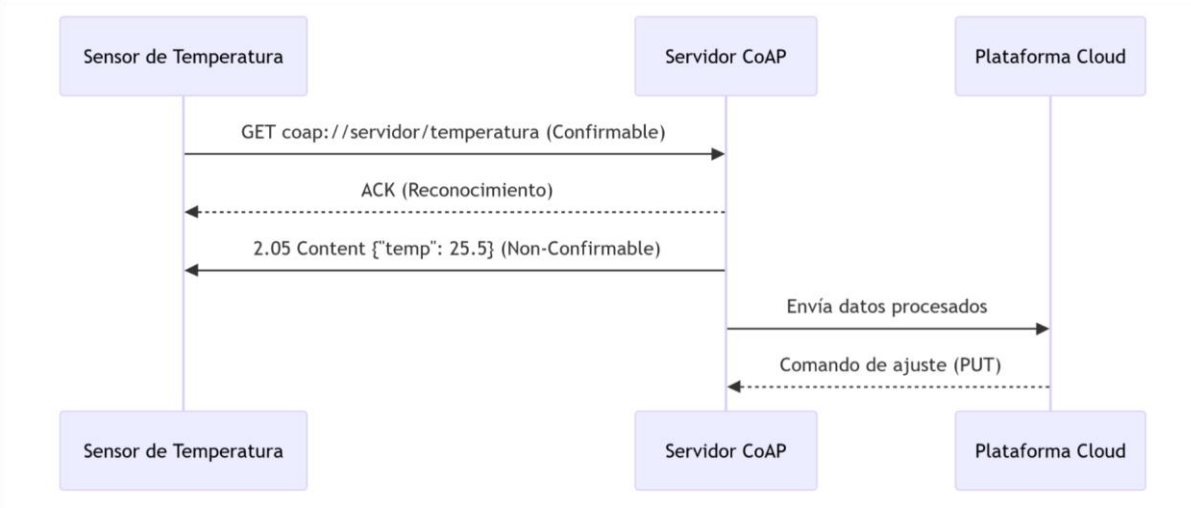
Explicación

- Los dispositivos IoT (clientes) se comunican con el servidor CoAP mediante UDP.

- El servidor centraliza los datos y puede integrarse con aplicaciones web o bases de datos.

- CoAP actúa como puente entre dispositivos restringidos y sistemas tradicionales.

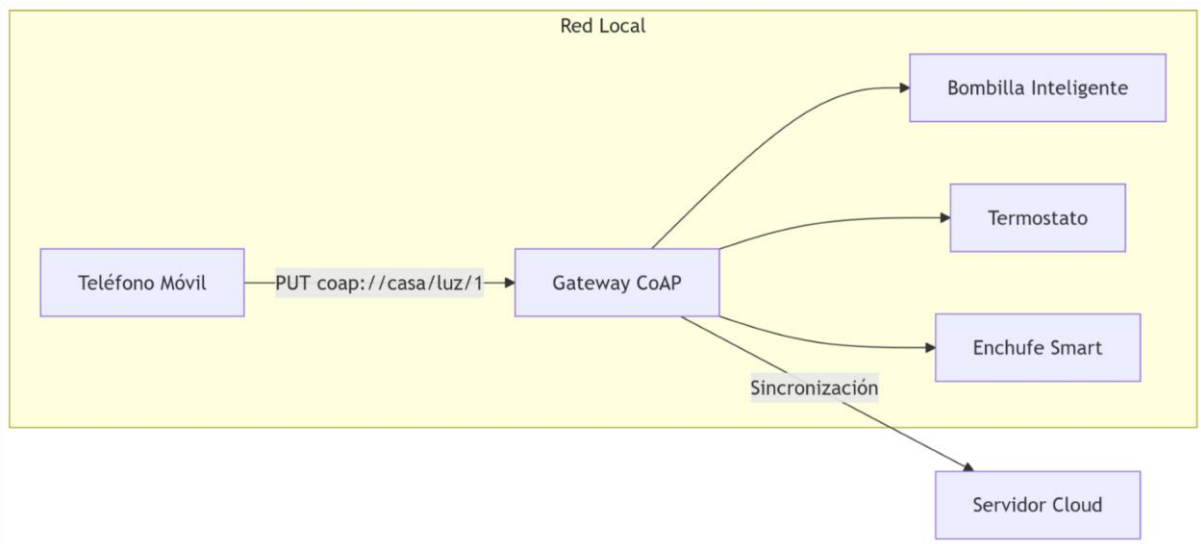
Diagrama de Secuencia - Monitoreo de Sensores



Características destacadas

- Uso de mensajes **Confirmable/Non-Confirmable**.
- Códigos de respuesta similares a HTTP (ej. 2.05 Content).
- Integración con plataforma cloud.

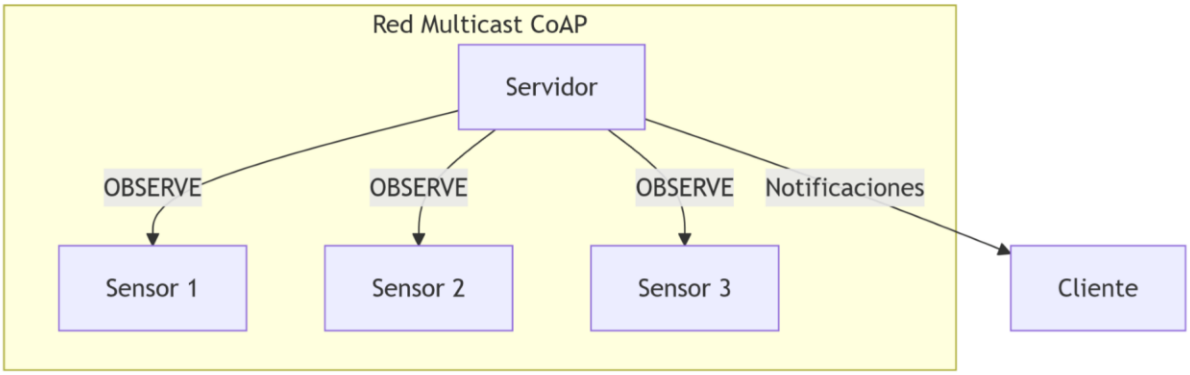
Diagrama de Caso de Uso - Automatización del Hogar



Flujo

1. El usuario envía un comando (ej. {"state": "on"}) desde su móvil.
2. El gateway CoAP (servidor local) distribuye la acción al dispositivo correcto.
3. Opcionalmente, los datos se sincronizan con la nube.

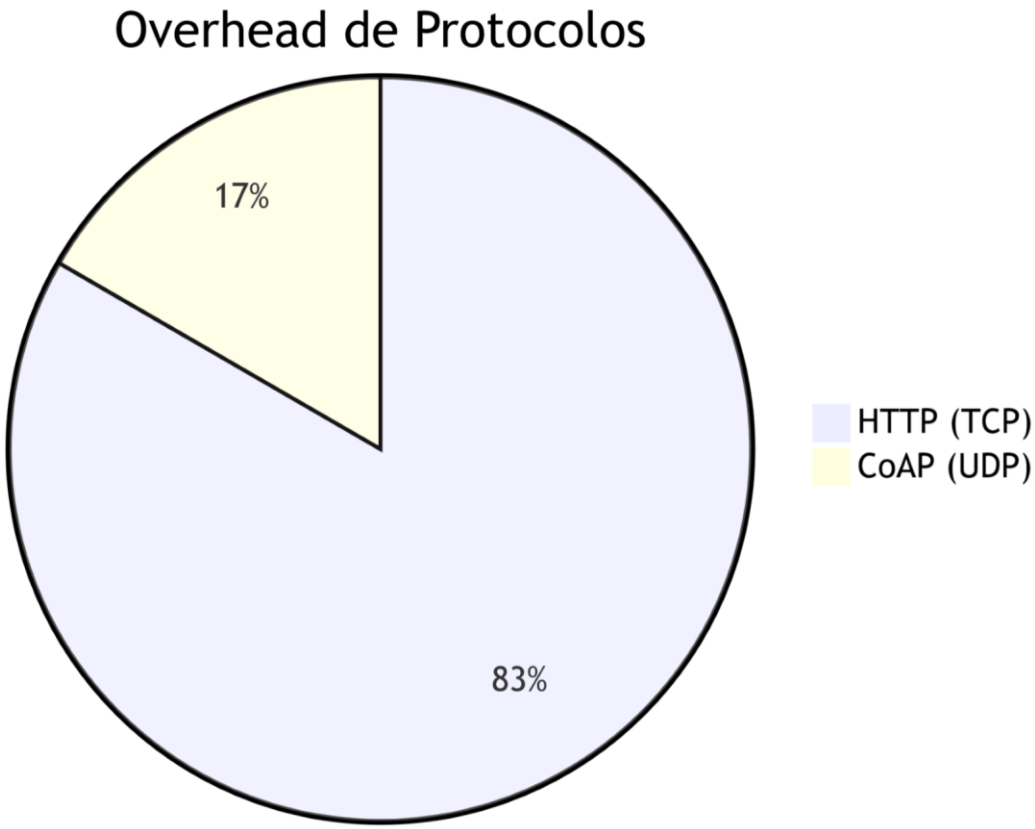
Diagrama de Red - Observación de Recursos



Funcionamiento

- El servidor suscribe (OBSERVE) a múltiples sensores usando **multicast**.
- Cuando un sensor cambia su estado (ej. temperatura), notifica automáticamente al cliente.

Diagrama de Comparación CoAP vs HTTP



Key Point: CoAP reduce el overhead con encabezados de **4 bytes** vs los típicos 20+ bytes de HTTP/TCP.

2. ¿Qué es un protocolo AMQP?, ¿Para qué se usa? Ejemplifique

AMQP (Advanced Message Queuing Protocol) es un protocolo abierto y estándar que opera a nivel de la capa de aplicación. Sus características principales definen la creación de mensajes, el encolamiento, el enrutamiento de los mensajes producidos y la exactitud para entregarlos a los consumidores. Se compone de un broker de mensajería que internamente posee exchanges (donde se conectan los productores de mensajes) y colas (que se vinculan a los exchanges a través de diferentes criterios). Los consumidores de los datos se conectan a las colas para extraer los mensajes que producen los publicadores.

El protocolo AMQP establece el comportamiento tanto del servidor de mensajería como de los clientes que se conectan al broker, de manera que las implementaciones de diferentes proveedores son interoperables. Esto permite implementar aplicaciones multiplataforma utilizando agentes, bibliotecas y frameworks heterogéneos, todos independientes del proveedor. El formato del mensaje AMQP proporciona la unidad de trabajo necesaria para intercambiar información, creando un "cable" entre las aplicaciones conectadas. Incluye funcionalidad para la entrega fiable de mensajes, representar los datos a través de diferentes formatos, flexibilidad para definir los datos, está preparado para la escalabilidad y tiene la capacidad de definir varias topologías en un mismo sistema.

AMQP fue diseñado con objetivos clave como seguridad, fiabilidad, interoperabilidad, estándar y apertura. Es un protocolo binario con características como negociación, multicanal, portabilidad, eficiencia y mensajería asincrónica. Se divide en una capa funcional que define los comandos para la aplicación y una capa de transporte que ayuda a transportar las diferentes técnicas entre el servidor y la aplicación.

¿Para qué se usa?

AMQP se utiliza para pasar mensajes comerciales entre aplicaciones u organizaciones, conectando sistemas y alimentando los procesos comerciales con la información que necesitan. También transmite de manera fiable las instrucciones para lograr sus objetivos. Permite la multiplexación, por lo que se puede usar una sola conexión para muchas rutas de comunicación entre los nodos.

Algunos casos de uso comunes incluyen:

- Sistemas de mensajería y colas de mensajes, permitiendo la comunicación asíncrona entre diferentes aplicaciones de manera fiable y eficiente.

- Integración de aplicaciones y sistemas diversos, facilitando la comunicación y el intercambio de información. Por ejemplo, conectar sistemas de gestión de inventario

  con sistemas de ventas o logística.

- Internet de las Cosas (IoT), para el intercambio de datos entre dispositivos y sistemas, como en entornos de hogares inteligentes.

- Finanzas y servicios financieros, para la comunicación segura y eficiente entre sistemas relacionados con la transmisión de datos financieros, procesamiento de transacciones y gestión de riesgos.

- Implementación de arquitecturas distribuidas y microservicios.

- Intercambio de información entre distintas aplicaciones, tanto internas como externas.

- Creación de APIs confiables y seguras, facilitando la transmisión y recepción de mensajes entre aplicaciones.

- Implementación de una Arquitectura Orientada a Servicios (SOA).

- Posibilitar la comunicación asíncrona entre transmisor y receptor.

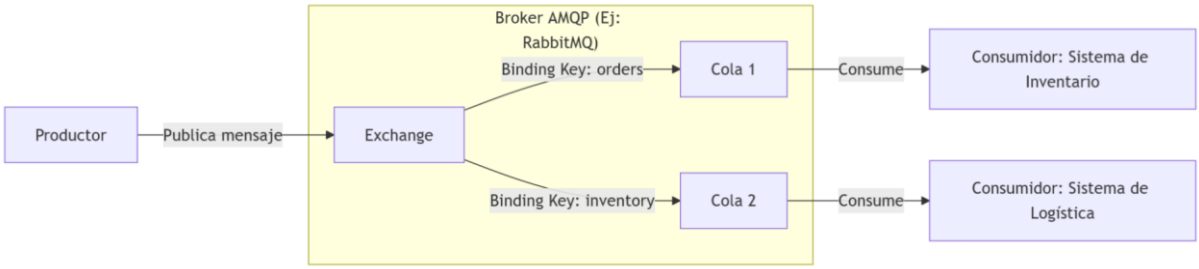
Ejemplifique.

El uso de AMQP en una aplicación de comercio electrónico que necesita enviar notificaciones de pedidos a un sistema de gestión de inventario. En lugar de comunicarse directamente, la aplicación de comercio electrónico envía mensajes al sistema de gestión de inventario utilizando el protocolo AMQP. Estos mensajes contienen información sobre los pedidos realizados, como los productos solicitados y las cantidades. El sistema de gestión de inventario recibe los mensajes a través de una

cola, los procesa y actualiza su inventario en consecuencia. De esta manera, el protocolo AMQP facilita la comunicación entre ambas aplicaciones, asegurando que los mensajes sean entregados de manera confiable y permitiendo una integración eficiente.

Diagramas

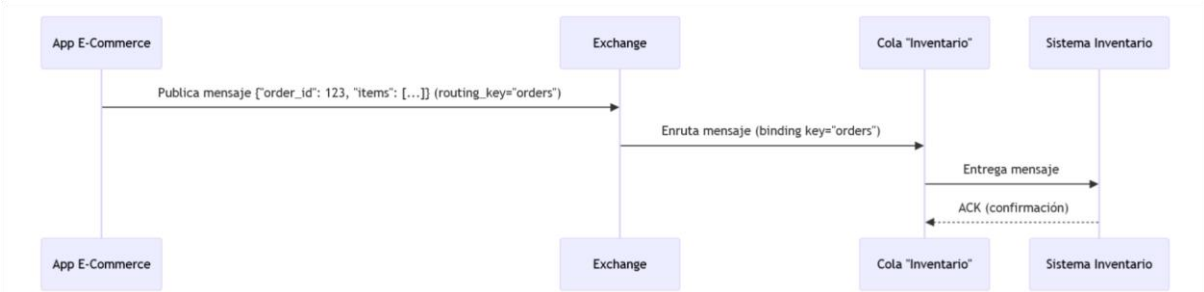
Diagrama de Arquitectura AMQP Básica



Componentes clave

- **Exchange**: Recibe mensajes y los enruta a colas según reglas (bindings).
- **Colas**: Almacenan mensajes hasta que son consumidos.
- **Bindings**: Reglas de enrutamiento (ej: routing keys).

Diagrama de Secuencia - Comercio Electrónico

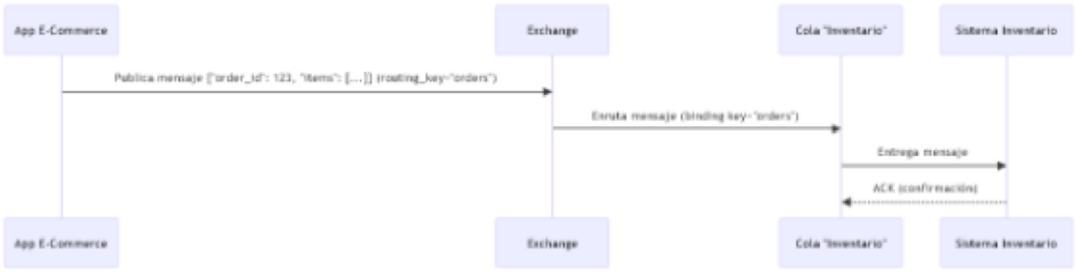


Flujo típico

- El productor publica mensajes en un exchange con routing key.
- El broker enruta el mensaje a la cola correspondiente.

- El consumidor procesa el mensaje y envía ACK.

Diagrama de Topologías AMQP



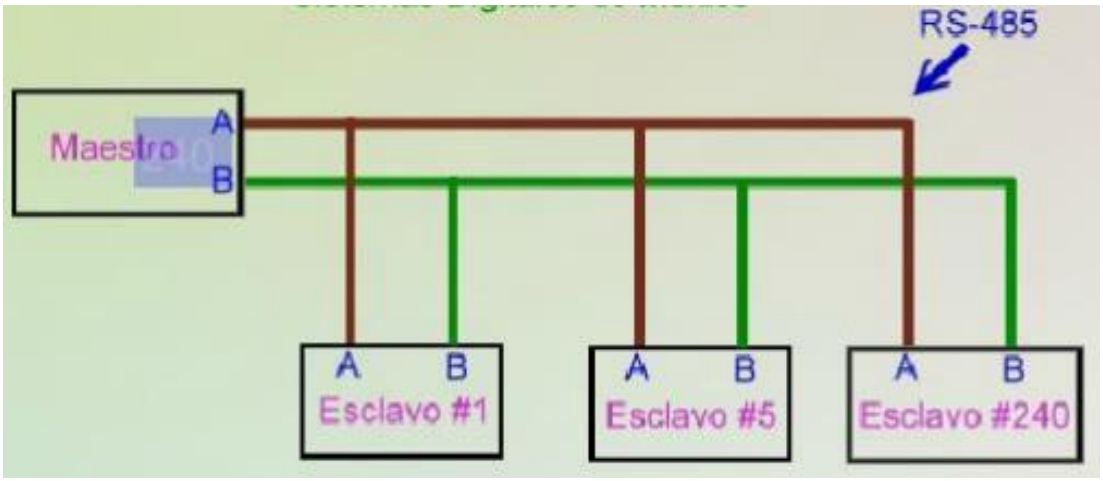
Tipos de Exchange

1. **Direct**: Enrutamiento exacto (1:1).
2. **Fanout**: Broadcast (1:N).
3. **Topic**: Enrutamiento por patrones (ej: *.critical).

3) ¿Qué es un protocolo MODBUS?, ¿Para qué se usa? Ejemplifique

MODBUS es un protocolo de comunicación abierto y estándar, desarrollado por la empresa Modicon (hoy parte de Schneider Electric) en 1979. Fue creado para facilitar la comunicación entre dispositivos electrónicos industriales, especialmente en sistemas de automatización y control.

Es ampliamente utilizado debido a su simplicidad, robustez y facilidad de implementación.



¿Para qué se usa MODBUS?

MODBUS permite que dispositivos como sensores, controladores lógicos programables (PLC), actuadores y sistemas SCADA (Supervisory Control and Data Acquisition) se comuniquen entre sí para monitorear y controlar procesos industriales.

Se utiliza principalmente para:

- **Monitoreo de sensores**: lectura de datos de temperatura, presión, humedad, etc.
- **Control de dispositivos**: encender o apagar válvulas, motores, bombas.
- **Supervisión de procesos**: enviar datos a sistemas SCADA para visualizar el estado de las operaciones.

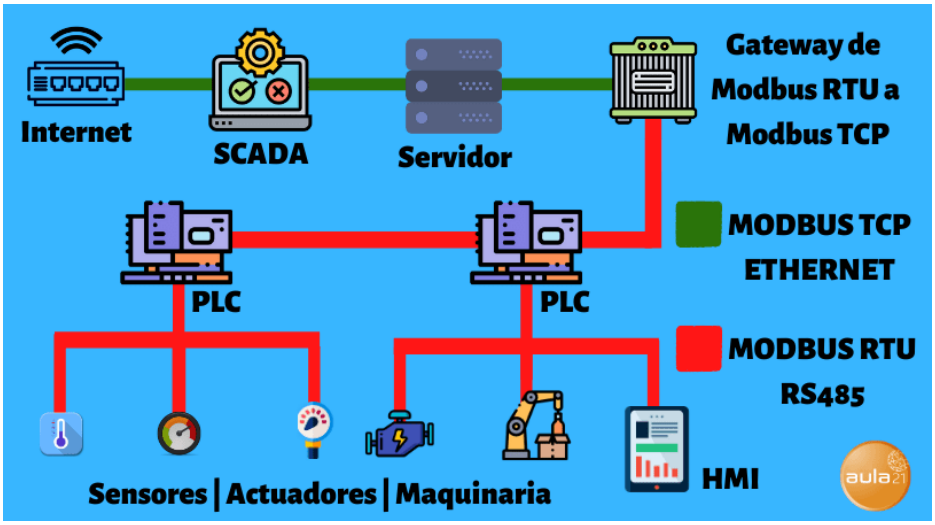
Características de MODBUS

- **Modelo maestro-esclavo**: Un dispositivo maestro inicia las comunicaciones y los esclavos responden.

- **Flexible**: Puede funcionar sobre distintos medios de transmisión (cable serial, Ethernet, radiofrecuencia).
- **Estandarizado**: Es un protocolo abierto, lo que facilita su adopción.
- **Datos estructurados**: La información se organiza en registros o bobinas.

Tipos de MODBUS

- **MODBUS RTU**: Comunicación serial tradicional (RS-232, RS-485), usando una representación binaria compacta.
- **MODBUS ASCII**: Comunicación serial donde los datos son codificados como caracteres ASCII (menos eficiente, pero más fácil de leer).
- **MODBUS TCP/IP**: Variante que utiliza redes Ethernet (TCP/IP) para transmitir los datos.

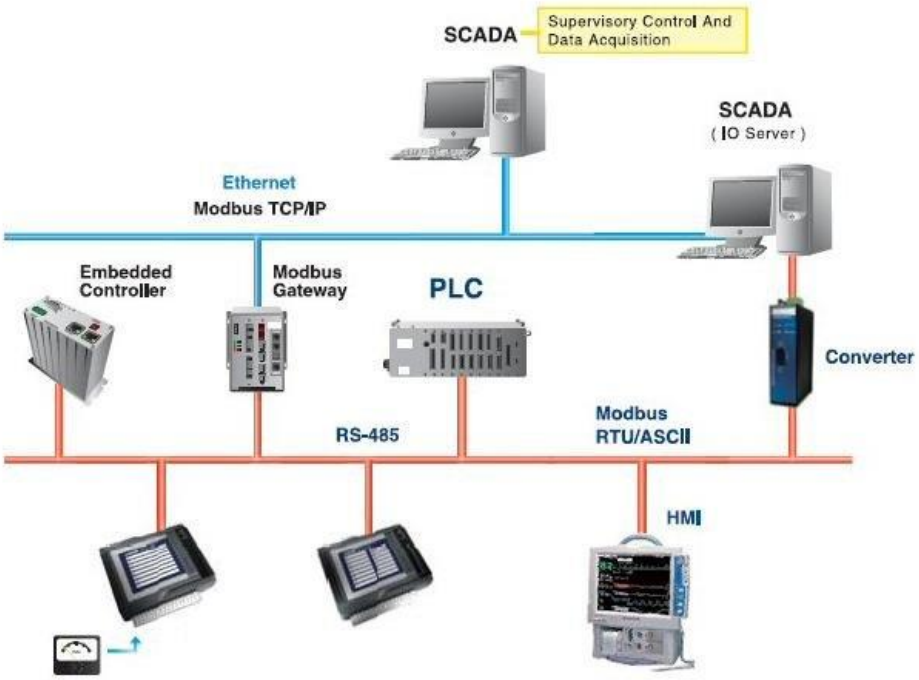


Ejemplo de uso

Imaginemos una fábrica de procesamiento de alimentos donde se necesita monitorear la temperatura de varios hornos. Cada horno está equipado con un sensor de temperatura que se comunica usando MODBUS RTU.

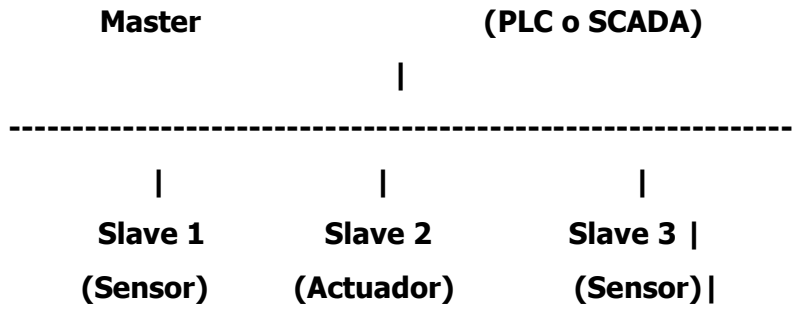
Un PLC actúa como maestro y consulta periódicamente a cada sensor esclavo para obtener las lecturas de temperatura. Los datos recolectados son enviados a un sistema SCADA para ser visualizados en tiempo real.

En la figura de abajo vemos un ejemplo de red con el protocolo Modbus, con una gateway haciendo la conexión entre los dos tipos de Modbus, el serial sobre RS-485 y el TCP/IP en ethernet. En el mercado existe la opción de gateway Modbus Wireless. El maestro de la red, que en este caso es un PLC envía y recibe datos de los esclavos, que son un inversor de frecuencia, una HMI, un controlador de temperatura y una interface de I/O.



La estación maestra inicia la comunicación solicitando que los esclavos envíen sus datos. Los esclavos, por su parte, reciben el pedido del maestro y devuelven los datos solicitados. Los datos transmitidos pueden ser discretos o números, es decir, es posible enviar un bit para encender o apagar un motor o enviar valores numéricos como temperatura y presión.

DIAGRAMA



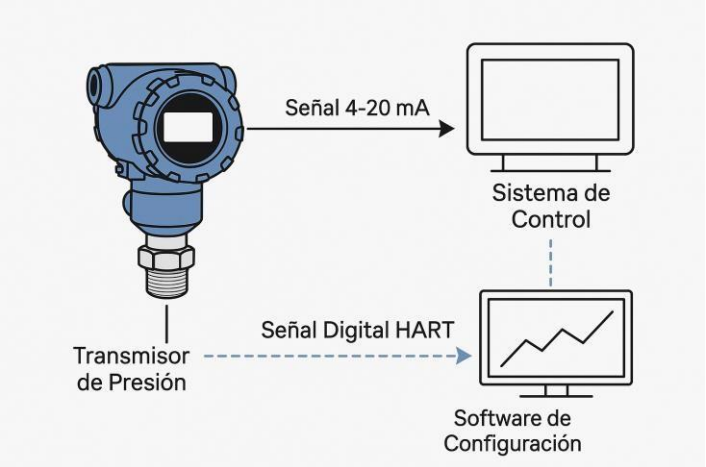
⇅ Comunicaciones MODBUS RTU (RS-485)

Explicación rápida:

- El **Master** es quien inicia la comunicación (pide datos o da órdenes).
- Los **Slaves** responden únicamente cuando el Master les habla.
- La comunicación se realiza sobre un bus físico (por ejemplo, **RS-485**) donde todos están conectados.
- Utilizan el protocolo **MODBUS RTU** (formato binario eficiente).

4. ¿Qué es un protocolo HART?, ¿Para qué se usa? Ejemplifique

HART (Highway Addressable Remote Transducer)

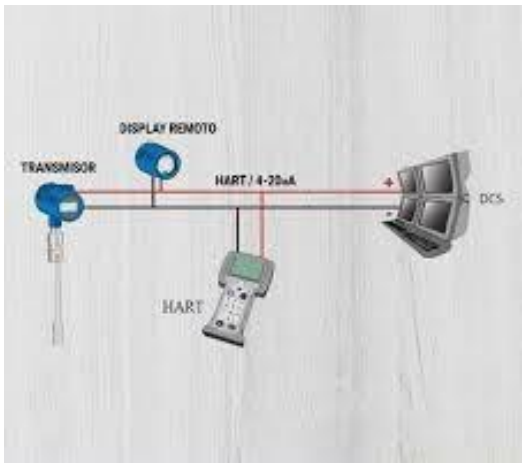


La comunicación entre dispositivos de campo y sistemas de control es fundamental para garantizar la eficiencia, el control de procesos y el mantenimiento predictivo. En este contexto, surge el protocolo HART (Highway Addressable Remote Transducer) como una solución que combina las señales analógicas tradicionales con capacidades digitales avanzadas. Este informe tiene como objetivo describir qué es el protocolo HART, para qué se utiliza y ejemplificar su aplicación práctica en el entorno industrial.

¿Qué es un protocolo HART?

Es un estándar de comunicación que permite la transmisión de datos digitales sobre una señal analógica convencional de 4-20 mA. Desarrollado en los años 80 por Rosemount Inc. y actualmente administrado por la FieldComm Group, HART permite la comunicación bidireccional entre dispositivos de campo (como sensores y actuadores) y los sistemas de control, sin interrumpir la operación de las señales analógicas.

Esta tecnología ha sido ampliamente adoptada por su compatibilidad con infraestructuras existentes y por ofrecer una capa adicional de información, útil para configuraciones, diagnósticos y monitoreo de dispositivos.



¿Para qué se usa?

Se utiliza en una gran variedad de procesos industriales, destacándose en:

- **Configuración remota de dispositivos:** Permite ajustar parámetros sin necesidad de intervenir físicamente en el dispositivo.
- **Monitoreo de variables de proceso:** Facilita la supervisión de variables como presión, temperatura y caudal.
- **Diagnóstico de estado:** Brinda información sobre el estado interno de los dispositivos, lo que permite implementar estrategias de mantenimiento preventivo o predictivo.
- **Calibración de instrumentos:** Mejora la precisión y la facilidad de calibrar sensores y actuadores desde sistemas centrales.

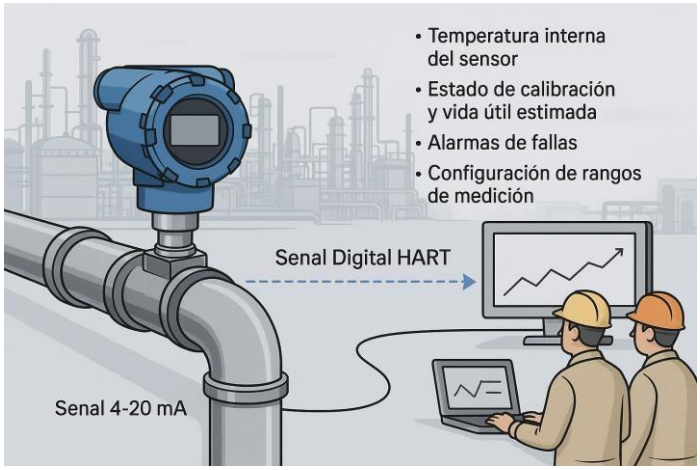
Su principal ventaja es mantener la señal analógica continua para control de procesos, mientras que simultáneamente transmite datos digitales adicionales para gestión avanzada.

Ejemplo de uso

HART es en un transmisor de presión instalado en una planta petroquímica. Este dispositivo envía una señal de 4-20 mA proporcional a la presión medida hacia el sistema de control. De forma simultánea, utilizando la comunicación HART, puede transmitir datos adicionales como:

- Temperatura interna del sensor.
- Estado de calibración y vida útil estimada.
- Alarmas de fallas.
- Configuración de rangos de medición.

De este modo, los operadores pueden hacer ajustes o diagnósticos remotos, optimizando la operación y reduciendo tiempos de parada.



De este modo representa una evolución significativa en la comunicación industrial, al permitir la coexistencia de señales analógicas y digitales en un mismo par de cables. Gracias a su capacidad de configuración remota, diagnóstico y transmisión de datos avanzados, se ha convertido en una herramienta clave para mejorar la eficiencia, confiabilidad y mantenimiento de los sistemas de automatización industrial. La implementación de HART en dispositivos de campo permite a las empresas optimizar procesos, reducir costos de mantenimiento y aumentar la disponibilidad de la planta.

5. ¿Qué es un protocolo PROFINET? ¿Para qué se usan? Ejemplifique.

Son muchas las voces en la industria que consideran a PROFINET un estándar de redes de comunicación en las empresas manufactureras.

PROFINET (Process Field Network) es un protocolo de comunicación Ethernet industrial estándar basado en estándares abiertos TCP/IP e IT y desarrollado con un enfoque en la semejanza a PROFIBUS DP, que permite la conexión y el intercambio de datos entre dispositivos en entornos de automatización industrial. Se usa para conectar controladores lógicos programables (PLCs), dispositivos de entrada/salida (I/O), sensores, actuadores y otros dispositivos en una red de campo, facilitando la comunicación en tiempo real y la integración de sistemas de automatización.

¿Por qué se utiliza PROFINET?

La integración de la tecnología de la información en la automatización abre opciones de comunicación significativamente mejores entre los sistemas de automatización, ampliando las posibilidades de configuración y diagnóstico, así como la funcionalidad de servicio en toda la red.

Estas funciones han sido componentes integrales de PROFINET desde el principio. Además, la demanda de una mayor productividad de las máquinas y de las plantas de producción y, al mismo tiempo, la reducción de los costos ha sido siempre la fuerza motriz de las innovaciones en la automatización industrial.

Satisface todos los requisitos de la tecnología de automatización. Tanto si se trata de la automatización de fábricas, de procesos o de accionamientos (con o sin seguridad funcional).

¿Para qué se usa?

- **Intercambio de datos en tiempo real:** PROFINET garantiza la transmisión rápida y confiable de datos entre dispositivos, lo que es crucial para aplicaciones de automatización industrial.
- **Integración de sistemas de automatización:** Permite la conexión de diferentes dispositivos y sistemas en una red, lo que facilita la gestión y el control de procesos industriales.

- **Diagnóstico y configuración:** Facilita la configuración y el diagnóstico de dispositivos y sistemas de automatización, permitiendo identificar y solucionar problemas de manera eficiente.

- **Redes industriales:** Proporciona una forma de comunicación estandarizada y confiable para redes de campo en entornos industriales, mejorando la productividad y la eficiencia.

Ejemplos:

- **Control de máquinas:** En una fábrica de fabricación, PROFINET puede ser utilizado para conectar un PLC con un motor variable, permitiendo el control preciso del motor.

- **Robótica:** En la robótica industrial, PROFINET puede ser utilizado para conectar un PLC con un robot, permitiendo el control y la programación del robot.

- **Industria de procesos:** PROFINET puede ser utilizado en la industria de procesos para conectar instrumentos de proceso, controladores y otros dispositivos en una red, permitiendo la gestión y el control de procesos químicos.

- **Automatización de edificios:** En la automatización de edificios, PROFINET puede ser utilizado para conectar dispositivos de iluminación, climatización, seguridad y otros dispositivos en una red, permitiendo la gestión y el control de sistemas de edificios.

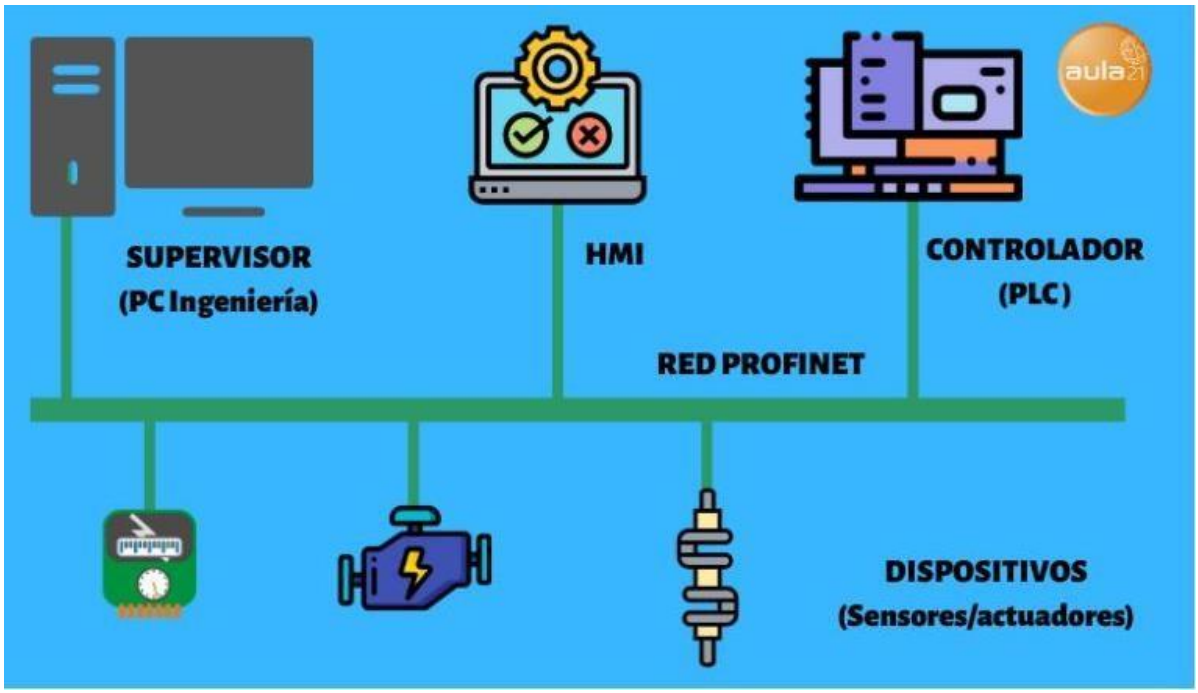
Características principales

- Instalación flexible y topología de red.
- Escalable en tiempo real.
- Alta disponibilidad.
- Seguridad integrada.

Cómo funciona PROFINET

PROFINET funciona con cable Ethernet de cobre, cable de fibra óptica (FO), cable de alimentación a través de Ethernet (PoE) e inalámbrico. Los componentes disponibles para su infraestructura dependen de la dureza del entorno y de si se utiliza o no PROFINET IRT.

Diagrama Básico de PROFINET



Roles del nodo PROFINET

PROFINET clasifica los dispositivos en tres tipos: controladores, dispositivos y supervisores.

- Los **controladores** son dispositivos que ejecutan un programa de automatización e intercambian datos con los dispositivos.
- Los **dispositivos** son sensores/actuadores conectados al controlador a través de Ethernet.
- Los **supervisores** son un HMI, un PC u otros dispositivos de puesta en marcha, monitoreo o análisis de diagnóstico. **Ventajas de PROFINET**

  Alta velocidad: capacidad de desplegar miles de nodos con actualizaciones de 1ms.

  Amplia difusión: tiene la mayor base de instalación de cualquier Ethernet Industrial y está creciendo rápidamente.

  Diagnósticos avanzados: proporciona diagnósticos a nivel de dispositivo, módulo y canal. Los protocolos Ethernet como el Simple Network Management Protocol (SNMP) se utilizan para extraer datos de los conmutadores Ethernet.

  Apoyo de la comunidad de usuarios: muchos expertos de PROFINET, un activo comité técnico/grupo de trabajo y asociaciones de proveedores en colaboración.

Facilidad de instalación.

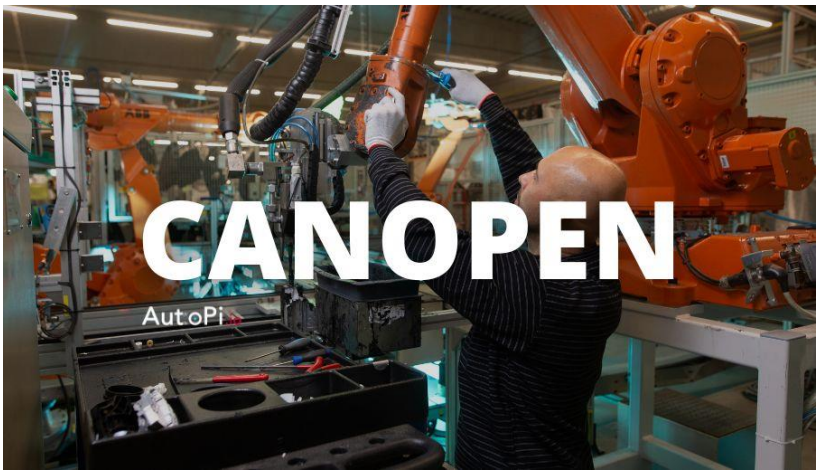
Tiempo mínimo de puesta en marcha y apoyo de ingeniería.

6) ¿Qué es un protocolo CANopen?, ¿Para qué se usa? Ejemplifique

Protocolo CANopen

CANopen es un protocolo de comunicación basado en el bus de campo **CAN** (Controller Area Network), diseñado específicamente para sistemas de automatización industrial, como máquinas, vehículos y dispositivos embebidos.

Fue desarrollado por la organización **CiA** (CAN in Automation) en los años 90, para permitir la comunicación entre diferentes dispositivos inteligentes de una manera flexible, estandarizada y eficiente.



¿Para qué se usa CANopen?

Se utiliza para facilitar la comunicación y coordinación entre múltiples dispositivos en un sistema distribuido. Cada dispositivo conectado a la red CANopen puede ser un nodo inteligente capaz de intercambiar información de control, estado y configuración en tiempo real.

Aplicaciones típicas:

- Control de motores eléctricos.
- Automatización de fábricas y plantas industriales.
- Equipos médicos (por ejemplo, máquinas de rayos X).
- Vehículos especiales (grúas, autobuses, maquinaria agrícola).

- Robots industriales.

Características principales de CANopen

- **Comunicación en tiempo real**: muy adecuada para sistemas que requieren alta sincronización.
- **Arquitectura flexible**: permite agregar o quitar nodos fácilmente.
- **Estándares de perfil**: define perfiles para diferentes tipos de dispositivos (por ejemplo, perfil de motor, perfil de sensor).
- **Eficiencia**: bajo consumo de ancho de banda, ideal para sistemas embebidos.
- **Basado en objetos**: la comunicación se organiza mediante un *Object Dictionary* (Diccionario de Objetos) donde se describen todos los parámetros del dispositivo.

Ejemplo de uso

En una línea de producción automatizada, un sistema CANopen puede controlar varios motores, sensores de temperatura y válvulas neumáticas:

- Los motores reciben comandos de velocidad o posición desde el controlador principal.
- Los sensores de temperatura informan continuamente el estado del entorno.
- El sistema coordina todos los nodos para sincronizar los movimientos de la maquinaria en tiempo real.

Así, mediante el protocolo CANopen, todos los componentes trabajan coordinadamente como si fueran un único sistema inteligente.

Un vistazo más de cerca a la gama de protocolos de CANopen

- **Protocolo DOP:** Utiliza objetos de datos de proceso para el control y el estado de alta prioridad transmisión, transmisión de datos en tiempo real entre dispositivos.
- **Protocolo SDO:** Los objetos de datos de servicio permiten el acceso y la modificación de CANopen Entradas del diccionario de objetos.
- **Protocolo NMT:** Administración de red utilizada para controlar los estados de los dispositivos, como estados de inicialización, operativos y detenidos.

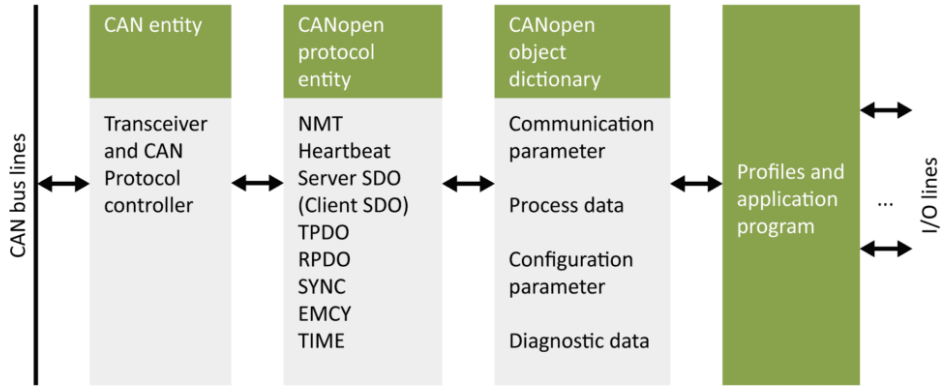
- **Protocolos de control de errores:** Supervise el estado de la red CANopen, incluidos los latidos Protocolo para comprobaciones de estado 'activo'.
- **Protocolo SYNC:** Facilita las actividades de red sincrónicas.
- **Protocolo de marca de tiempo (TIME):** Ajusta el tiempo de la red y sincroniza los dispositivos.
- **Protocolo de Emergencia (EMCY):** Notifica a la red los errores internos del dispositivo.
- **Protocolo de protección:** Comprueba regularmente el estado de los nodos para garantizar que la red integridad.
- **Servicios de configuración de capas (LSS):** Permite la configuración del ID de nodo y la consulta de Propiedades del dispositivo.
- **Protocolo Flying Master:** Permite la selección dinámica de maestros para la flexibilidad de la red.
- **Protocolo de seguridad CANopen:** Mejora la seguridad de la red a través de la comprobación de errores adicional Medidas.

Características y ventajas clave Características y ventajas clave de CANopen

1. Escalabilidad y flexibilidad: Una de las principales fortalezas de CANopen reside en su escalabilidad, que se adapta a redes de distintos tamaños y complejidades.

Su estructura modular permite una fácil integración y expansión de nodos adicionales, lo que lo hace adecuado para aplicaciones que van desde máquinas simples hasta sistemas automotrices complejos.

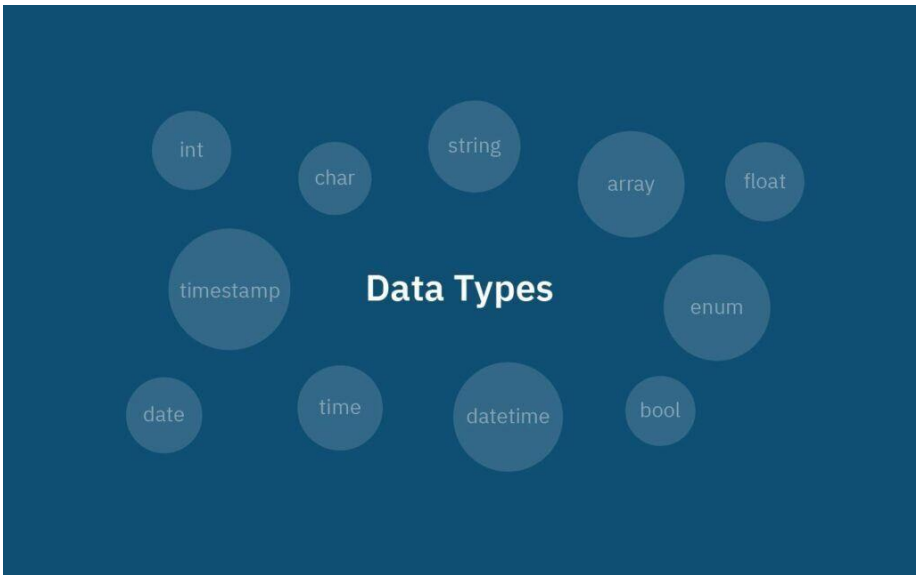
2. Perfiles de dispositivos y diccionario de objetos: CANopen ofrece una amplia gama de perfiles de dispositivos estandarizados, conocidos como perfiles de dispositivos (DP), que se adaptan a diversas funciones como motores, sensores, actuadores y más. Estos DP garantizan una interoperabilidad perfecta entre diferentes componentes, lo que contribuye a la eficiencia general de los vehículos eléctricos ligeros.



3. Comunicación en tiempo real: En el contexto de los vehículos eléctricos ligeros, la comunicación en tiempo real es de suma importancia para garantizar respuestas rápidas y precisas entre los distintos componentes del vehículo. El enfoque basado en mensajes de CANopen permite la transferencia de datos en tiempo real, lo que lo hace adecuado para aplicaciones que requieren una coordinación oportuna, como el frenado regenerativo, la gestión de la batería y el control del motor.

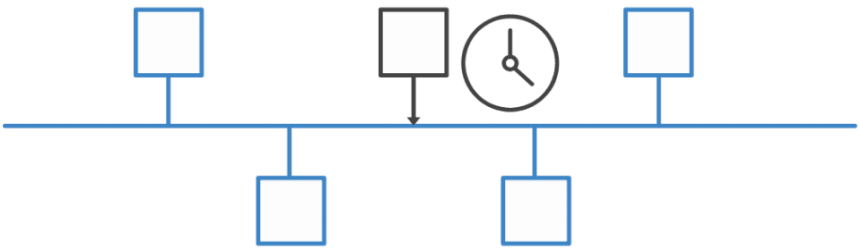
4. Funciones de diagnóstico y seguimiento: Con funciones integradas de diagnóstico y monitoreo, CANopen permite una detección de fallas y una resolución de problemas eficientes, lo que minimiza el tiempo de inactividad y mejora la confiabilidad del sistema.

5. Tipos de datos completos: CANopen admite una amplia gama de tipos de datos, incluidos números enteros, flotantes, cadenas, matrices y más. Esta versatilidad permite una representación eficiente de varios datos, lo que facilita el intercambio de información compleja entre los nodos de la red.



6. Direccionamiento de nodos: CANopen emplea identificadores de nodo únicos, que van del 1 al 127, que se utilizan para el direccionamiento de nodos. Esto permite la comunicación dirigida con dispositivos específicos dentro de la red, lo que permite un control y una coordinación precisos.

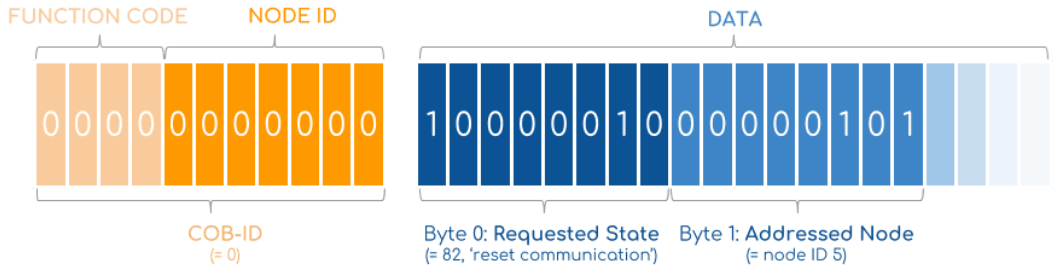
7. Sellado de tiempo: CANopen brinda la opción de mensajes con marca de tiempo, lo que permite que los dispositivos sincronicen sus relojes y mantengan referencias de tiempo precisas. Esta característica es especialmente valiosa en aplicaciones donde las mediciones de tiempo precisas son cruciales.



8. Protección de latidos y nodos: CANopen admite mecanismos de protección de latidos y nodos, que garantizan la presencia continua y el control del estado de los dispositivos en la red. Los mensajes de latido indican que un dispositivo está operativo, mientras que la protección de nodos detecta la ausencia de las comunicaciones esperadas, lo que permite una detección rápida de las fallas del dispositivo.

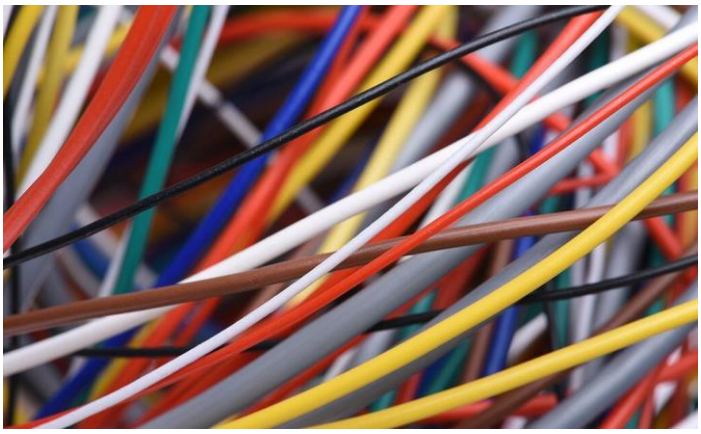
9. Gestión de red: CANopen ofrece varios servicios de gestión de red, como el direccionamiento dinámico de nodos, la configuración de nodos y la supervisión del estado de los dispositivos. Estos

servicios simplifican la gestión y el mantenimiento de la red, especialmente en aplicaciones donde se pueden agregar o quitar dispositivos durante la operación.



10. PDO (Objeto de datos de proceso) y SDO (Objeto de datos de servicio): CANopen define dos métodos de comunicación principales: PDO y SDO. Los PDO se utilizan para el intercambio de datos en tiempo real entre dispositivos, lo que permite una transmisión rápida y eficiente de información crítica. Los SDO, por otro lado, se utilizan para configurar y acceder a los parámetros y configuraciones del dispositivo, proporcionando un método estructurado para la configuración remota del dispositivo.

11. Complejidad de cableado reducida: La capacidad de CANopen para admitir la comunicación de múltiples dispositivos en un solo bus reduce significativamente la complejidad del cableado en los sistemas industriales. Con menos conexiones físicas requeridas, los esfuerzos de instalación y mantenimiento se agilizan, lo que genera ahorros de costos y mejora la confiabilidad. Esta ventaja es particularmente valiosa en aplicaciones donde las limitaciones de espacio y la gestión de cables son consideraciones críticas.

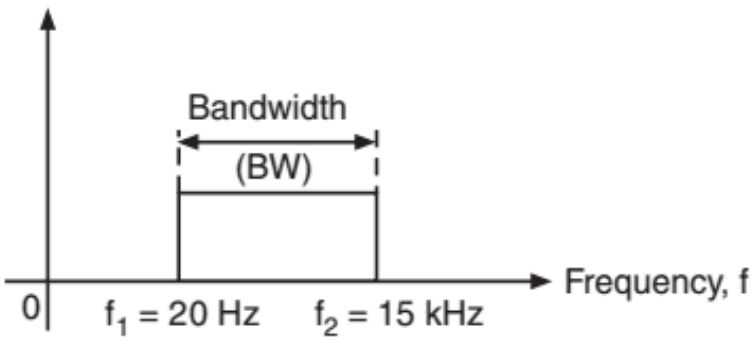


Desventajas

Si bien CANopen ofrece numerosas ventajas para la comunicación y la coordinación en varias aplicaciones, también presenta algunos inconvenientes que deben tenerse en cuenta al implementar el protocolo. Exploremos algunas de las desventajas clave de usar CANopen:

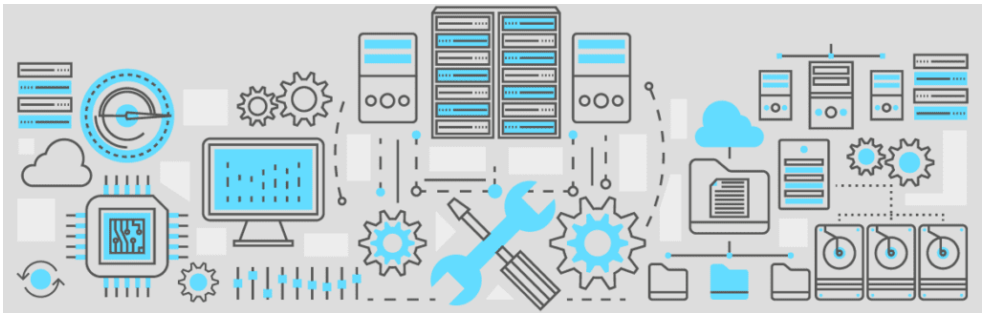
1. Complejidad de la implementación: La implementación de CANopen en un sistema puede ser una tarea compleja, especialmente para aquellos con experiencia o conocimientos limitados del protocolo. La configuración del diccionario de objetos, la configuración de PDO y SDO y la administración de parámetros de red requieren una planificación cuidadosa y una comprensión de las especificaciones del protocolo. Esta complejidad puede conducir a tiempos de desarrollo más prolongados y mayores costos de integración y mantenimiento.

2. Ancho de banda y velocidad de datos limitados: CANopen opera a través del bus CAN, que tiene un ancho de banda y una velocidad de datos limitados en comparación con otros protocolos de comunicación como Ethernet. Si bien CAN Bus es adecuado para muchas aplicaciones, puede convertirse en un cuello de botella para los sistemas que requieren un intercambio de datos de alta velocidad o grandes cantidades de datos. Esta limitación puede restringir el uso de CANopen en ciertas aplicaciones de alto rendimiento.



3. Falta de funciones de seguridad: CANopen carece de sólidas funciones de seguridad integradas. Como un protocolo más antiguo diseñado principalmente para aplicaciones industriales y de automatización, no ofrece mecanismos de seguridad avanzados para protegerse contra posibles amenazas cibernéticas o acceso no autorizado. A medida que las industrias se vuelven más interconectadas y enfrentan mayores riesgos de seguridad, es posible que sea necesario implementar medidas de seguridad adicionales junto con CANopen.

4. Problemas de compatibilidad con sistemas heredados: El uso extensivo de CANopen de perfiles de dispositivos estandarizados y diccionarios de objetos es ventajoso para la interoperabilidad entre dispositivos de diferentes fabricantes. Sin embargo, esto también puede generar problemas de compatibilidad cuando se integra con sistemas heredados que no cumplen completamente con el estándar. En tales casos, puede ser necesaria una configuración y adaptación adicionales para garantizar una comunicación fluida.

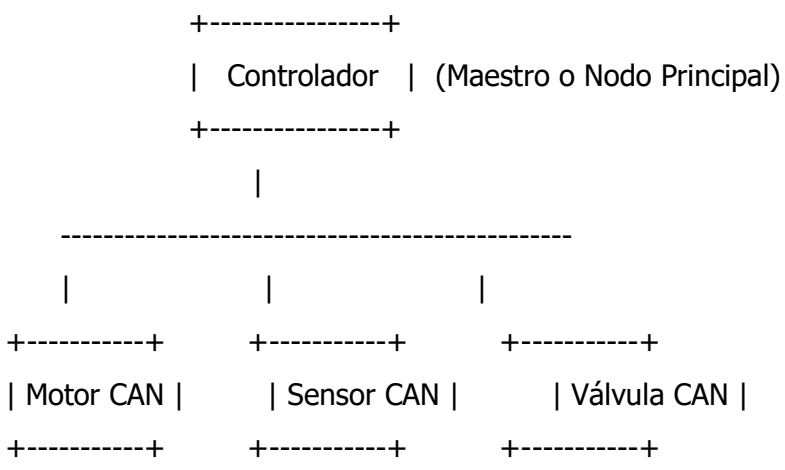


5. Tamaño de red limitado: Si bien CANopen es escalable hasta cierto punto, existe un límite práctico para la cantidad de nodos que se pueden conectar en una red. A medida que aumenta la cantidad de nodos, el tráfico de datos y la probabilidad de colisión pueden aumentar, lo que podría afectar la comunicación en tiempo real y el rendimiento general de la red. En escenarios que requieren una gran cantidad de nodos, los protocolos de comunicación alternativos pueden ser más adecuados.

6. Determinista pero no garantizado: CANopen proporciona un intercambio de datos determinista, lo que garantiza la entrega oportuna de mensajes críticos. Sin embargo, es importante tener en cuenta que CANopen no garantiza la entrega de mensajes ni los tiempos de respuesta en todos los escenarios. Las condiciones de la red, como el tráfico pesado de datos o los conflictos de arbitraje de bus, pueden provocar demoras ocasionales y afectar el rendimiento en tiempo real.

7. Rango de distancia limitada: CAN Bus, el sistema de comunicación subyacente de CANopen, tiene un rango de distancia limitado debido a su diseño para uso en sistemas de tamaño pequeño a mediano. Las distancias más largas entre nodos pueden requerir repetidores de señal adicionales u otros medios de amplificación de señal, lo que podría agregar complejidad y costo a la infraestructura de la red.

Diagrama simple de un sistema basado en CANopen



Comunicación CANopen sobre Red CAN

7. ¿Qué es un protocolo PROFIBUS-DP/PA?, ¿Para qué se usa? Ejemplifique.

¿Qué es el protocolo PROFIBUS-DP/PA?

PROFIBUS (Process Field Bus) es un estándar de comunicación industrial desarrollado en Alemania a finales de los años 80 por la asociación PROFIBUS Nutzerorganisation (PNO). Se diseñó para permitir una comunicación digital eficiente entre controladores (como PLCs) y dispositivos de campo (como sensores y actuadores).

Dentro de PROFIBUS existen varias variantes, entre ellas las más relevantes son:

- **PROFIBUS-DP (Decentralized Peripherals)**: orientado a la automatización de fábricas, conecta dispositivos periféricos distribuidos de forma eficiente y rápida a sistemas de control centralizados. Prioriza la velocidad de transmisión.
- **PROFIBUS-PA (Process Automation)**: desarrollado específicamente para aplicaciones de automatización de procesos industriales, donde se requiere comunicación confiable a largas distancias, seguridad intrínseca y alimentación de dispositivos a través del mismo cable de comunicación.

Diferencias clave:

Característica	PROFIBUS-DP	PROFIBUS-PA
Aplicación	Automatización de fábricas	Automatización de procesos
Velocidad	Hasta 12 Mbps	31.25 kbps
Cableado	RS-485 (cable estándar)	MBP (Manchester Bus Powered)
Alimentación	Separada	Integrada en el mismo bus
Seguridad intrínseca	No necesaria	Frecuentemente requerida

¿Para qué se usa PROFIBUS-DP/PA?

PROFIBUS-DP se utiliza principalmente para la **automatización de fábricas**, donde la velocidad y la cantidad de datos transmitidos son factores críticos. Ejemplos comunes incluyen líneas de ensamblaje de automóviles, fábricas de alimentos y manufactura de bienes electrónicos.

PROFIBUS-PA, en cambio, se aplica en **entornos de procesos** como plantas químicas, farmacéuticas, refinerías de petróleo y tratamiento de agua, donde la confiabilidad de la comunicación y la seguridad son esenciales. Su baja velocidad permite que la comunicación sea más robusta frente a interferencias y permite el uso de zonas peligrosas (atmósferas explosivas).

Aplicaciones prácticas

PROFIBUS-DP en una planta automotriz

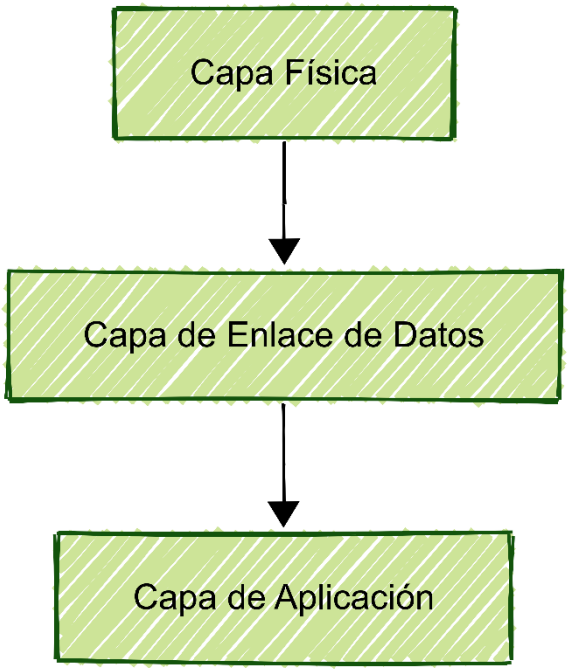
En una línea de ensamblaje de automóviles, múltiples robots de soldadura, transportadores, estaciones de prueba y controladores lógicos programables (PLC) necesitan comunicarse en tiempo real. PROFIBUS-DP conecta todos estos dispositivos, permitiendo el envío de comandos de control y la recolección de datos de operación en fracciones de segundo. Esto maximiza la eficiencia de producción y reduce el cableado al usar buses en lugar de conexiones punto a punto.

PROFIBUS-PA en una refinería de petróleo

En una refinería, se requieren mediciones precisas de temperatura, presión, flujo y nivel en áreas clasificadas como peligrosas debido a la presencia de gases inflamables. PROFIBUS-PA permite la conexión de instrumentos de campo con **alimentación a través del mismo bus** y, gracias a sus características de seguridad intrínseca, garantiza que las señales no representen un riesgo de ignición. Además, permite la configuración remota de instrumentos y la detección temprana de fallas.

Arquitectura

PROFIBUS sigue una arquitectura simplificada basada en el modelo OSI de 7 capas, pero implementa solo 3 capas principales:



Capa Física

Define los aspectos eléctricos y mecánicos del bus, como el tipo de cableado, conectores, niveles de voltaje, y métodos de modulación de señal.

- PROFIBUS-DP utiliza principalmente cables de par trenzado bajo la norma RS-485.
- PROFIBUS-PA usa MBP (Manchester Bus Powered), que permite comunicación y alimentación a través del mismo cable.

Capa de Enlace de Datos (DLL)

Controla el acceso al medio de comunicación y la detección de errores. Utiliza el protocolo **token passing** para la comunicación entre maestros y un esquema de **polling** para la comunicación maestro-esclavo.

Funciones principales:

- Manejo de la transmisión de datos confiable.
- Control de acceso al bus.
- Detección y corrección de errores de transmisión.

Capa de Aplicación

Define los servicios de comunicación específicos que permiten la configuración, monitoreo y control de dispositivos.

Dentro de esta capa se encuentran los perfiles de dispositivos, que aseguran que dispositivos de diferentes fabricantes puedan comunicarse siguiendo normas comunes.

Consideraciones prácticas para la implementación

Topologías de Red

PROFIBUS soporta diferentes topologías:

- Línea (bus).
- Estrella (mediante repetidores).
- Árbol (combinaciones de líneas y estrellas).

Tipos de Cables

- **PROFIBUS-DP**: par trenzado con resistencia característica de 150 Ohm.
- **PROFIBUS-PA**: cable específico para MBP con requisitos de seguridad intrínseca.

Conectores

- Conectores estándar DB9 o conectores específicos M12 para entornos industriales.

Configuración de Dispositivos

- **Maestro Clase 1**: Dispositivo que controla el bus (por ejemplo, un PLC).
- **Maestro Clase 2**: Dispositivo de programación y diagnóstico (por ejemplo, una laptop con software de configuración).
- **Esclavo**: Dispositivo de campo que responde a las solicitudes del maestro.

Cada dispositivo debe configurarse con una dirección única en el bus.

Diagnóstico y Mantenimiento

PROFIBUS permite la detección automática de fallas como:

- Pérdida de comunicación.
- Fallas de dispositivos.
- Errores de configuración.

Esto facilita el mantenimiento predictivo y la reducción de tiempos de parada.

Conclusión

PROFIBUS-DP/PA representa una solución robusta, eficiente y confiable para la comunicación en entornos industriales. Permite integrar dispositivos de múltiples fabricantes bajo un mismo estándar, facilita la automatización de procesos complejos y ofrece capacidades avanzadas de diagnóstico y mantenimiento. Entender su arquitectura, aplicaciones y aspectos de implementación es esencial para aprovechar todo su potencial en proyectos de automatización modernos.