

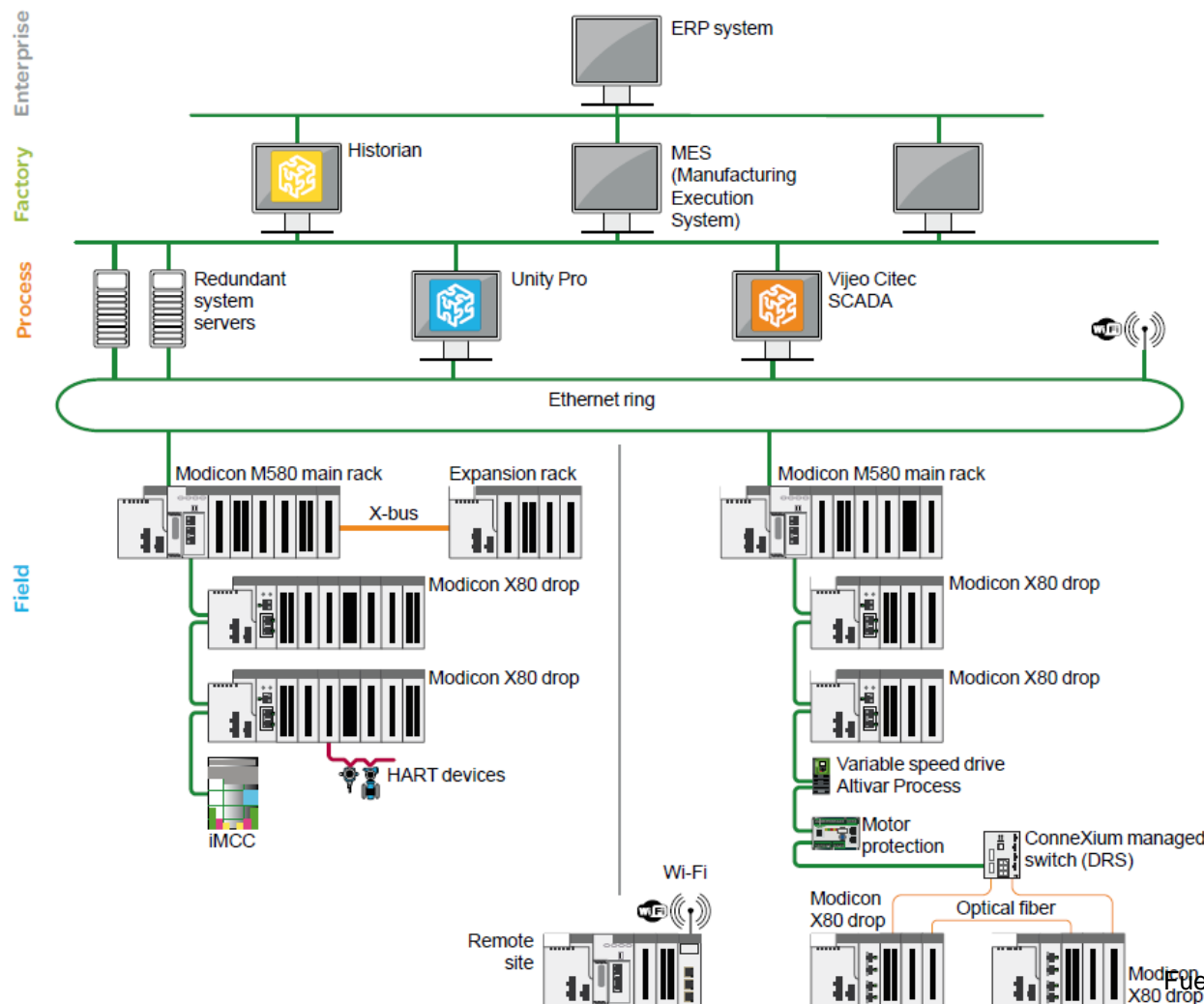
# ARQUITECTURAS Y TECNOLOGÍAS

## SEGURIDAD DE LOS SISTEMAS DE CONTROL

# ARQUITECTURAS Y TECNOLOGÍAS

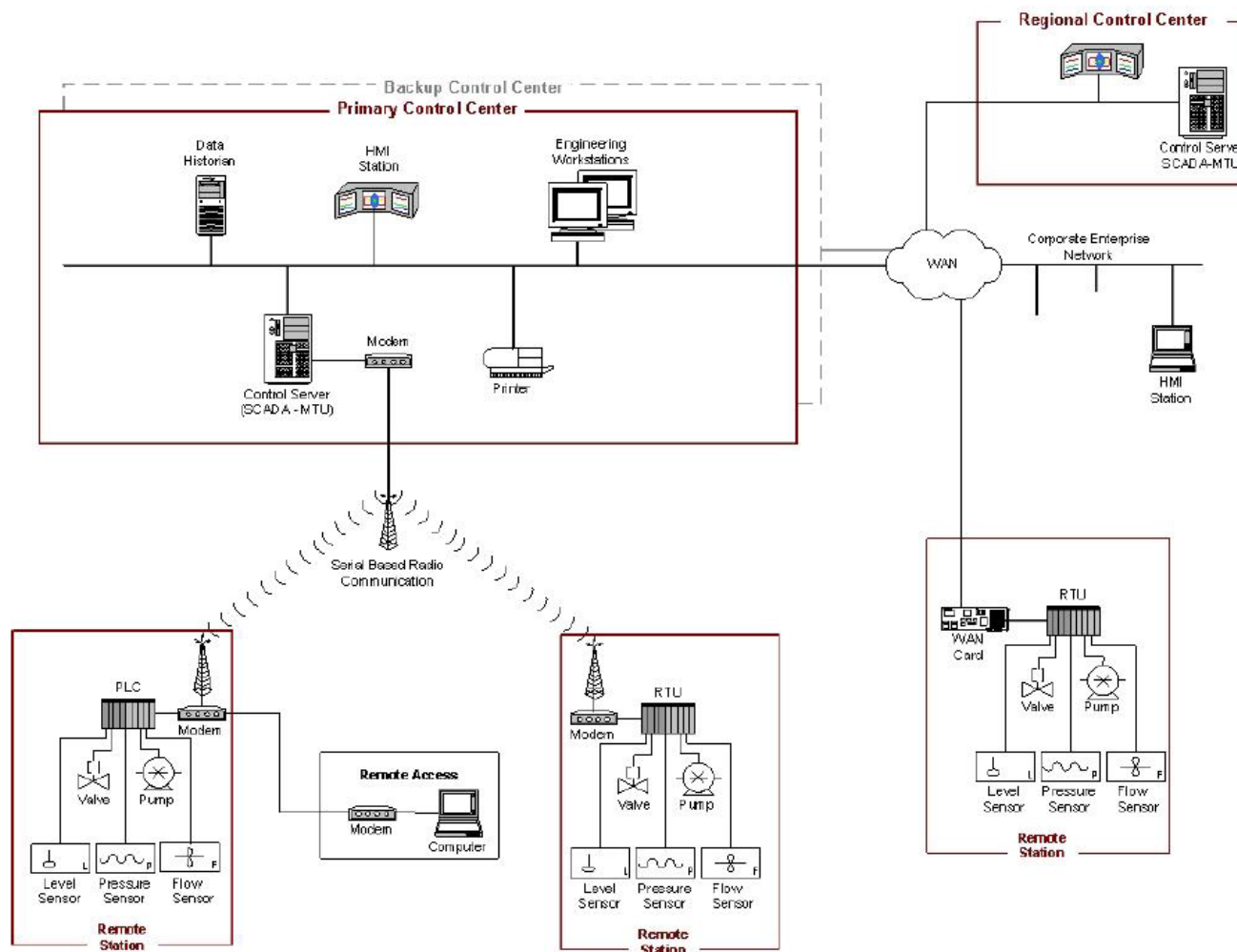
## Arquitectura tradicional

# ESTRUCTURAS TÍPICAS



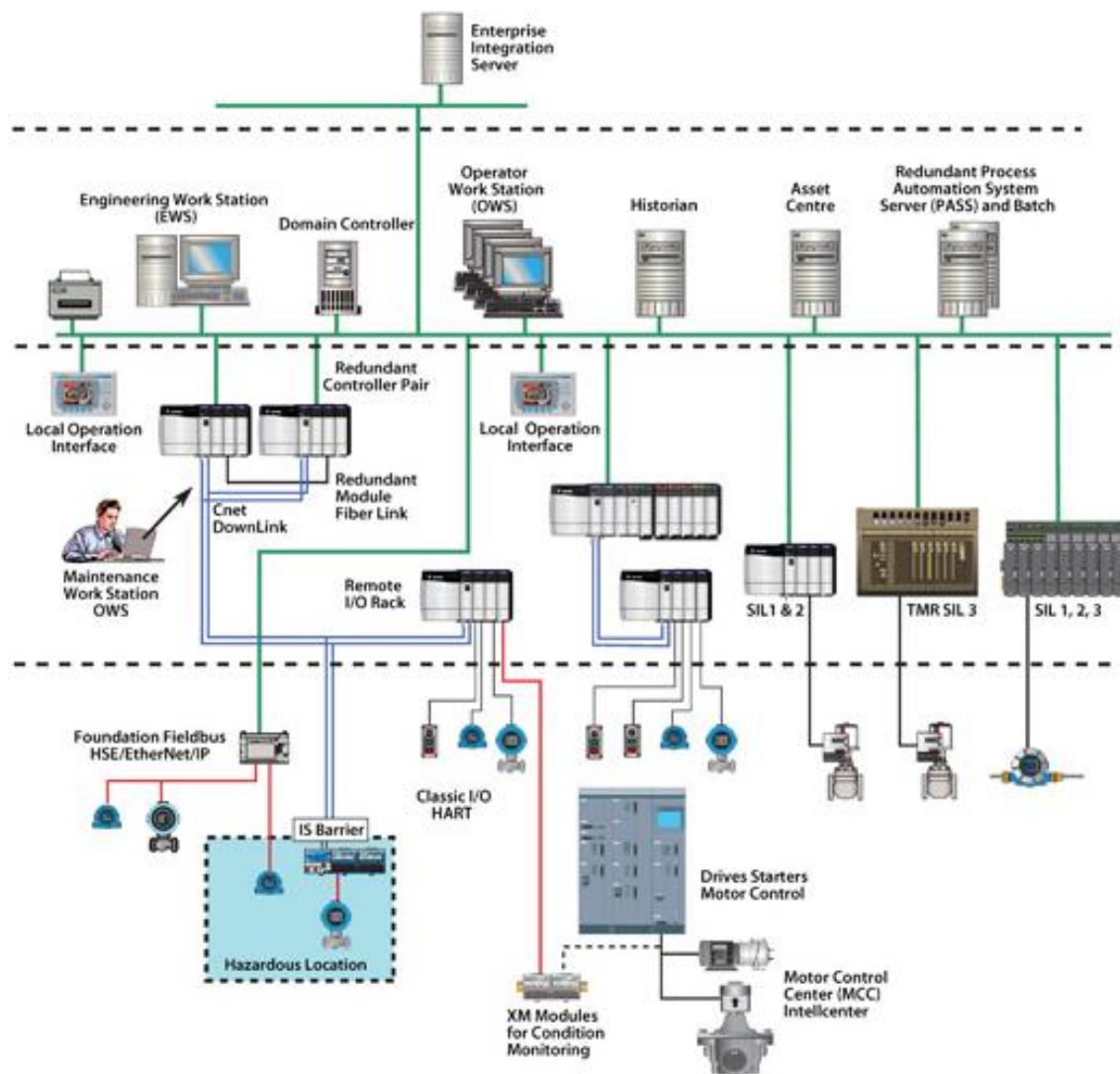
Fuente: Schneider Electric

# ESTRUCTURAS TÍPICAS

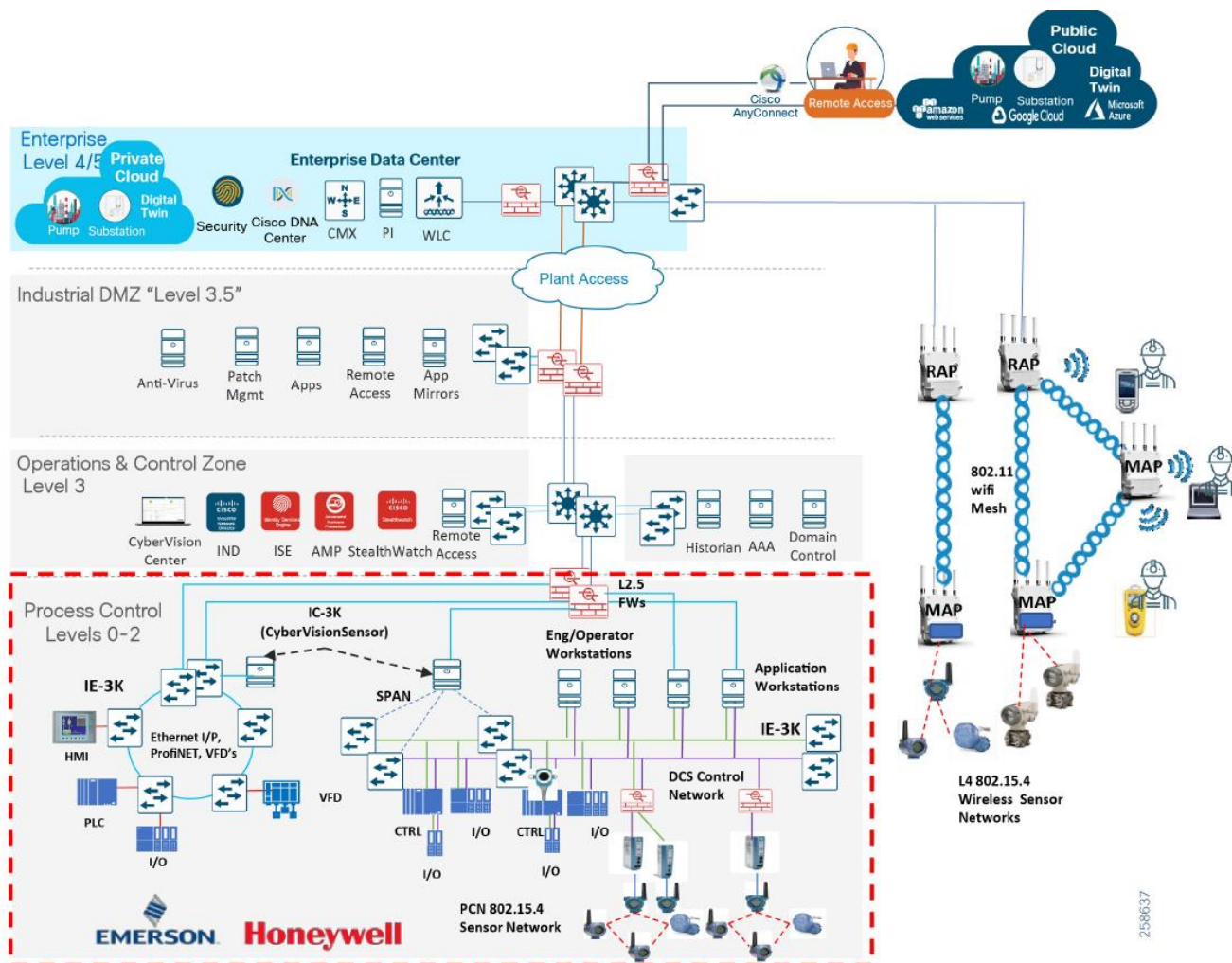


Fuente: Guide to Industrial Control Systems (ICS) Security, NIST

# ESTRUCTURAS TÍPICAS



# ESTRUCTURAS TÍPICAS



2558637

## ARQUITECTURAS Y TECNOLOGÍAS

# Industria 4.0 e IIoT (Internet industrial de las cosas)

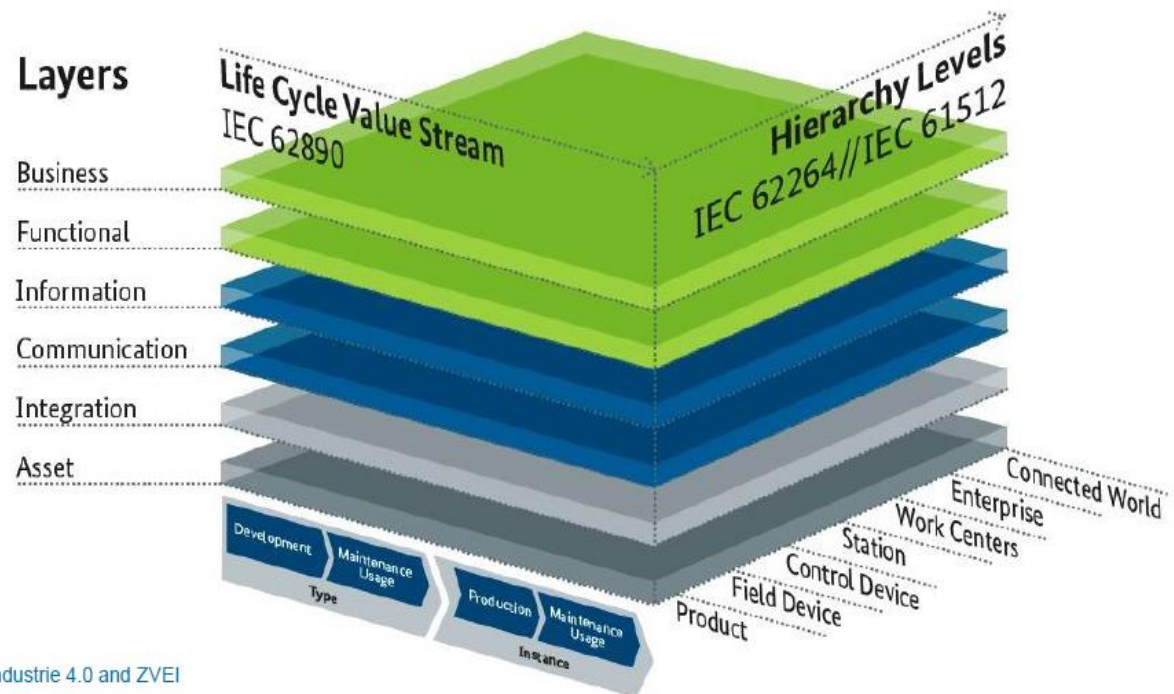
# INDUSTRIA 4.0 / IIOT

- **Industria 4.0, Industria Conectada, Internet Industrial de las Cosas, ...**
- **Enfoque centrado en los sistemas ciberfísicos**
- **El proceso de digitalización está replanteando la forma en que funciona un sistema de control industrial:**
  - Mayor conectividad
  - Mayor integración con los servicios IT
  - Aplicación de nuevas tecnologías habilitadoras como gemelos digitales, realidad aumentada, interfaces móviles, fabricación aditiva, robótica colaborativa, servicios web o servicios en la nube
  - Análisis de datos para mejorar el proceso y el producto
  - Mayor integración con proveedores y clientes



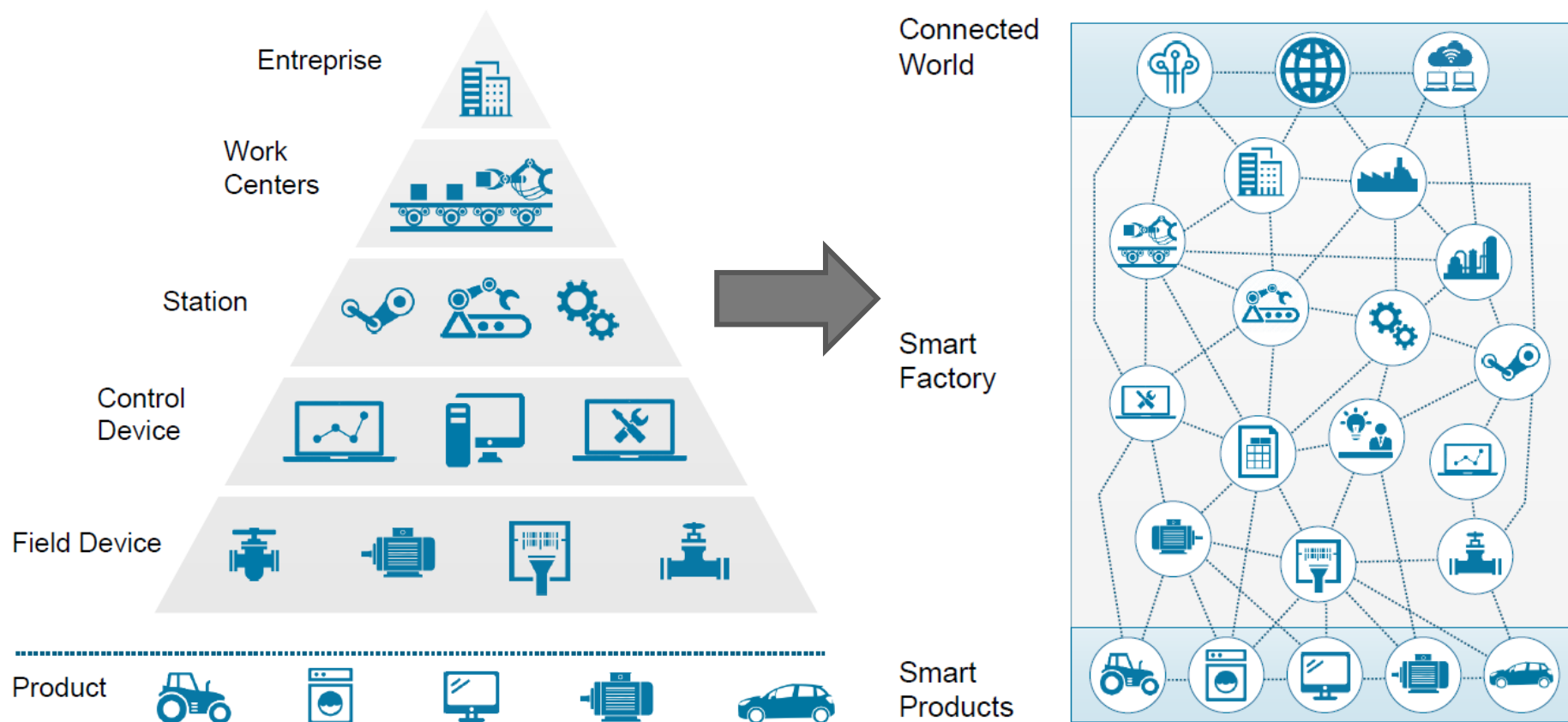
# INDUSTRIA 4.0 / IIOT

- **Modelo de referencia de arquitectura Industria 4.0 (RAMI)**
  - De un modelo jerárquico en el que la función está enlazada al hardware y el producto está aislado
  - A un sistema flexible con funciones distribuidas en la red, interacción entre niveles y en el que el producto es parte de la red



# INDUSTRIA 4.0 / IIOT

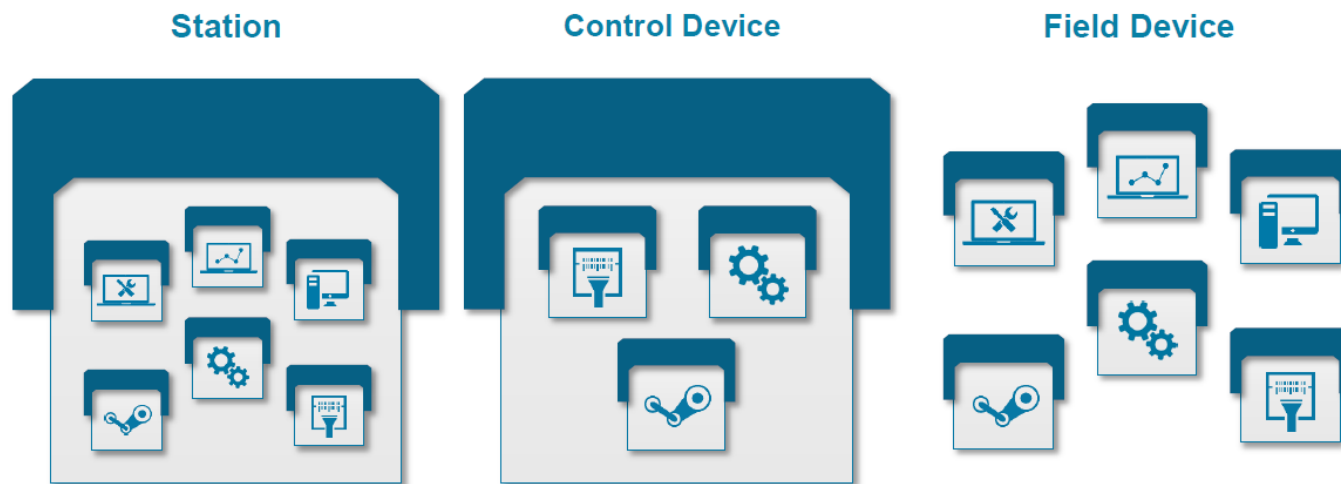
- Interconexión menos jerárquica, más compleja y flexible



Graphics © Anna Salari, designed by freepik

# INDUSTRIA 4.0 / IIOT

- “Capa de administración” como aquello que almacena toda la información sobre el activo y estandariza la comunicación



Graphics © Anna Salari, designed by freepik, Administration Shell © ZVEI SG Modelle und Standards

- Se continúa trabajando en modelos y marcos de actuación

# INDUSTRIA 4.0 / IIOT: CLOUD Y EDGE COMPUTING



- La tecnología *cloud* se está incorporando como una tecnología útil para:
  - Tareas de tratamiento de los datos
  - Supervisión
- **Modelos de nube pública, privada o híbrida**
  - Eficiencia y funcionalidad frente a dependencia de terceros, pérdida de la custodia de la información
  - Perímetro de seguridad más difuso
- **Diferentes modelos de distribución de la computación**
  - *Edge computing*: Elementos “concentradores” con tecnologías genéricas de comunicación como HTTPS, OPC UA, MQTT o CoAP

## ARQUITECTURAS Y TECNOLOGÍAS

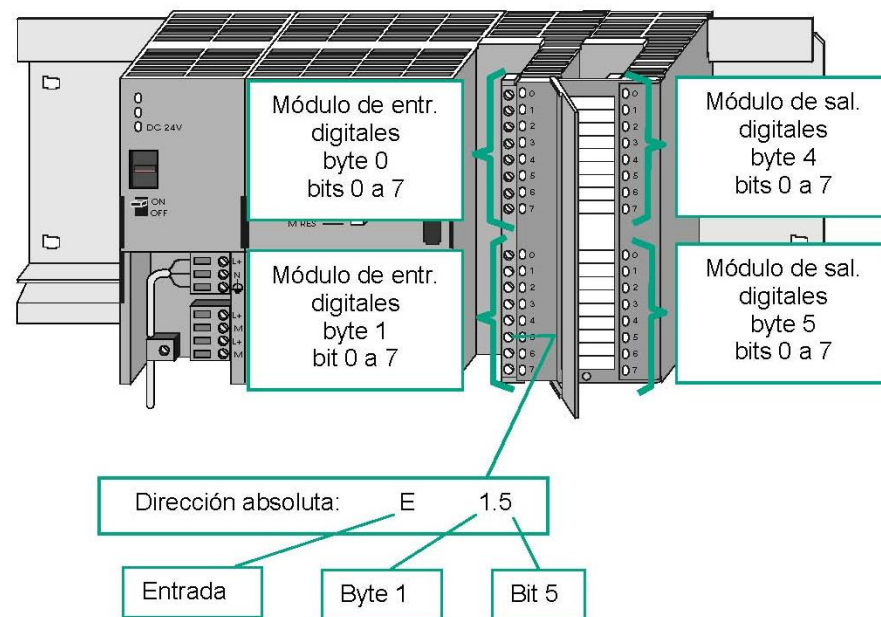
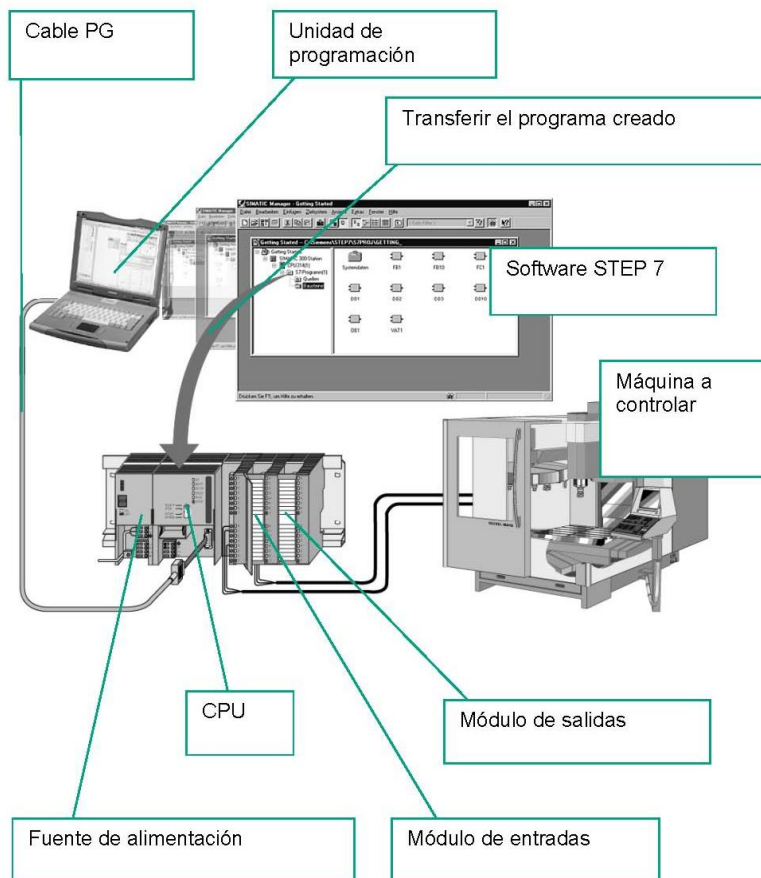
# Dispositivos de control industrial: estructura y programación

# DISPOSITIVOS DE CONTROL INDUSTRIAL

- **Gama cada vez más continua de posibilidades:**
  - Autómata programable (PLC), sistema de control distribuido (DCS), microautómata, unidad terminal remota (RTU), dispositivo electrónico inteligente (IED), computador industrial, ...
- **Los dispositivos utilizados en este ámbito presentan una mayor heterogeneidad que los computadores de propósito general**
  - **Procesador:** ARM, MIPS, PPC, 8086, AVR, V850, 68K, ...
  - **Sistemas operativos (generalmente de tiempo real):** VxWorks, ThreadX, QNX, FreeRTOS, MQX, Nucleus, distribuciones BSD/Linux, ...

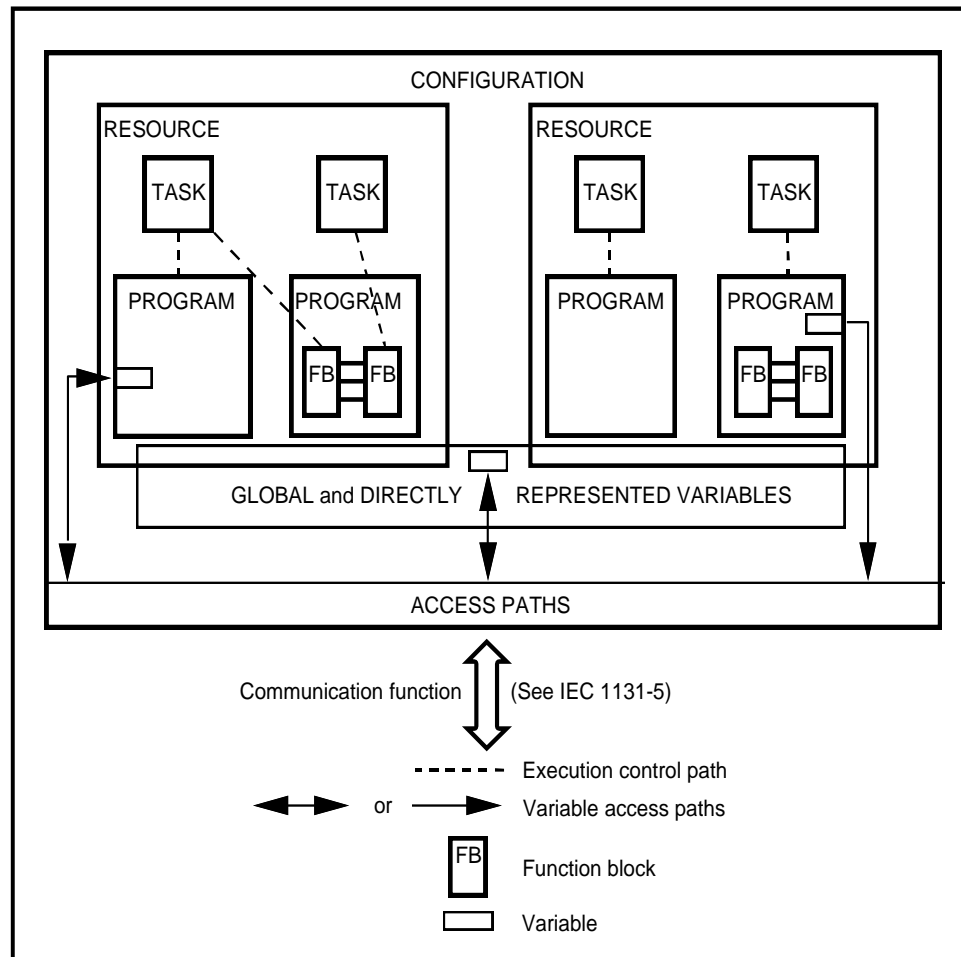
# AUTÓMATAS PROGRAMABLES: ESTRUCTURA

- A nivel de hardware



# AUTÓMATAS PROGRAMABLES: ESTRUCTURA

- Modelo de software de un autómata programable: IEC 61131-3



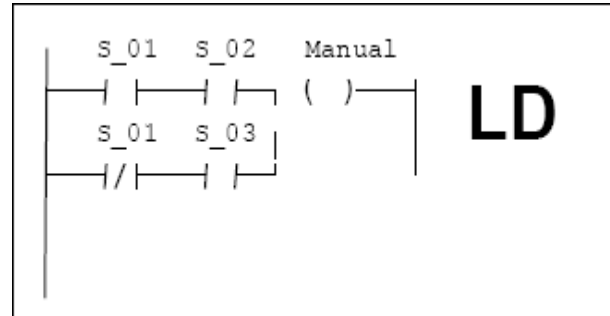


# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

- **Programación mediante los lenguajes definidos en el IEC 61131-3**
  - Dos lenguajes textuales
    - Lista de instrucciones (IL)
    - Texto Estructurado (ST)
  - Dos lenguajes gráficos
    - Lenguaje de contactos o *Ladder Diagram* (LD)
    - Diagrama de funciones (FBD)
  - Un metalenguaje gráfico
    - Diagrama funcional de secuencias (SFC)

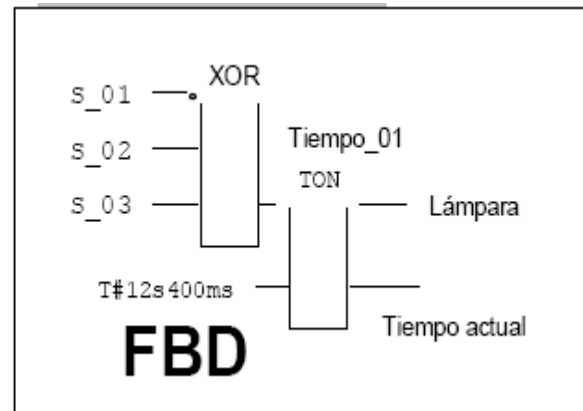
# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

- **LD (Esquema de contactos):**
  - Basado en los esquemas eléctricos de control clásicos
  - Orientado a realizar operaciones lógicas
  - Fácil para personal sin cualificación



# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

- **FBD (Diagrama de funciones):**
  - Similar a los diagramas empleados por los ingenieros electrónicos para representar los circuitos lógicos
  - Más flexible que el LD



# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

- **IL (Lista de instrucciones):**
  - Antiguo
  - De bajo nivel, tipo ensamblador
  - Base a la que podrían traducirse todos los demás lenguajes

**IL**  
LD Entrada\_Manual  
OR Entrada\_Automática  
AND Desbloqueo  
ST Funcionamiento  
  
LD Entrada\_01

# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

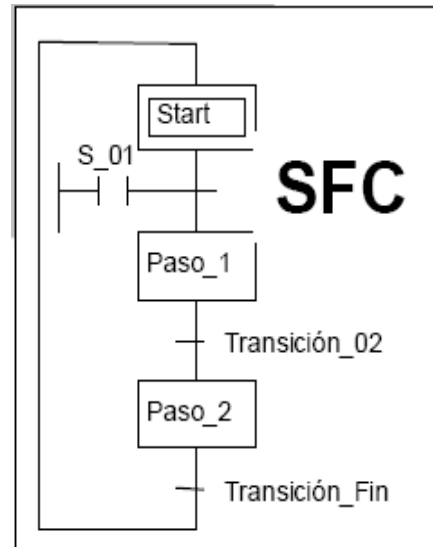
- **ST (Texto estructurado)**
  - Lenguaje literal de alto nivel
  - Más flexible y potente especialmente indicado para la representación de algoritmos de control complejos

```
IF Data = "EOF" THEN
  FOR Index:=1 TO 128 DO
    X:=Read_Data(Datenfeld[Index]);
    IF X > 2500 THEN Alarma:=TRUE;
    END IF;
  END FOR;
END_IF;
```

**ST**

# AUTÓMATAS PROGRAMABLES: PROGRAMACIÓN

- **SFC (Diagrama funcional de secuencias)**
  - Lenguaje de modelado de sistemas secuenciales
  - Define etapas y transiciones
  - Cada etapa realiza unas acciones programadas en cualquier de los otros lenguajes
  - Las transiciones dependen de unas determinadas condiciones



# AUTÓMATAS PROGRAMABLES: CARACTERÍSTICAS DE SEGURIDAD

- **La mayoría de PLC y DCS permiten contraseña de protección del programa**
  - Funciona en conjunción con el software de programación
  - Es un parámetro más en la configuración, que en muchas ocasiones ha demostrado ser fácilmente evitable
- **A menudo, disponen de servicios web o FTP**
  - Para labores de monitorización, configuración y mantenimiento
  - Estos servicios pueden estar accesibles sin contraseña, o con una protección débil o son difícilmente bloqueables o actualizables

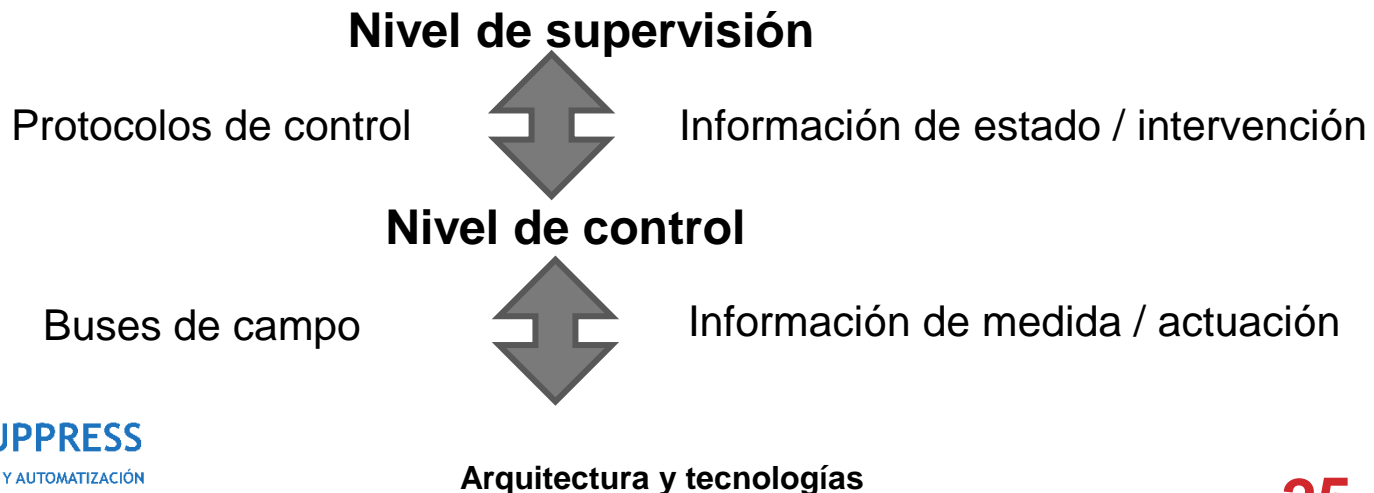
# AUTÓMATAS PROGRAMABLES: CARACTERÍSTICAS DE SEGURIDAD

- **A veces, se incluye protección física contra la sobreescritura del programa**
  - Algunos PLCs permiten grabar el programa en memorias de sólo lectura
- **Algunos PLCs y RTUs modernos ya incorporan firewalls**
  - limitando las comunicaciones a través de listas de control de acceso
  - Las opciones más modernas permiten realizar túneles VPN



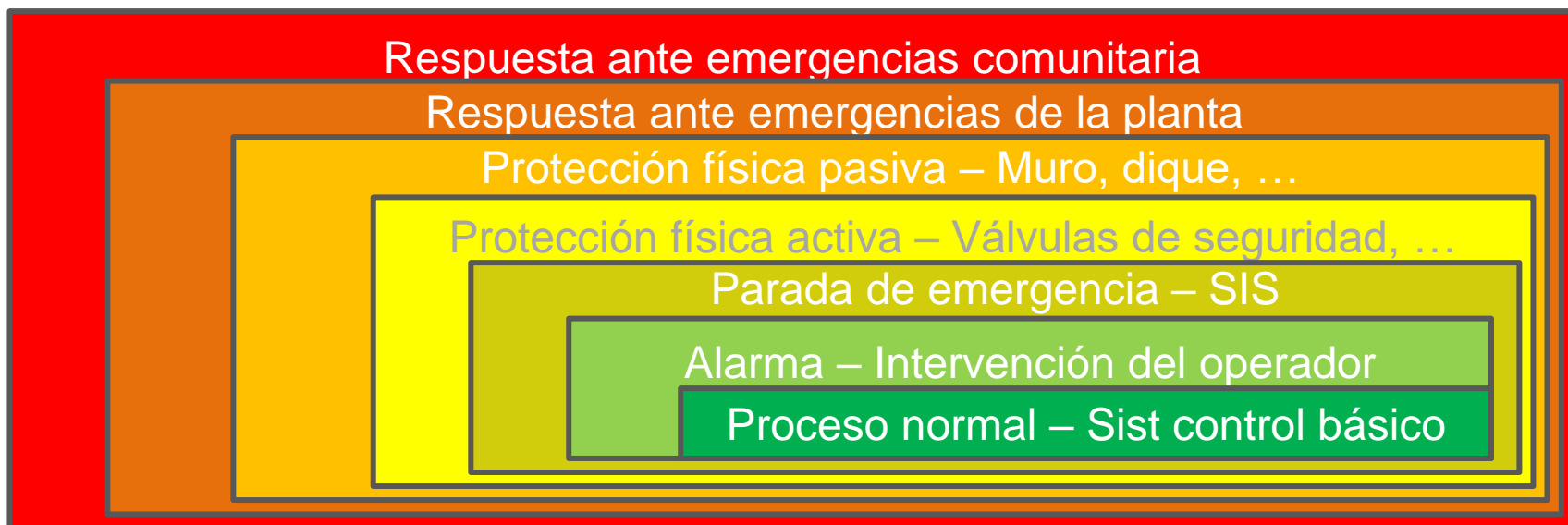
# AUTÓMATAS PROGRAMABLES: COMUNICACIÓN

- **Comunicaciones con el puesto de ingeniería durante su programación, configuración y mantenimiento**
  - A través de herramientas propietarias
  - Protocolos propietarios o extensiones propietarias de protocolos estándares
  - Antes por serie, ahora por Ethernet y TCP/IP
- **Comunicaciones durante la ejecución del programa**



# SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS)

- También conocidos como Sistemas de Parada de Emergencia o Sistemas de Enclavamientos
- Capa de seguridad operacional
- Controla que determinados límites de operación no son violados y, en caso de serlo, para evitar situaciones peligrosas, lleva al proceso a un estado seguro de parada de emergencia



# SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS)

- El estado seguro debe alcanzarse en un tiempo adecuado
- Sistemas más sofisticados pero similares a los PLCs, necesitan instrumentación
- La reprogramación del SIS no se suele permitir en modo de operación



# SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS)

- Puesto que el SIS se antepone al sistema de control básico, sería también de extrema gravedad que fuese comprometido
- Si estos sistemas no funcionasen adecuadamente, se producirían daños
  - Se debe garantizar que no sean vulnerables a ataques de denegación de servicio
- **Por ello, es necesario:**
  - Aislar lo más posible estos sistemas de otros activos del sistema de control, así como eliminar las posibles amenazas
  - Revisarlos periódicamente para garantizar su operatividad
  - Se debería aprovechar también para revisar también su ciberseguridad y aplicar parches

# ARQUITECTURA Y TECNOLOGÍAS

## Comunicaciones

# PROTOCOLOS DE CONFIGURACIÓN

- **Generalmente se usan protocolos propietarios o extensiones propietarias de los protocolos abiertos para:**
  - La programación y parametrización de los dispositivos
- **Inicialmente mediante bus serie, en la actualidad mediante protocolos sobre TCP/IP**
- **Ejemplos:**
  - UMAS (Schneider Electric): Código de función 90 de Modbus TCP
  - S7Comm (Siemens): Protocolo propietario
- **El desconocimiento de la estructura y contenido de los mensajes puede suponer una vulnerabilidad importante**
- **Se comienza a incorporar capacidad de filtrado de estos protocolos en los firewalls, pero solamente de forma limitada**

# FAMILIAS DE REDES DE COMUNICACIÓN INDUSTRIAL

- **MODBUS:**
  - RTU
  - TCP
- **CIP (Protocolo Industrial Común):**
  - DeviceNet, ControlNet
  - Ethernet/IP
- **PROFIBUS:**
  - DP, PA, FMS
  - PROFINET
- **Foundation Fieldbus:**
  - H1
  - HSE

# BUSES DE CAMPO

- Generalmente son del tipo petición-respuesta, con estructuras maestro-esclavo o cliente-servidor
- Serie, habitualmente RS485
- No implementan cifrado ni autenticación
- Protocolos de interés en el ámbito industrial:
  - MODBUS RTU
  - CIP DEVICENET (Y CONTROLNET)
  - PROFIBUS
  - FIELDBUS H1
  - AS-I
  - OTROS





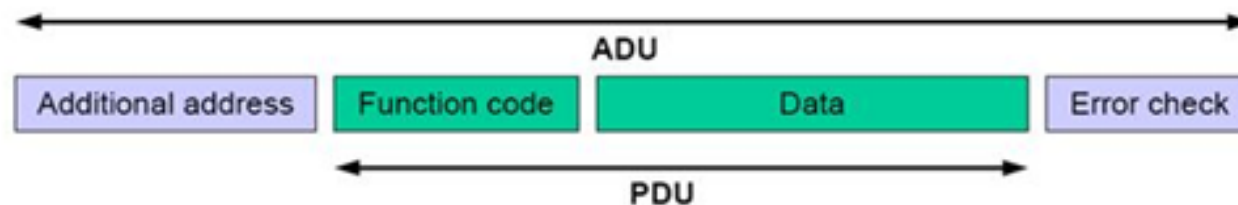
# BUSES DE CAMPO: MODBUS RTU



- **Desarrollado por Modicon (Schneider)**
- **Comunicación maestro-esclavo.**
  - El maestro (único) realiza una consulta al esclavo, que devuelve el código de acción enviado, los datos recopilados y el estado
- **Muy simple**
- **Sobre RS-232 (punto a punto) y RS-485**

# BUSES DE CAMPO: MODBUS RTU

- Cada trama contiene una sección de inicio, otra de dirección (1 byte), otra de función (1 byte), datos (n bytes) y verificación de redundancia
  - Funciones de lectura, actualización, diagnóstico, carga, ...
- **Dos tipos de tramas**
  - PDU (Unidad de datos de protocolo), que contiene un código de función seguido de datos
  - ADU (Unidad de datos de aplicación), que incluyen dirección, código de función, datos y comprobación de errores



# BUSES DE CAMPO: CIP

- Estándar flexible basado en objetos
- Perfiles de dispositivos: Para cada uno, objetos requeridos, opciones de configuración y formatos de E/S
- Modelo productor/consumidor
- Sobre diferentes medios físicos
- Tipos de mensajes:
  - **Implícitos:** Lecturas escrituras cíclicas o de cambio de estado
  - **Explícitos:** Información del protocolo o petición de servicios

Capa de  
aplicación

Perfiles ( <i>Control de motores, Transductores, E/S, Safety, ...</i> )
Objetos (comunicaciones, aplicaciones, sincronización, safety)
Servicios de gestión de datos
Gestión de la conexión y enrutado

# BUSES DE CAMPO: CIP

- **DeviceNet**

- CIP sobre bus CAN, Muy utilizado
- Basado en diálogo productor-consumidor

- **ControlNet**

- CIP sobre red dedicada
- Elevada velocidad de transferencia, determinismo y repetibilidad
- Para sustituir muchas E/S cableadas o como eje central de varias redes DeviceNet

# BUSES DE CAMPO: PROFIBUS



- ***Process Fieldbus***, familia de protocolos creada por el gobierno alemán
- Orientada a procesos de fabricación
- Rápido, buena inmunidad frente a ruido
- Muy utilizado
- Tres niveles de servicio: intercambio cíclico de datos y diagnósticos, acíclico de datos y alarmas y broadcast/por intervalos

# BUSES DE CAMPO: PROFIBUS

- **DP (Decentralized Periphery)**
  - El más común
  - Maestro-esclavo. Generalmente monomaestro. Los maestros hacen *polling* cíclicamente a los esclavos (individualmente, a varios o todos)
  - Intercambio de datos automático según la configuración inicial
- **PA (Process Automation)**
  - Variante de PROFIBUS DP con seguridad intrínseca para atmósferas explosivas
- **FMS (Fieldbus Message Specification)**
  - Acíclico, para transmitir grandes cantidades de datos entre autómatas

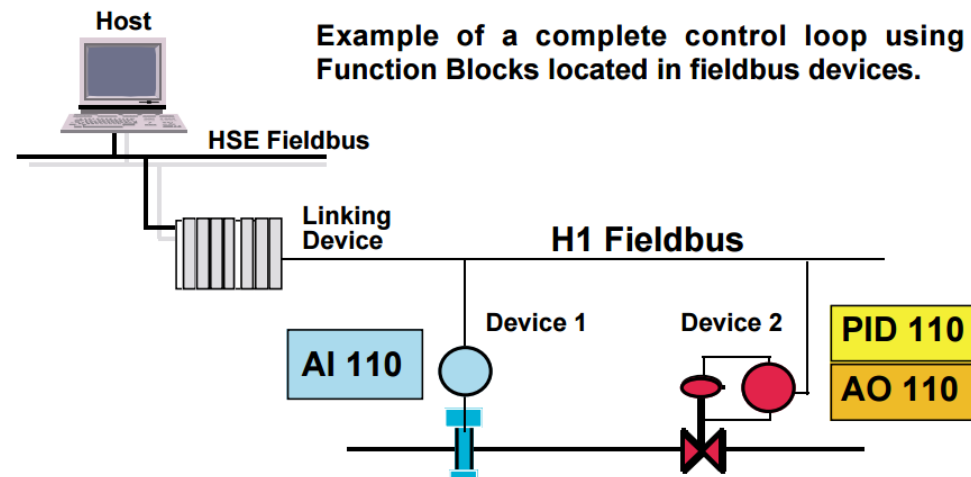
# BUSES DE CAMPO: FOUNDATION FIELDBUS H1

- Estándar ligeramente más moderno
- Orientado a soportar aplicaciones críticas donde la transferencia y manejo de información son esenciales
  - Sector petroquímico
- Interoperabilidad entre instrumentos de campo y sistemas de múltiples proveedores
  - Sin necesidad de pasarelas
- Soporte de redundancia
- Comunicación productor/consumidor (adquisición continua), cliente/servidor (puntual) y de distribución de informes (alarmas)



# BUSES DE CAMPO: FOUNDATION FIELDBUS H1

- **Gran interactividad con elementos de campo:**
  - configurar parámetros, modificar rangos y realizar calibraciones
  - configurar lazos de control sin un equipo de control externo



Fuente: Foundation Fieldbus Technical Overview



# BUSES DE CAMPO: OTROS

- **AS-i (interfaz actuador sensor)**

- De bajo nivel y funcionalidad limitada
- Cableado mínimo y flexible: dos hilos para transmitir alimentación y datos
- Fácil configuración, la realiza el maestro de forma transparente
- *Polling* cíclico
- Tablas de usuario, configuración y estado

- **CANOpen**

- Usa el bus CAN
- Trabaja en broadcast, carece de maestro
- Orientado a mensajes, con identificadores y prioridades
- Intercambio de información en forma de objetos de comunicación COB: de proceso, de datos, de funciones especiales y de gestión de red
- Datos reconocidos y validados por todos los nodos o rechazados
- Control embebido

# BUSES DE CAMPO: OTROS

- **EtherCAT**

- Sobre Ethernet pero no se basa en TCP/IP
- Mensaje de maestro con datos para todos los nodos esclavos. Cada nodo lee y añade datos
- Rápido y simple
- Tiempo real
- Susceptible a ataques DoS o MitM

- **Interbus**

- Phoenix Contact
- Para aplicaciones estándar con E/S distribuidas
- Maestro se comporta como una tarjeta de E/S del propio PLC

- **CC-Link**

- Mitsubishi
- Usado en Asia

# PROTOCOLOS DE COMUNICACIÓN INDUSTRIAL A NIVEL DE CONTROL

- **Sobre TCP/IP, a menudo un simple encapsulado del bus de campo de la misma familia**
- **Tampoco tienen mecanismos de seguridad**
- **Protocolos relevantes en el ámbito industrial**
  - MODBUS TCP
  - CIP ETHERNET/IP
  - PROFINET
  - FIELDBUS HSE

# MODBUS TCP

- Tramas encapsuladas sobre TCP/IP
- Se usa el protocolo TCP en la capa de transporte, estableciéndose conexiones entre cliente y servidor
- El servidor (esclavo) escucha en el puerto 502
- Comunicación punto a punto (unicast)
- Simple y ampliamente soportado

# MODBUS: TIPOS DE DATOS Y CÓDIGOS DE FUNCIÓN

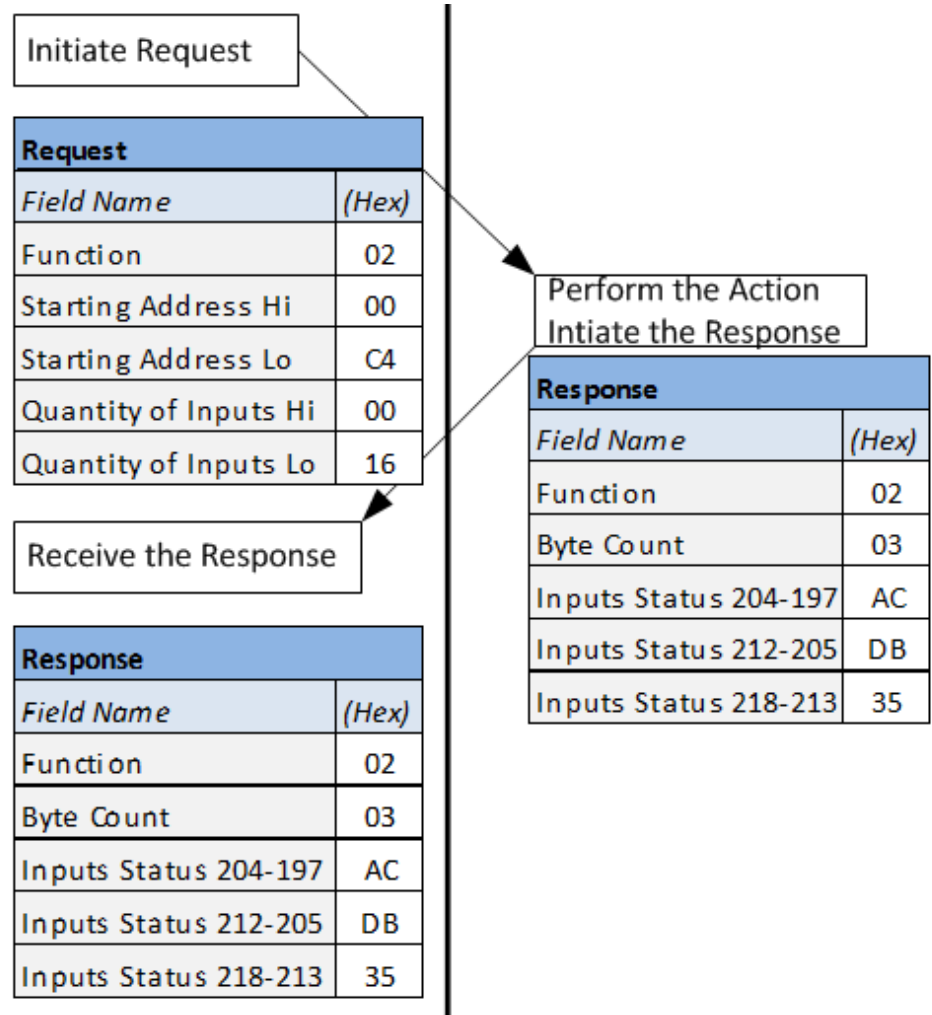
- **Entradas digitales (*discrete inputs*):**  
1 bit, sólo lectura
- **Salidas digitales (*coils*):**  
1 bit, lectura/escritura
- **Registros de entrada (*input registers*):**  
16 bits, sólo lectura
- **Registros de salida (*holding registers*):**  
16 bits, lectura/escritura

Códigos de función				
Acceso a datos	1 bit	Entradas digitales	Read Discrete Inputs	02
		Salidas digitales (Coils)	Read Coils	01
			Write Single Coil	05
			Write Multiple Coils	0F
	16 bits	Registros de entrada	Read Input Register	04
		Registros de Salida	Read Holding Registers	03
			Write Single Register	06
			Write Multiple Registers	10
			Read/Write Multiple Registers	17
			Write Mask Register	16
			Read FIFO Queue	18
			Ficheros	Read File Record
	Write File Record	15		
Diagnóstico		Read Exception Status	07	
		Diagnostics	08	
		Get Comm Event Counter	0B	
		Get Comm Event Log	0C	
		Report Slave ID	11	
		Read Device Identification	2B	
Otros		Encapsulated Interface Transport	2B	

# MODBUS: EJEMPLO DE PETICIÓN DE LECTURA

- El maestro solicita un conjunto de datos correspondientes a entradas discretas (función 0x02). La dirección de inicio es 0xC4 y el número de direcciones solicitadas es 16.
- El esclavo recibe la petición y procede a responder con 3 bytes cuyos valores son 0xAC, DB y 35.
- El maestro recibe los datos procedentes del esclavo.

Esclavo



# MODBUS: SEGURIDAD

- **Varios problemas:**
  - Ausencia de autenticación:
    - Solamente se necesita utilizar direcciones, códigos de función y datos válidos que podrían fácilmente extraerse de un análisis del tráfico
    - No se verifica que el mensaje provenga de un dispositivo legítimo, por lo que ataques *man-in-the-middle* (MitM) o *replay* simples son posibles
  - Ausencia de cifrado: Los comandos y direcciones se transmiten en texto plano por lo que las capturas de tráfico pueden relevar información significativa acerca de la configuración del sistema y de sus dispositivos
  - Ausencia de *checksums* a nivel de aplicación: No se puede verificar la integridad del mensaje

# CIP: ETHERNET/IP

- **CIP sobre TCP/IP**
- **Mensajes implícitos**
  - Más críticos, comunicaciones en tiempo real)
  - Peticiones en TCP, respuestas en UDP (puerto 2222) en multicast, generalmente
- **Mensajes explícitos**
  - Petición/respuesta
  - En TCP (puerto 44818)
- **Supervisión y comunicación entre elementos de control**
- **Tres tipos de objetos: requeridos (identificación del dispositivo, de direccionamiento, etc.), de aplicación y específicos del fabricante**



# CIP: ETHERNET/IP

- **Tampoco o cuenta con ningún mecanismo implícito ni explícito de seguridad**
- **Adicionalmente:**
  - La utilización de los objetos requeridos para la identificación del dispositivo puede facilitar la enumeración de los mismos
  - El uso de UDP y tráfico Multicast para transmisión en tiempo real puede facilitar la inyección de tráfico

# PROFINET

- *Process Field Network*
- Desarrollado por Siemens para complementar PROFIBUS
- Acceso a dispositivos PROFIBUS mediante pasarela
- Orientado a objetos, productor-consumidor
- UDP para comunicación acíclica
- Escalable, se puede adaptar al grado de determinismo y rendimiento que se requiera
- Modular, con diferentes subprotocolos
  - IO (comunicación con periféricas), CBA (automatización distribuida), DCP (descubrimiento y configuración básica), MRP y MRRT (redundancia),...

# PROFINET

- **Perfiles**
  - Profisafe (para seguridad operacional), Profienergy (gestión energética)
- **De hecho, es posible realizar comunicación cíclica de tiempo real**
  - Sin tiempo real: Sobre TCP/IP, para comunicaciones en el rango de 100ms, enrutable
  - Tiempo real (RT): Directamente sobre Ethernet, haciendo uso de métodos estándares para priorizar tráfico como tagging de VLANs, en rangos de 10ms
  - Tiempo real isócrono (IRT): con tiempos incluso menores de 1ms, modificaciones más profundas de Ethernet como la planificación estricta de la comunicación o la sincronización de alta precisión
- **Es posible comunicar datos de diagnóstico sobre SNMP**
- **No cuenta con medidas de seguridad**

# FOUNDATION FIELDBUS HSE

- *High Speed Ethernet*
- Para transmisión de datos a gran escala (de autómatas, por ejemplo) y la integración de sistemas
- Encapsula la trama de H1 sobre TCP/IP
- Dispositivos de enlace (con redes H1), Ethernet, de pasarela (interfaz con otros protocolos) o de host (sobre estación de trabajo de operador)

# ESTÁNDAR OPC

- En sistemas complejos, la comunicación con cada dispositivo podría requerir interfaces diferentes
- Necesidad de estandarización

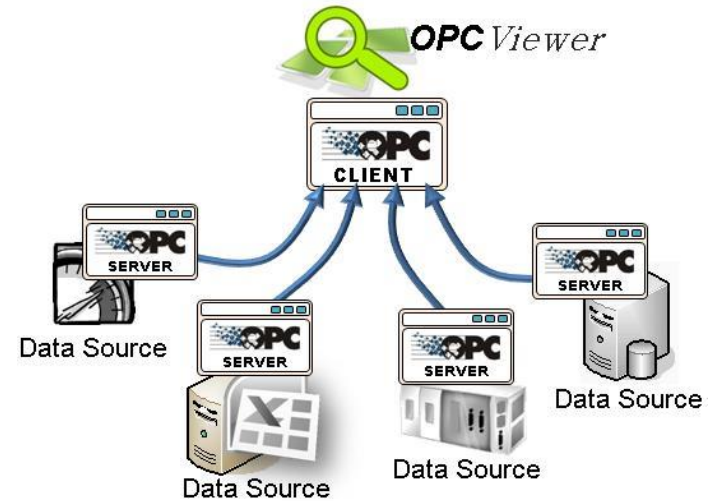


- OPC (OLE for Process Control): Estándar de comunicación
- Arquitectura cliente-servidor
- Permite que el cliente OPC utilice un interface estándar
- El servidor OPC proporciona la traducción desde este estándar a los drivers específicos de los autómatas
- Prácticamente todos los fabricantes proporcionan servidores OPC para sus PLCs



# ESTÁNDAR OPC

- **Cliente OPC:**
  - Software que utiliza el estándar OPC para controlar/supervisar un dispositivo
  - Realiza peticiones de lectura/escritura a un/os servidor/es OPC locales o remotos
  - Habitualmente disponible en SCADAs
- **Servidor OPC:**
  - Software que se ejecuta en un computador
  - Realiza la traducción al dispositivo
  - Fuente de datos

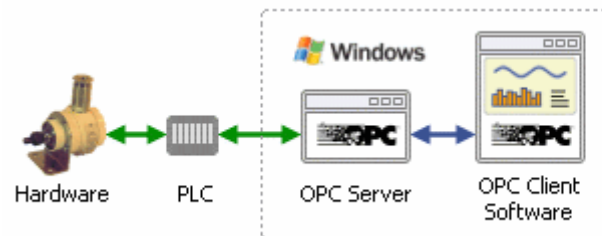


Fuente: [www.commsvr.com](http://www.commsvr.com)

- El cliente OPC pide al servidor que cree grupos OPC, que son objetos temporales que incluyen ítems, que hacen disponibles las variables. El cliente OPC del SCADA recreará los objetos en cada ejecución de acuerdo a su configuración
- Todos los datos ofrecidos por el servidor OPC están accesibles para cualquier cliente que pueda conectarse

# ESTÁNDAR OPC CLÁSICO

- **Inicialmente basado en tecnología Microsoft:**
  - *Object Linking and Embedding*
  - DCOM (*Distributed Component Object Model*):
    - Tecnología ya obsoleta de componentes distribuidos en diversos computadores
    - *Remote procedure calls*
    - Comienza la sesión en un puerto y después lo transfiere a otro
- **Diversas especificaciones centradas en los tipos de datos a intercambiar o los protocolos de comunicación**
- **El más aceptado por la industria ha sido OPC-DA (*Data Access*)**



# OPC CLÁSICO: SEGURIDAD

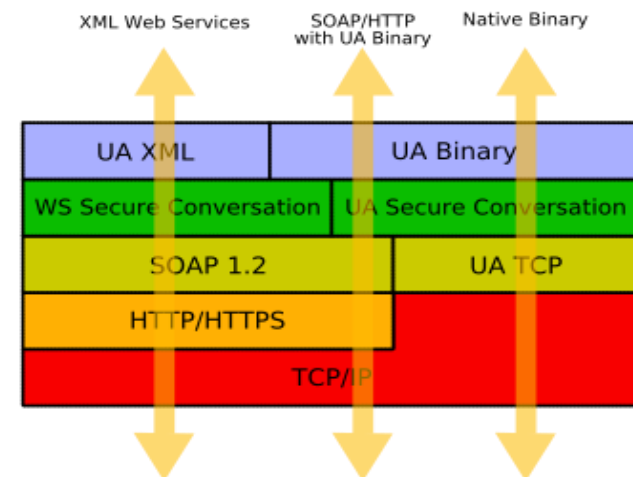
- **OPC DA sufre las vulnerabilidades de las tecnologías que usa: OLE, RPC, el sistema operativo,...**
- **RPC requiere autenticación local tanto en servidor como cliente**
  - Esto implica crear cuentas comunes locales o basadas en dominio
  - Puede introducir problemas si no están configuradas apropiadamente de acuerdo al principio de mínimo privilegio
- **Los equipos involucrados deberían usar autenticación y guardar en los logs las conexiones DCOM**
  - No obstante, los servicios de autenticación de alguno de estos equipos, posiblemente obsoletos, pueden ser vulnerables
- **OPC soporta otros protocolos de NetBIOS y HTTP, que generalmente serán innecesarios**
- **Se puede suplantar al servidor OPC**



# OPC UA

- **Unified Architecture**

- Nueva especificación del estándar no compatible hacia atrás
- Independiente de la plataforma
- Formato binario o XML
- Servicios web SOAP: clientes no específicos de OPC-UA podrían consumir datos
- Permite crear un modelo del dispositivo y los procesos: tipos, información semántica, relaciones



Fuente: Hochgeladen von Gergap, Wikipedia

# OPC UA

- **Medidas de seguridad:**
  - cifrado con infraestructura de clave pública
  - autenticación con tokens o certificados
  - WS Secure Conversation, TLS.
- **Al tratarse del “estándar moderno” en el ámbito industrial, parece haber tenido una rápida aceptación**
- **Utilizado en más ámbitos que el OPC clásico**

# RED INALÁMBRICA INDUSTRIAL

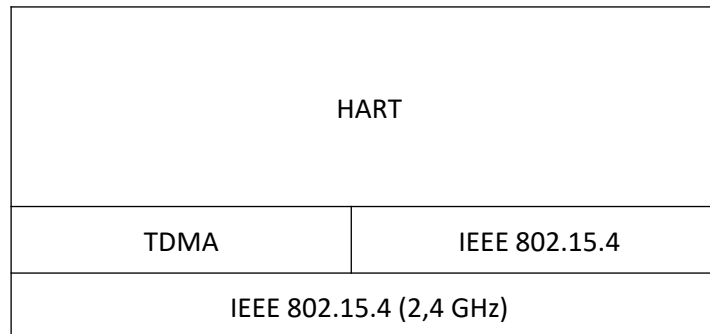
- **Para qué se utilizan**
  - Supervisión del estado de los equipos para mantenimiento
  - Monitorización ambiental y de emisiones
  - Localización y seguimiento de equipos
- **Adopción reciente pero en rápido aumento**
- **Dos protocolos específicos:**
  - ISA 100.11A
  - WirelessHart



# RED INALÁMBRICA INDUSTRIAL

- **WirelessHART (IEC 62591)**
  - Mantenimiento, monitorización y diagnóstico de dispositivos de campo
  - La comunicación utiliza comandos HART
  - Gestor de red central para establecer las rutas en la red mallada

WirelessHART



# RED INALÁMBRICA INDUSTRIAL

- **WirelessHART (IEC 62591)**
  - Confidencialidad: cifrado AES de 128 bits
  - Autenticación de dispositivos e integridad
  - Todo dispositivo WirelessHART requiere de una clave para poder unirse a una red.
  - Una vez asociado, se puede crear una lista de control de accesos y dotar al dispositivo con una nueva clave
  - No se soporta el uso de certificados por lo que no se puede garantizar el no repudio

# RED INALÁMBRICA INDUSTRIAL

- **ANSI/ISA100.11a**
  - Hace uso de IPv6
  - Red mallada
  - Capa de aplicación orientada a objetos
    - Diferentes objetos para optimizar el uso del canal, gestionar la transmisión de alarmas, cargar/descargar bloques de datos, gestionar funciones típicas de E/S (entradas y salidas analógicas y digitales), tunelar otros protocolos

ISA 100.11A

Protocolo nativo - Túnel a otros protocolos	
UDP	
6LoWPAN	IPv6
ISA100.11a Data Link	IEEE 802.15.4
IEEE 802.15.4 (2,4 GHz)	

# RED INALÁMBRICA INDUSTRIAL

- **ANSI/ISA100.11a**
  - Comprobación de integridad y protección ante ataques *replay*, ya que toda comunicación usa una marca temporal para construir una clave única
  - El proceso de unión usa claves asimétricas y no requiere un intercambio inicial seguro con el dispositivo
  - Cifrado a nivel de transporte (también AES 128)

# TENDENCIAS FUTURAS

- **Puesto que las funciones, generalmente expuestas como servicios, deben estar disponibles para diferentes recursos**
  - Cada vez más, tecnologías genéricas de comunicación como HTTPS, OPC UA, MQTT o CoAP.
- **Actualizaciones de protocolos para incluir medidas de seguridad:**
  - *Modbus/TCP security:*
    - Identidad basada en certificados (x.509v3)
    - Autenticación mediante credenciales o certificado y canal TLS
    - Autorización mediante roles codificados en los certificados
  - *CIP security:*
    - Autenticación mediante certificados X.509 o claves precompartidas
    - Integridad mediante el código de autenticación de mensaje de TLS
    - Cifrado de mensaje mediante TLS/DTLS
    - Perfiles de seguridad dependiendo el soporte del dispositivo



# TENDENCIAS FUTURAS

- **Ethernet con soporte para TSN (time-sensitive networking)**
  - Extensión para proveer a IEEE 802.3 de una latencia determinista para tráfico prioritario
- **5G para áreas como logística, robótica y aplicaciones de control de movimiento y localización de dispositivos y piezas**
  - Mayor capacidad, fiabilidad y velocidades de transmisión, menor consumo y latencia de red, lo que permite su uso en dispositivos pequeños y aislados
  - *Ultra-reliable low-latency communication*, espectro licenciado para el control de interferencias, autenticación mediante SIM o certificado, capacidad de segmentación virtual, posicionamiento en interiores, sincronización entre dispositivos

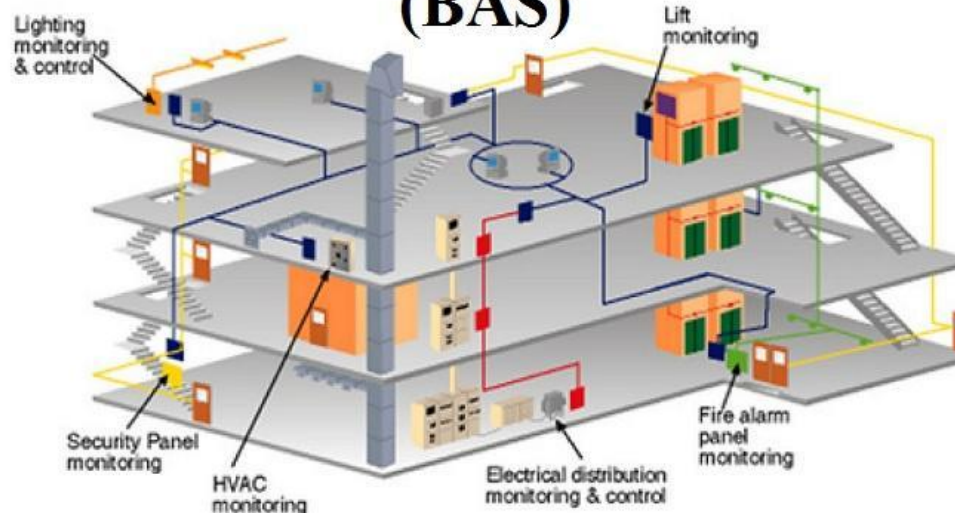
## ARQUITECTURA Y TECNOLOGÍAS

# Automatización de edificios

# AUTOMATIZACIÓN DE EDIFICIOS

- Protocolos semejantes a los del ámbito industrial
- Generalmente disponibles sobre más medios físicos
- La programación en la automatización de edificios suele ser más sencilla → Creación de grupos, enlace entre bloques, etc.
- Misma situación en cuanto a la seguridad

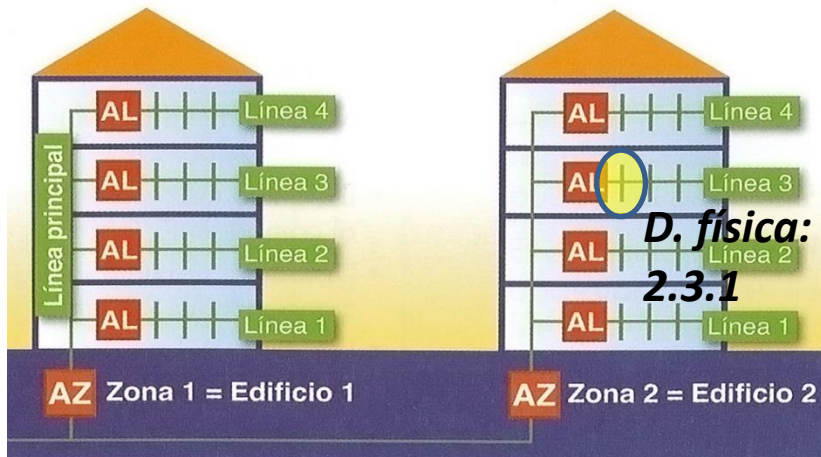
## Building Automation Systems (BAS)

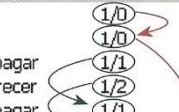




- De origen europeo, generalmente se usa en el control de sistemas de iluminación
- Sistema distribuido: en todos los elementos del bus hay una unidad de control
- Los sensores conectados al bus detectan eventos y envían los telegramas correspondientes a uno o varios actuadores para que ejecuten las órdenes
- Diferentes medios físicos disponibles: par trenzado, sobre TCP/IP, radiofrecuencia, PLC
- Configuración sencilla: software, equipo central o automática
- Los elementos tienen asociados objetos de comunicación (que implementan aplicaciones concretas)

- **Sistema de doble direccionamiento:**
  - **Dirección física (por ejemplo 1.1.2):** identificación única y clara del componente en función de su localización en la instalación (zona.línea.componente)
  - **Dirección de grupo (por ejemplo 5/2/12):** “cableado virtual” entre los objetos de comunicación de los componentes KNX que define su funcionalidad (subsistema/función/punto-final).
- **Se asigna una misma DG a un sensor y a uno o varios actuadores.**



Padre	Número	Nombre	Función del Objeto	C	Direccione...	longitud
1.1.1 Pulsa...	0	Conectar tecla izquierda	Encender	1/0		1 bit
	1	Conectar tecla izquierda	Apagar	1/0		1 bit
	2	Regulación E/A tecla de...	Encender / Apagar	1/1		1 bit
	3	Regulación tecla derecha	Aclarar / oscurecer	1/2		4 bit
1.1.3 Regu...	0	Conectar, Status	Encender / Apagar	1/1	1 bit	
	1	Regulación	Aclarar / oscurecer	1/2	4 bit	
	2	Ajustar x %	Valor 8 bits		1 Byte	
	3	Estado	Valor 8 bits		1 Byte	
1.1.2 Salid...	0	Conmutar	Canal A	1/0	1 bit	
	1	Conmutar	Canal B		1 bit	
	2	Enlace	Canal A		1 bit	
	3	Enlace	Canal B		1 bit	

# KNX

- **KNXnet/IP**
  - Sobre UDP
- **Hay una extensión (KNX Secure) de KNX que provee cifrado de paquetes, disponible para versiones recientes del software y dispositivos concretos**
- **Para los dispositivos seguros se crea un certificado basado en una clave interna que jamás se comparte por el medio de comunicación**
- **La gestión de la clave la realiza el software ETS**

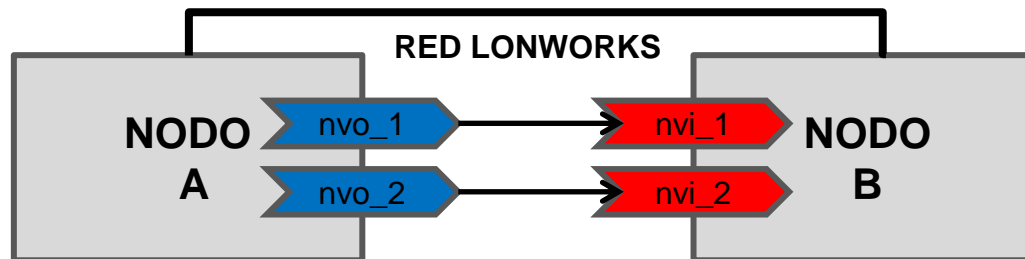
# LONWORKS



- De origen americano, *Local operating network*
- Modular y ampliable
- Sobre muy diversos medios físicos
- Varios tipos de direccionamiento:
  - Dirección física: fija para cada nodo (Neuron ID) para configurar
  - Dirección del dispositivo: para gestionar (Dominio / Subred / Nodo)
  - Direcciones de grupo y broadcast

# LONWORKS

- **Standard Network Variable Types (SNVTs)**
  - Simples (SNVT\_temp\_f), estructurados (SNVT\_switch) o enumerados (SNVT\_Occupancy)
- **Bindings (Cableado virtual):**
  - Conexiones lógicas entre una variable de salida en un dispositivo y una variable de entrada en otro, con el mismo tipo SNVT



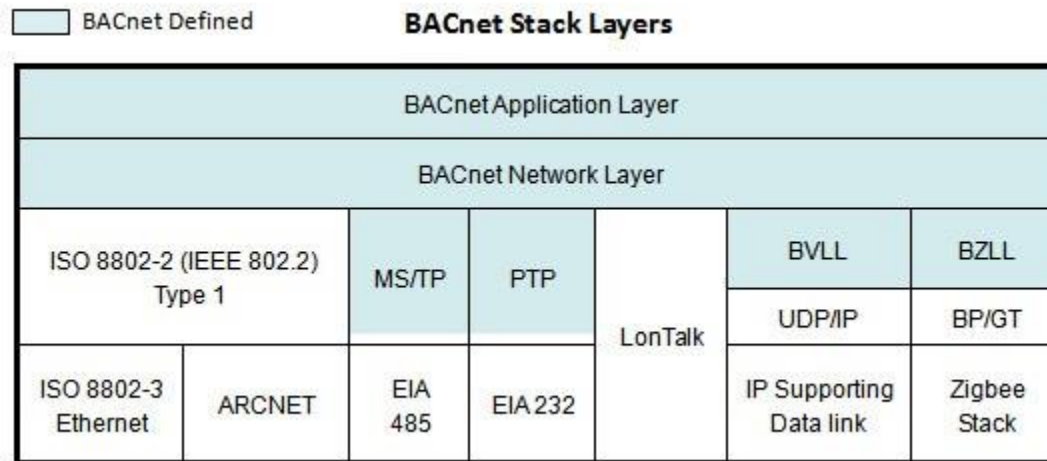


# LONWORKS

- LonTalk/IP
- El protocolo LonTalk no implementa cifrado de datos, sólo se dispone de autenticación del remitente
  - Basada en una clave única de 48 bits para cada dispositivo, preconfigurable, no recuperable y no modificable sin conocerla.
  - Cada dispositivo debe conocer la clave de cada uno de los miembros de la red
  - El dispositivo mandará los mensajes autenticados mediante un mecanismo de 4 pasos, basado en un reto de 64 bits
  - Esta autenticación es por mensaje, no por sesión

# BACNET

- Control y supervisión de sistemas de refrigeración y calefacción
- Representa la información del sistema en términos de objetos
- Las peticiones/interacción se formalizan en términos de servicios: De acceso a objetos (*ReadProperty*, *WriteProperty*, ... ), de alarma y eventos, de gestión de dispositivos remotos (*Who-Has*, *I-Have*, *Who-Is*, *I-Am*,...), de acceso a archivos y de terminal virtual



# BACNET

- **BACnet/IP: Especificación de BACNET sobre TCP/IP (sobre UDP)**
- **Permite cifrado:**
  - Sujeto a 4 políticas de seguridad de red: *Plain-trusted* (requiere seguridad física y no se aplica la seguridad del protocolo), *signed-trusted* (mediante firmas), *encrypted-trusted* (mediante cifrado AES), *plain-non-trusted* (en texto plano)
  - Hay 6 tipos de claves diferentes dependiendo de la tarea, distribuidas a todos los dispositivos desde el servidor de claves de la red: *General-Network-Access*, *User-Authenticated*, *Application-Specific*, *Installation*, *Distribution*, *Device-Master*
  - La seguridad en los mensajes BACnet es aplicada en la capa de red

# AUTOMATIZACIÓN DE EDIFICIOS INALÁMBRICA

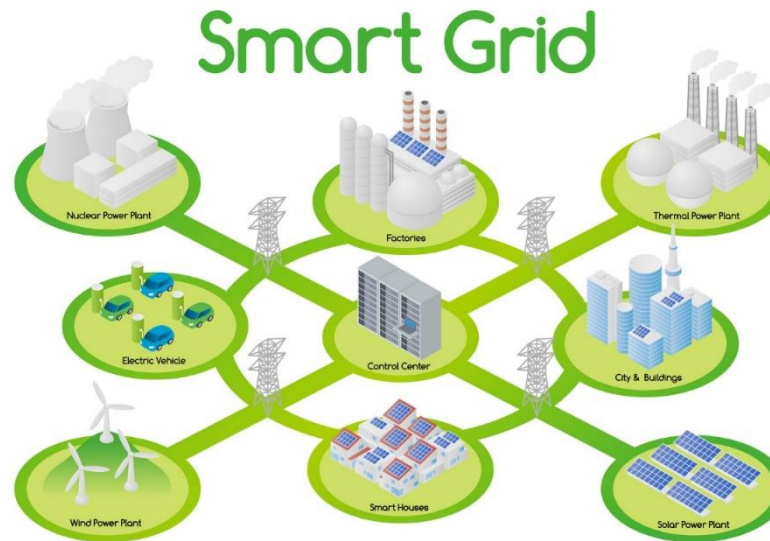
- **Tecnologías abiertas y propietarias**
  - Zigbee
  - EnOcean
  - Z-Wave
- **Convergencia con el mundo IoT**

## ARQUITECTURA Y TECNOLOGÍAS

# Automatización de las redes de energía eléctrica

# ENERGÍA ELÉCTRICA

- **Smart grid**
  - Red eléctrica que integra las acciones de todos los usuarios conectados (generadores, comercializadores y consumidores)
  - Complejo sistema de sistemas ciberfísicos
  - Optimización del sistema
    - mayor eficiencia, aplanando la curva de la oferta y demanda,
    - reduciendo de forma significativa el impacto medioambiental
    - incrementando la fiabilidad, calidad y seguridad



# ENERGÍA ELÉCTRICA

- **Sistema muy amplio y extenso:**

**Generación ⇔ transporte ⇔ distribución ⇔ consumo y medida**

- **La red de transporte lleva la electricidad en alta tensión a la red de distribución**
  - Elementos de control, protección y medida en sus subestaciones y de supervisión en centros de control
- **La red de distribución lleva la electricidad en media tensión al consumidor final**
  - De nuevo, elementos de control y protección en subestaciones y centros de transformación y de supervisión en centros de control
- **La medida del consumo se basa en la actualidad en el uso de medidores inteligentes, que permiten intercambio de información para facilitar la gestión de la red**

# TRANSPORTE Y DISTRIBUCIÓN

- Algunos de los dispositivos de control tienen que reaccionar ante situaciones de forma muy rápida, para evitar interrupciones en el suministro y otros problemas
- Otros controlan la actuación de las subestaciones y centros de transformación de acuerdo a la planificación de la red
- Tecnologías de comunicación tanto dentro de la propia subestación como con los centros de control
  - IEC 60870-5 101 y 104
  - DNP3
  - IEC 61850
  - Otros auxiliares, como Modbus



# TRANSPORTE Y DISTRIBUCIÓN

- **IEC 60870-5**

- El IEC 60870-5 se usa especialmente en Europa
- Principalmente las especificaciones 101 y 104
- **IEC 101**
  - Sobre serie
  - De forma local, para comunicar control y campo
- **IEC 104**
  - Sobre TCP/IP
  - Para la comunicación entre centros de control y subestaciones
  - Capa de aplicación similar a 101, aunque no todas las funciones están disponibles

# TRANSPORTE Y DISTRIBUCIÓN

- **DNP3**
  - Especialmente en EEUU
  - Sobre TCP/IP o sobre serie
  - Más complejo: tipos de datos, grupos de objetos, etc.
  - Mensajes con *timestamp* para sincronización
  - Orientado a eventos (3 clases o niveles de prioridad)
  - Funciones más allá de la mera lectura o escritura de variables



# TRANSPORTE Y DISTRIBUCIÓN

- **DNP3**

- Inicialmente con verificación de integridad, pero sin autenticación y cifrado
- Mayor complejidad de la implementación, que ha derivado en el descubrimiento de algunas vulnerabilidades
- Algunos posibles ataques:
  - desactivar mensajes explícitos (*unsolicited*) para silenciar alarmas,
  - falsificar mensajes para hacer creer que han ocurrido eventos,
  - inyección de *broadcasts* para DoS
  - manipulación de los datos de sincronización temporal
- **DNP3 Secure Authentication:**
  - Capa entre aplicación y transporte que incorpora autenticación y cifrado

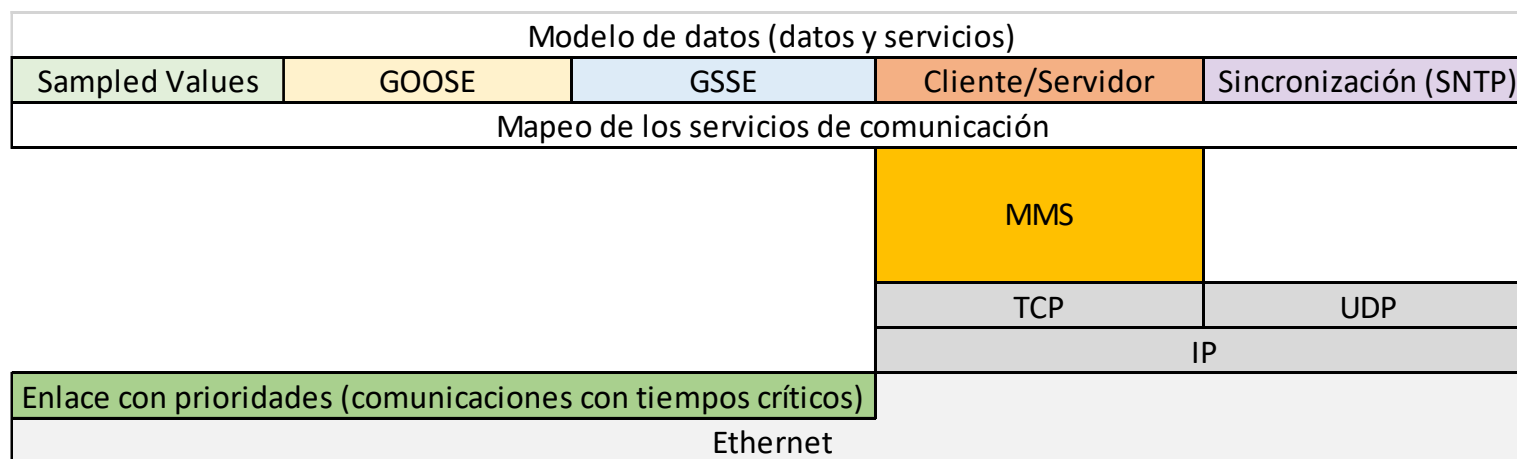
# TRANSPORTE Y DISTRIBUCIÓN: IEC 61850

- **Usado en Europa, centrado en la organización de los datos**
- **Diferentes perfiles de comunicación**
- **Abstrae la definición de los datos y servicios para hacerlos independientes de los protocolos subyacentes**
  - Es necesaria una configuración avanzada mediante un lenguaje de configuración de subestaciones (SCL) basado en XML
- **La descripción de los dispositivos es autocontenida**
  - Se requiere menos configuración manual
  - Un dispositivo físico puede tener varios dispositivos lógicos, que a su vez contienen nodos lógicos, que son agrupaciones de datos y servicios relacionadas con una función (medida, supervisión, protección, etc.)

# TRANSPORTE Y DISTRIBUCIÓN: IEC 61850

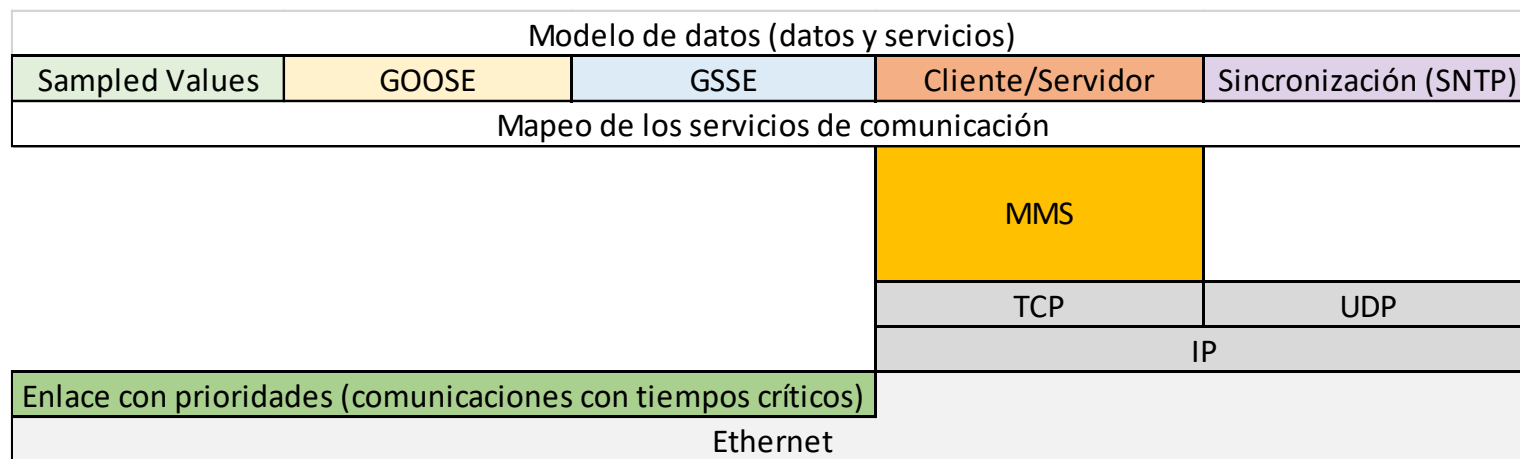
- **Perfiles de comunicación asociados:**

- SMV (Sampled Measured Values): comunicación rápida de valores de medición, protección y control en multicast
- GOOSE (Generic Object Oriented Substation Event): transmisión en tiempo real de eventos críticos en multicast
- GSSE (Generic Substation Status Event): alternativa a GOOSE más antigua y limitada



# TRANSPORTE Y DISTRIBUCIÓN: IEC 61850

- **Perfiles de comunicación asociados:**
  - Pila de protocolos MMS (Manufacturing Message Specification)
    - Intercambio de datos de aplicación, parámetros de configuración de los dispositivos, datos de monitorización
    - Normalmente sobre TCP aunque MMS también está definido sobre pila propia
  - SNTP (Simple Network Time Protocol): Sincronización de tiempo



# TRANSPORTE Y DISTRIBUCIÓN: IEC 61850

- **SMV, GOOSE y MMS no implementan por sí mismos ningún mecanismo de cifrado ni autenticación**
- **Por ello, existe un estándar de seguridad que acompaña al IEC 61850: el IEC 62351**
  - Presenta medidas y mecanismos desde diversos puntos de vista: arquitectura, autenticación, uso de certificados,... (IEC 62351 )
  - Las aplicaciones con requisitos de tiempo menores a 4 milisegundos como GOOSE y SV dificultan el cifrado
  - Se plantean mecanismos de firmado eficiente, protecciones frente a retransmisión, el uso de VLANs
  - Para el MMS se plantea el uso de TLS y certificados, así como mecanismos de configuración

# MEDIDA DE LA ENERGÍA ELÉCTRICA

- ***Advanced Metering Infrastructure***
- **Los medidores inteligentes generalmente se comunican con un concentrador**
  - Sobre *powerline communication*, Ethernet, inalámbrico, ...
- **Los contadores inteligentes están accesibles físicamente y por tanto necesitan seguridad interna además de seguridad de red**
- **Protocolos: diversas alternativas dependiendo de zona geográfica u operador**





# MEDIDA DE LA ENERGÍA ELÉCTRICA

- **PRIME+DLMS/COSEM**

- PRIME es un protocolo abierto sobre *power line communications* definido hasta capa de enlace
  - Permite cifrar a nivel de capa de enlace
- DLMS/COSEM (*Device Language Message Specification / Companion Specification for Energy Metering*)
  - Es un protocolo de aplicación basado en objetos
  - La clase que configura la seguridad permite niveles, desde al acceso sin contraseña a una autenticación mutua de 4 pasos
  - Utiliza perfiles en el sistema de autorización (público, lectura, escritura y actualización del firmware) que pueden ser matizados por medio de un contexto)
  - Además de la protección del mensaje, se pueden proteger los datos extremo a extremo

# MEDIDA DE LA ENERGÍA ELÉCTRICA

- **Meters&More**

- Protocolo más sencillo que el DLMS/COSEM, aunque se puede usar conjuntamente con él
- Comunicación mediante PLC, TCP/IP, puerto óptico
- Ofrece:
  - Cifrado de la comunicación mediante clave simétrica AES128
  - Autenticación mediante claves simétricas
  - Comprobación de integridad

- **Otras alternativas**

- G3-PLC
- OSGP (Open Smart Grid Protocol)

# ARQUITECTURA Y TECNOLOGÍAS

## Redes de sensores (inalámbricas)

# COMUNICACIÓN INALÁMBRICA

- En entornos no críticos como *smart cities* o *IoT* están mucho más presentes
- **Ventajas**
  - Ausencia de cableado
  - Flexibilidad: dispositivos en lugares poco accesibles
- **Problemas:**
  - Interferencias – Denegación de servicio por inhibición
  - Seguridad – Medio accesible
- **Dispositivos embebidos → Sector muy activo**
- **Coexistencia de protocolos abiertos y propietarios, así como de tecnologías específicamente inalámbricas o más generales**

# COMUNICACIÓN INALÁMBRICA

- **Medios**

- Wi-Fi (IEEE 802.11)
- Bluetooth
- **IEEE 802.15.4**
  - Es un estándar de comunicación inalámbrica de bajo coste y baja potencia
  - Define capa física y de enlace
- ISO/IEC 14543-3-10
  - Base de EnOcean



# COMUNICACIÓN INALÁMBRICA - IOT

- **Tecnologías propiamente inalámbricas**

- Zigbee
- WirelessHart
- ISA 100.11a
- EnOcean
- LoRa
- Sigfox
- Z-Wave
- Thread
- ...



- **Tecnologías no necesariamente inalámbricas pero ampliamente utilizadas**

- MQTT
- CoAP

# COMUNICACIÓN INALÁMBRICA - IOT

- Protocolos IoT

Zigbee Device Object	MQTT		LWM 2M	XMPP, AMQP
			CoAP	
Zigbee APS (Application Support Sublayer)	TCP (+SSL/TLS)	UDP (+DTLS)		TCP (+SSL/TLS)
Capa de red Zigbee	IPv6		IP	
	6LoWPAN			
Capa enlace IEEE 802.15.4	Capa enlace IEEE 802.15.4		Capa Enlace IEEE 802.11	
Capa física IEEE 802.15.4	Capa física IEEE 802.15.4		Capa Física IEEE 802.11	

## Protocolos abiertos

EnOcean Equipment Profiles
ISO/IEC 14543

## EnOcean

Aplicación
LoRa MAC
Radiofrecuencia

## LoRaWAN

- EnOcean para automatización de edificios para dispositivos sin alimentación → Cifrado y autenticación a nivel de MAC
- LoRa y Sigfox son tecnologías de red de área amplia (LPWAN) de bajo consumo.

# ZIGBEE

- **Basado en IEEE 802.15.4: capa física y enlace**
- **Redes de tipo malla**
- **Dispositivos de bajas prestaciones: baja velocidad, bajo consumo**
- **Capas de red, transporte y aplicación propias**
  - Las dos últimas se implementan mediante:
    - Capa soporte de aplicación
    - Objeto de dispositivo ZigBee (ZDO)
    - Objetos de aplicación
- **Tipos de dispositivos**
  - Coordinador de red
  - Routers
  - Dispositivos finales
  - Proveedor de servicios de seguridad



# ZIGBEE

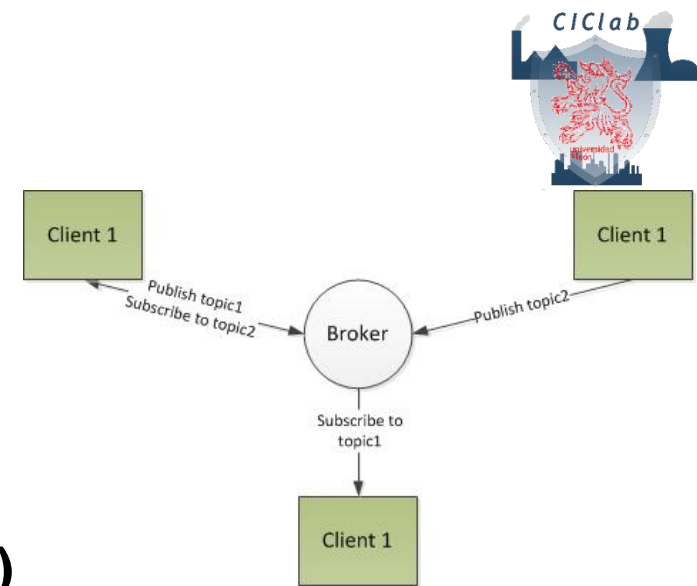
- **ZigBee especifica 3 niveles de seguridad:**
  - Sin seguridad
  - Listas de control de acceso (ACL)
  - Encriptación y autenticación AES (Advanced Encryption Standard) de 128 bits de clave simétrica
    - Claves de red: entre dos nodos
    - Claves de enlace: garantizar la seguridad extremo a extremo
    - Clave maestra, para generar las claves de enlace
  - Diversas opciones de gestión/establecimiento de claves: preinstalación (sólo para claves maestras), transporte de clave desde un centro de confianza, generación a partir de clave maestra
- **Denegación de servicio mediante múltiples dispositivos ficticios o *jamming***
- **Las claves se almacenan en memoria**

# COAP

- ***Constrained Application Protocol***
- **Protocolo cliente/servidor con comunicaciones N a 1 (un servidor a varios clientes)**
- **Implementación RESTful ligera:**
  - Se puede conectar con HTTP REST mediante proxies
- **Sobre UDP**
  - Cabecera fija de 4 bytes, diseñado para ser muy ligero
  - Dos niveles QoS (confirmable o no confirmable),
- **Mecanismo estándar para descubrir recursos, posibilidad de suscripción**
- **Permite encriptar con DTLS (*Datagram Transport Layer Security*)**

# MQTT

- ***Message Queue Telemetry Transport***
- **Modelo cliente/servidor**
- **Un servidor central (*broker*), recibe mensajes de los clientes (todos los nodos)**
- **Los mensajes pueden ser publicaciones o suscripciones a un *topic* (variable)**
- **Los *topics* se estructuran de manera jerárquica y se pueden usar *wildcards***
- **Permite comunicación N a N y desacopla productor y consumidor**



# MQTT

- Flexible y sencillo, facilita la conexión de dispositivos de bajos recursos a middleware y aplicaciones
- Tramas ligeras sobre TCP (o UDP si se usa la especificación MQTT-SN para redes de sensores)
- Tres niveles de QoS (a lo sumo un mensaje, al menos uno o exactamente uno)
- Admite autenticación mediante usuario/contraseña y encriptación con TLS/SSL

# COMUNICACIÓN INALÁMBRICA - IOT

- **La gestión de redes IoT requiere diversas funcionalidades**
  - Descubrimiento, autenticación, aprovisionamiento, supervisión, mantenimiento del firmware/software, etc.
- **Aparecen protocolos de gestión que complementan los anteriores**
- **LWM2M es uno de los más conocidos**
  - Usado conjuntamente con CoAP
  - Proporciona servicios adicionales
    - Descubrimiento, inicialización y registro de dispositivos
    - Gestión de dispositivos
    - Modelo de objetos (que proporcionan recursos)
- **También hay diversos frameworks, con funcionalidades de descubrimiento y gestión de dispositivos: AllJoyn, IoTivity,...**

# ARQUITECTURA Y TECNOLOGÍAS

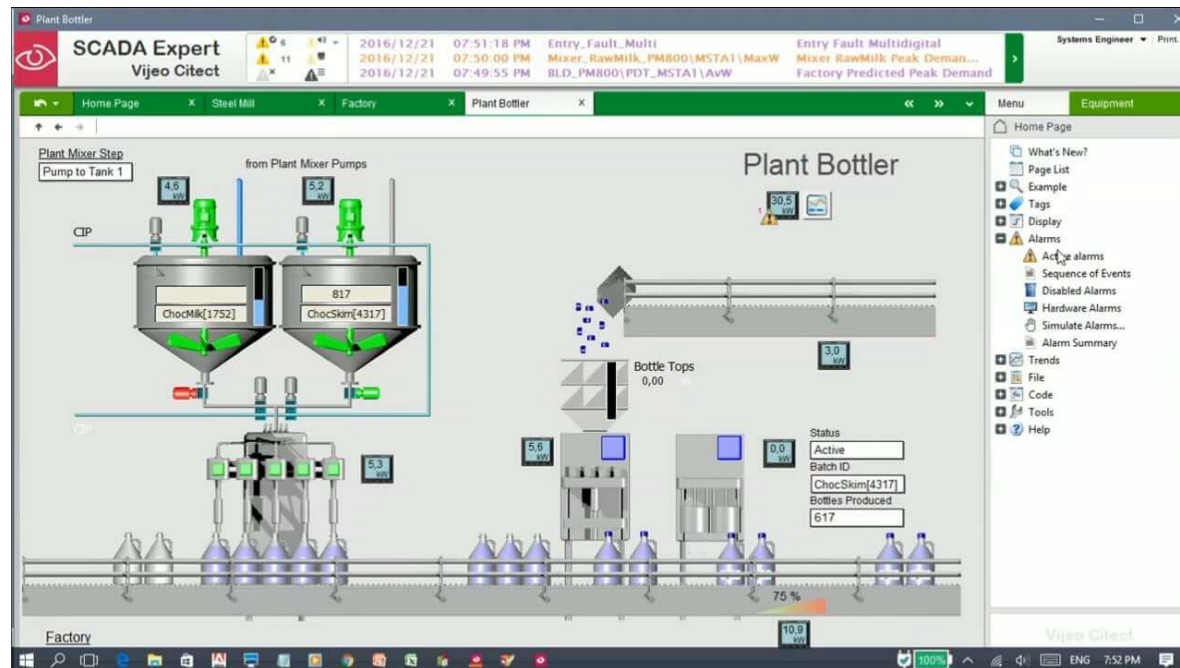
## Elementos de supervisión

# ELEMENTOS DE SUPERVISIÓN

- **La programación de pantallas de operador HMI y de los SCADA se realiza a través de aplicaciones específicas del fabricante**
  - Creación de pantallas lógicas con objetos predefinidos como pulsadores, visualizadores, entradas de teclado, gráficos tendencia, cuadros de alarmas
  - Es necesaria una configuración que incluye, entre otros,
    - los datos sobre las entradas/salidas que se supervisan y su tratamiento
    - los datos sobre la configuración de la comunicación con el equipamiento,
    - las condiciones de alarma, etc.
- **A menudo, las órdenes enviadas del SCADA/HMI al dispositivo de control utilizan extensiones o funciones especiales de los protocolos, lo que dificulta su monitorización**

# SCADA

- La arquitectura de los SCADA es generalmente cliente-servidor
  - Clientes “pesados” o clientes web
  - Algunos autores opinan que hay una tendencia hacia el SCADA *as a service*





# SCADA

- **Puede necesitarse redundancia a diferentes niveles**
  - El despliegue en entornos virtualizados puede facilitar la creación de entornos tolerantes a fallos
- **Un gran porcentaje de las vulnerabilidades encontradas en el ámbito industrial corresponden a plataformas SCADA**
- **Los fabricantes ya proporcionan guías para el bastionado del servidor**

# HMI

- **Los operadores de HMI generalmente no se autentican**
  - Durante una emergencia, ese mecanismo podría bloquear el acceso a la HMI, lo que se considera inseguro y viola el principio de disponibilidad garantizada
- **Sí que se suelen tener controles de acceso para funciones específicas, como parte de la propia interfaz**



# HMI

- **Estos dispositivos se instalan habitualmente en áreas con un nivel alto de seguridad física**
- **También corresponden a plataformas para HMI gran parte de las vulnerabilidades encontradas**
- **Los fabricantes comienzan a proporcionar políticas de grupo basadas en dominio**
  - Restringen la ejecución de aplicaciones locales y el acceso no autorizado a medios extraíbles

# HISTORIZADORES

- **La información almacenada en historizadores generalmente se replica en las redes industrial y corporativa, o bien se proporciona un acceso remoto**
  - En el nivel de supervisión, uso más limitado pero a un menor nivel de granularidad, analizando en profundidad eventos de interés
  - En el nivel de gestión, se usará para proporcionar una visión de conjunto de la instalación a los responsables
- **Los historizadores realizan una gestión eficiente o comprimida de los datos en forma de valor-*timestamp*-calidad del dato**
- **Mecanismos para asegurar integridad y salvaguarda de los datos**
- **Obtención de información generalmente a través del SCADA**

# HISTORIZADORES

- En ocasiones, redundante o replicado
- Un historizador en una zona menos segura pudiese utilizarse como vector para acceder a otras zonas
- Esta replicación o acceso remoto debe configurarse y vigilarse con especial atención
- Puesto que este software se basa generalmente en tecnologías de SGBD estándares, es también necesario estar al tanto de sus vulnerabilidades