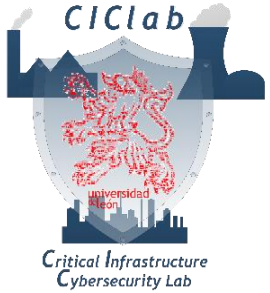
INTRODUCCIÓN

CIBERSEGURIDAD DE LOS SISTEMAS DE CONTROL

GRUPO SUPPRESS

SUPERVISIÓN, CONTROL Y AUTOMATIZACIÓN

universidad de león



Conceptos

SISTEMAS

- **Sistema de Control:** El que permite regular otro sistema para conseguir el comportamiento deseado
- Los sistemas de control modernos son **sistemas ciber-físicos** ya que combinan de forma integral los sistemas de control, la computación y las comunicaciones
- **Proceso Industrial:** Proceso que se encarga de obtener, transformar o transportar uno o varios productos primarios
- **Automatización:** Utilización de equipos y técnicas para que un proceso industrial funcione con poca o ninguna intervención humana
- **Sistema de Control Industrial:** Conjunto de dispositivos tecnológicos que permiten controlar la maquinaria que realiza un proceso industrial
- **Activo industrial:** Todo dispositivo usado dentro de un sistema de control industrial

SAFETY & SECURITY

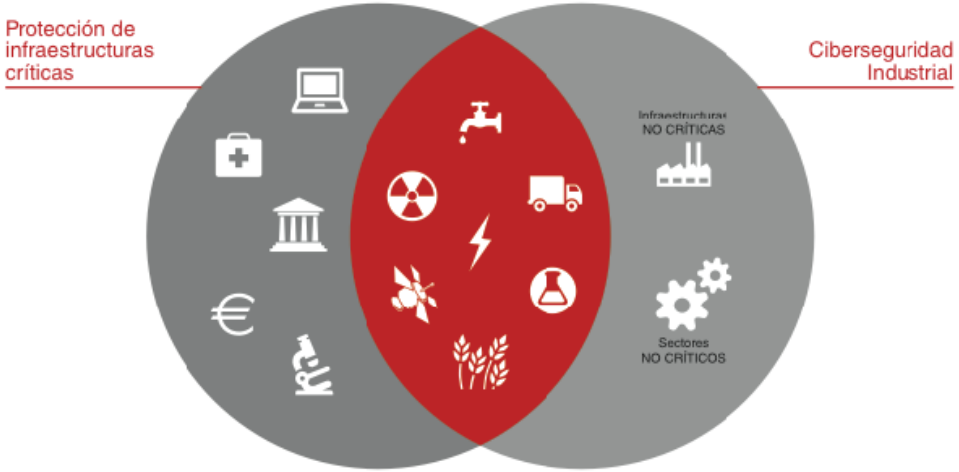
- **Seguridad operacional (*Safety*)**
  - Protección ante eventos accidentales
  - Prevención de daños a nivel de equipamiento, instalaciones y personas
  - Desastres naturales, fallos de equipamiento, error humano
  - Tradicionalmente muy tenida en cuenta en el desarrollo y operación de los sistemas de control

- **Seguridad (*Security*)**
  - Protección ante daños intencionados
    - Seguridad física: robos, sabotajes, etc.
    - Seguridad de la información (o ciberseguridad): ataques internos, malware, ataques externos, APTs

Relevancia

INFRAESTRUCTURAS CRÍTICAS

- Los sistemas de control son componentes esenciales de las infraestructuras críticas
- Una **infraestructura crítica** es una instalación o sistema que soporta servicios esenciales para la seguridad nacional o el conjunto de la economía de un país



INFRAESTRUCTURAS CRÍTICAS

- **No hay actividad humana que no se encuentre vinculada o dependa de algún sector estratégico contemplado por la normativa española:**
  - Administración
  - Agua
  - Alimentación
  - Energía
  - Espacio
  - Industria Química
  - Industria Nuclear
  - Instalaciones de Investigación
  - Salud
  - Sistema Financiero y Tributario
  - Tecnologías de la Información y las Comunicaciones (TIC)
  - Transporte

UBICUIDAD

- **Aunque una industria no esté catalogada como infraestructura crítica, su seguridad sigue siendo especialmente relevante por las serias consecuencias que podría acarrear un ataque:**
- **Los sistemas de control están presentes en todos los ámbitos imaginables, más allá de las infraestructuras críticas:**
  - Automóviles
  - Aeronáutica
  - Automatización de edificios
  - Dispositivos “inteligentes”
  - …

SITUACIÓN DE PARTIDA

- **Originalmente, la ciberseguridad en los sistemas de control no se consideraba una prioridad**
  - Ni por parte de los fabricantes ni de los operadores
  - No existía un marco regulador
- **Falsa sensación de seguridad**
  - Personal no formado
  - Se suponía que el sistema de control funcionaba de forma aislada y no estaba conectado a otros sistemas de información
  - Seguridad por oscuridad, pues se usa tecnología específica
- **Ignorancia de lo aprendido en el campo IT en las últimas décadas**

HECHOS PREOCUPANTES

- **Convergencia:**
  - actualmente se utiliza masivamente software comercial de uso común en otros sistemas de información

- **Por necesidades de gestión y operación, los sistemas de control están interconectados a redes corporativas (y/o al exterior)**

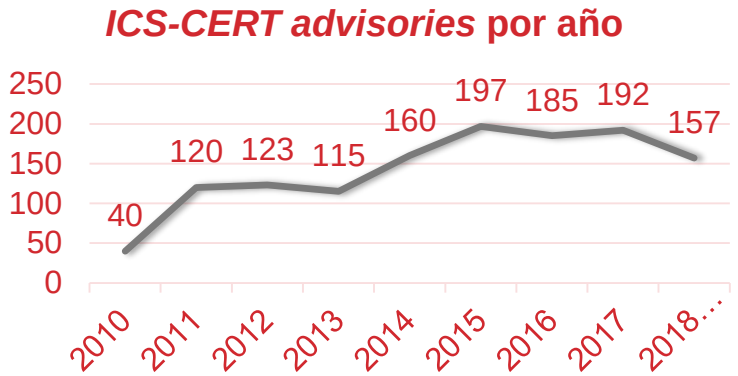
- **Hay suficiente información públicamente accesible**

~~AIR GAP~~

HECHOS PREOCUPANTES

- **Estos sistemas son un objetivo extremadamente atractivo para los atacantes con suficiente capacidad y recursos**

- **Las vulnerabilidades encontradas han aumentado**



- **Incidentes con gran repercusión: Stuxnet, red eléctrica ucraniana**

- **Cambios radicales: IoT, Industria 4.0,…**

SITUACIÓN ACTUAL

- En 2018, el 77% de las empresas ya otorga gran prioridad a la ciberseguridad de los sistemas de control
- Los fabricantes de tecnología industrial comienzan a incorporar las consideraciones de seguridad en el desarrollo del producto
- Desarrollos normativos y creación de entidades de supervisión en multitud de países
- Creación de CERTs específicos: ICS CERT, CERTSI, …
- Identificación de las infraestructuras críticas
- Exigencias y apoyo a sus operadores

SITUACIÓN ACTUAL

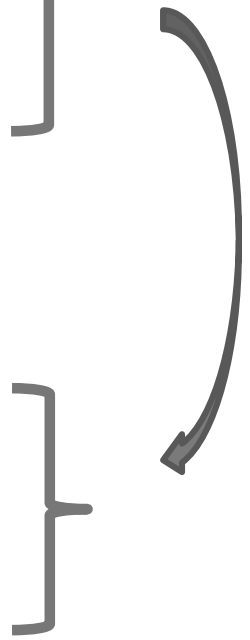
- **PERO sigue habiendo:**
  - Un nivel de madurez mucho menor que en otros ámbitos
  - Necesidad de desarrollar procedimientos más sistemáticos
  - Necesidad de desarrollar tecnologías adaptadas
  - Necesidades de formación

Particularidades

PARTICULARIDADES DE LOS SISTEMAS DE CONTROL

- **Longevidad de las instalaciones**
- **Funcionamiento continuo de las mismas**
- **A menudo se requieren bajas latencias y determinismo/tiempo real**

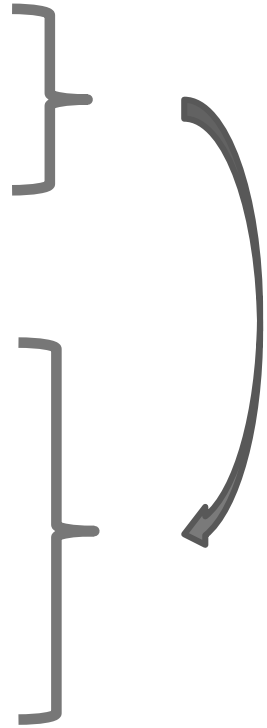
- **Difícil mantenimiento y parcheo**
- **Tecnologías obsoletas que ofrecen protección limitada o carecen de medidas de seguridad**



PARTICULARIDADES DE LOS SISTEMAS DE CONTROL

- La disponibilidad es más importante que la integridad y la confidencialidad, al contrario que en otros sistemas
- Software y hardware específico

- Protocolos de comunicación específicos e inseguros
- Dificultad para introducir modificaciones, deshabilitar servicios, añadir software adicional al proporcionado
- Ciertas prácticas habituales pueden perturbar la operación normal del sistema: antivirus, análisis activo de vulnerabilidades



PARTICULARIDADES DE LOS SISTEMAS DE CONTROL

- **Los recursos computacionales de muchos dispositivos son más limitados de lo habitual**
- **Arquitecturas de red específicas y potencialmente extensas**
- **Puede ser necesaria una certificación u homologación**
- **La gestión de logs y el análisis forense es complicado**

PARTICULARIDADES DE LOS SISTEMAS DE CONTROL

- **El personal no es únicamente de tipo informático:**
  - Diferentes prioridades, diferente lenguaje, diferente formación
- **Mayor dependencia de los fabricantes/proveedores del sistema de control**
- **Impactos más tangibles de los incidentes de seguridad:**
  - daños personales, en equipamiento y al entorno
  - impacto en la seguridad nacional
  - pérdida de producción, de calidad o de información confidencial
  - pérdida de reputación o confianza
  - violación de requisitos legales, etc.

Elementos de un sistema de control

HISTORIA

- Los primeros automatizaciones se basaban en sistemas cableados
- En 1969 se crea el primer autómata programable o PLC (*Programmable Logic Controller*), el Modicon 084
- A partir de ese momento, se produce una evolución, tanto en prestaciones como en capacidad de programación y conectividad
- Se pasa de un cableado directo de las señales de E/S a la utilización de redes de comunicaciones
- Aparecen arquitecturas de control distribuido
- La utilización de sistemas operativos y software comercial de uso común en otros ámbitos, junto con el uso de redes TCP/IP se populariza por la búsqueda de eficiencia y de funcionalidades como la supervisión eficaz o la gestión remota de los procesos

ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

- La norma ISA-95 define 5 niveles de funcionalidad en una automatización industrial

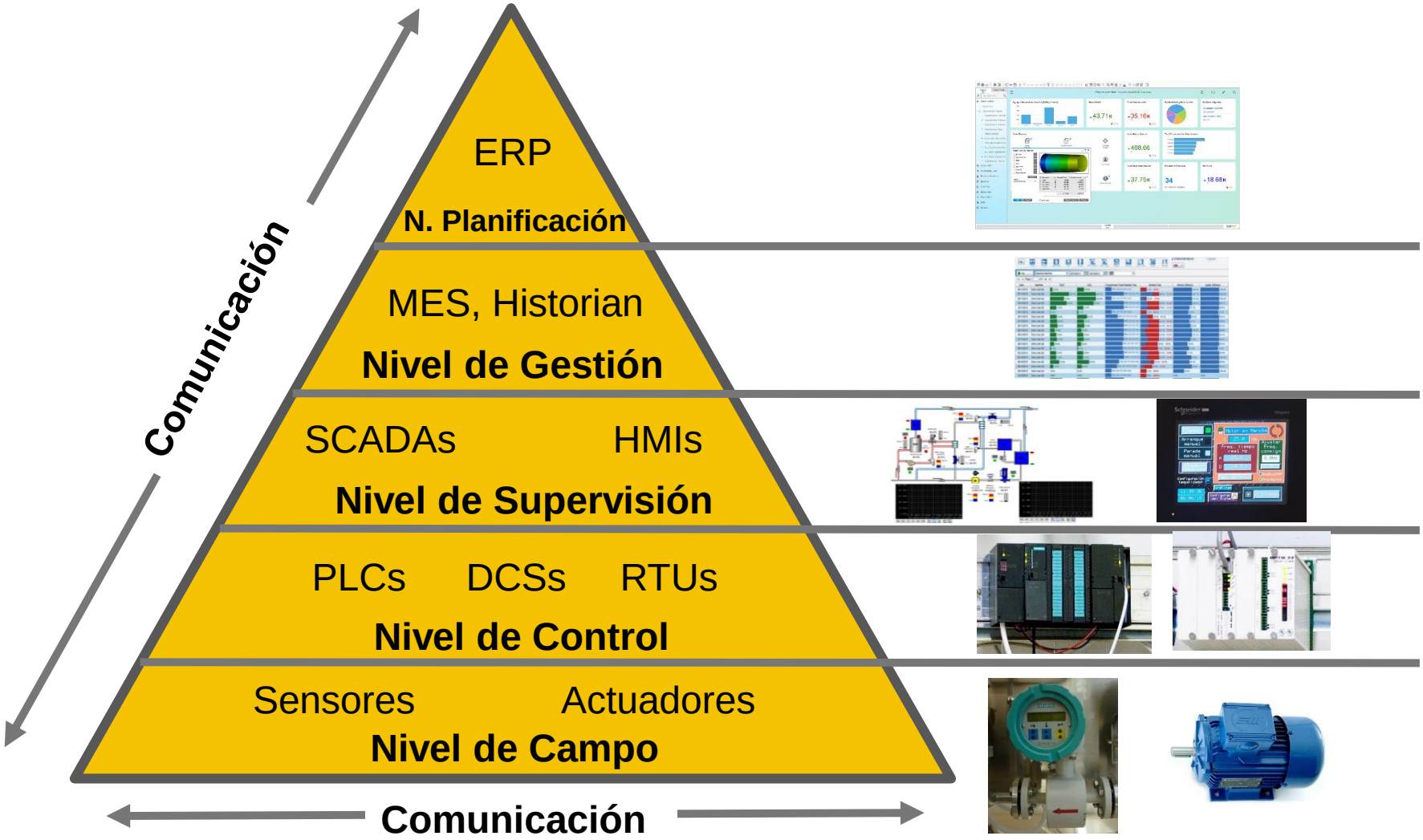
- Integración de los procesos de producción (diseño, ingeniería y fabricación) con los de gestión de la empresa

ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

- **Niveles ISA95**

NIVEL 4: Planificación de negocio y logística / *Enterprise resource planning* (ERP),*Business Intelligence*
NIVEL 3: Gestión del flujo de trabajo / *Manufacturing Execution System* (MES), gestión de lotes, gestión de históricos
NIVEL 2: Supervisión y control / SCADAs, controladores, interfaces hombre-máquina
NIVEL 1: Medición y manipulación de los procesos / Sensores, actuadores y controladores
NIVEL 0: Procesos físicos

ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

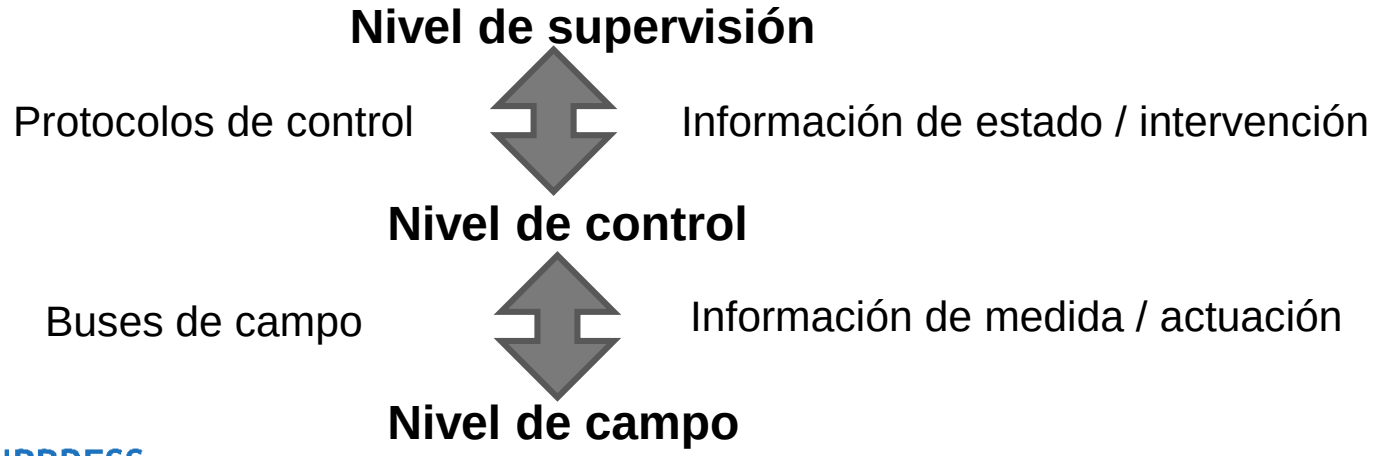


ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

- **Nivel de campo/ proceso:**
  - Conjunto de dispositivos, subprocesos, instrumentación en general, con que se realizan las operaciones elementales
  - Se adquieren datos mediante los sensores
  - Los actuadores ejecutan las acciones sobre el sistema físico determinadas por los algoritmos de control y consignas del nivel superior.
- **Nivel de control/estación:**
  - Encargado del mando y control de los elementos de campo.
  - Forman parte de él los diferentes sistemas electrónicos de control: Autómatas programables (PLCs), sistemas de control distribuido (DCSs), computadores industriales, microcontroladores,...

ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

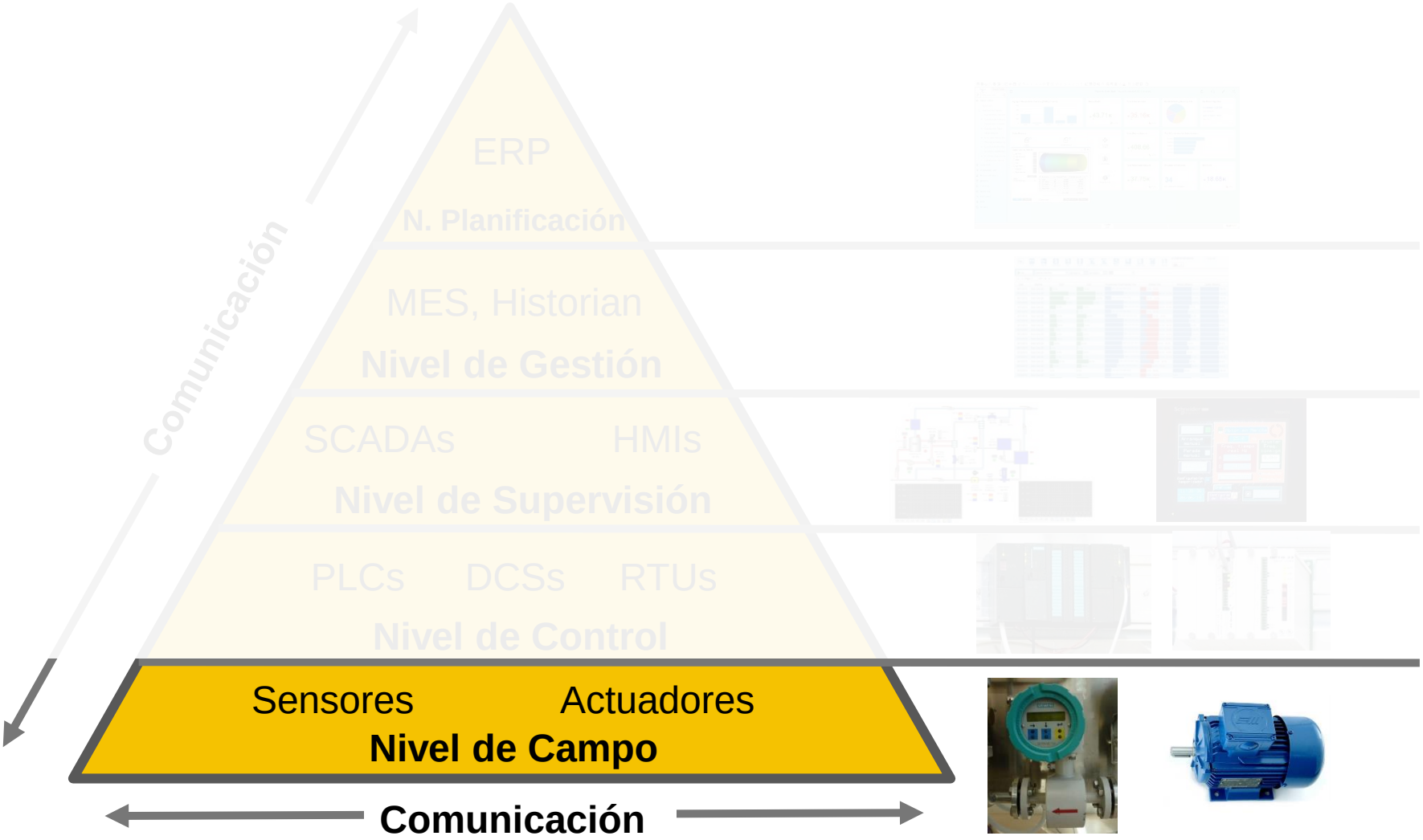
- **Nivel de supervisión:**
  - Sistemas encargados de la monitorización de las unidades productivas funcionales y de la intervención sobre las mismas
  - Tareas de toma de decisiones, establecimiento de consignas manuales, adquisición y tratamiento de datos, gestión de alarmas, mantenimiento, etc.
  - Interfaces hombre-máquina y sistemas SCADA (*Supervisory Control And Data Adquisition*)



ARQUITECTURA BÁSICA: PIRÁMIDE DE AUTOMATIZACIÓN

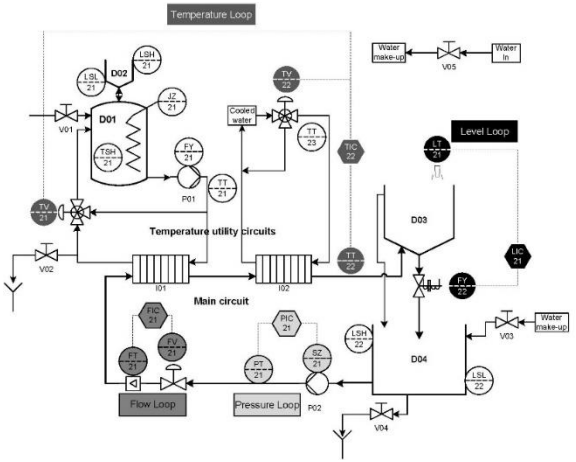
- **Nivel de gestión**
  - Actividades orientadas a la optimización de entornos industriales, la mejora de la productividad y el aseguramiento de la calidad
  - Asignación y gestión de recursos y procesos
  - MES (*Manufacturing Execution Systems*) y gestores de históricos (aunque estos últimos pueden también aparecer en el nivel de supervisión)
- **Nivel de planificación**
  - Integración de toda la información de la actividad industrial con el resto de actividades de la empresa (logística, distribución, inventario, contabilidad, recursos humanos, etc.)
  - Sistemas de planificación de recursos empresariales (ERP)

ELEMENTOS DE CAMPO



ELEMENTOS DE CAMPO

- **TRANSDUCTOR**
  - Dispositivo que convierte una señal de entrada, función de una o más cantidades físicas, en una de salida.
- **SENSOR**
  - Dispositivo capaz de medir una variable física
- **TRANSMISOR**
  - Capta la variable a través del sensor y la transmite a distancia en forma de señal (neumática o electrónica)
- **ACTUADOR o ACCIONAMIENTO**
  - Dispositivo que convierte una magnitud, generalmente eléctrica, en una salida, generalmente mecánica, que puede provocar un efecto sobre el proceso.



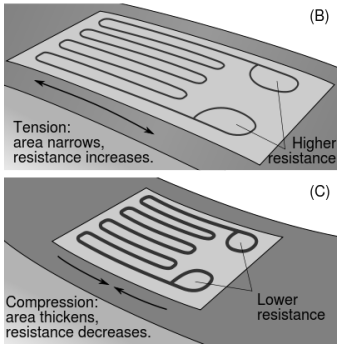
ELEMENTOS DE CAMPO: SENSORES

- **De cualquier magnitud física:**
  - Posición lineal o angular, velocidad lineal o angular, pequeños desplazamientos, aceleración, fuerza y par, presión, caudal, temperatura, presencia o proximidad, nivel, viscosidad, pH,…
- **De acuerdo a su principio de funcionamiento, pueden clasificarse como:**
  - Activos: La magnitud física medida proporciona la alimentación necesaria para generar señal de salida.
  - Pasivos: Con alimentación externa, modifican parámetros característicos como resistencia, capacidad,...
- **Se describen por medio de características:**
  - Estáticas, como el rango de medida, la resolución, la exactitud, la precisión, la sensibilidad, la linealidad o la histéresis
  - Dinámicas, como la deriva, la respuesta frecuencial o la velocidad de respuesta

ELEMENTOS DE CAMPO: SENSORES

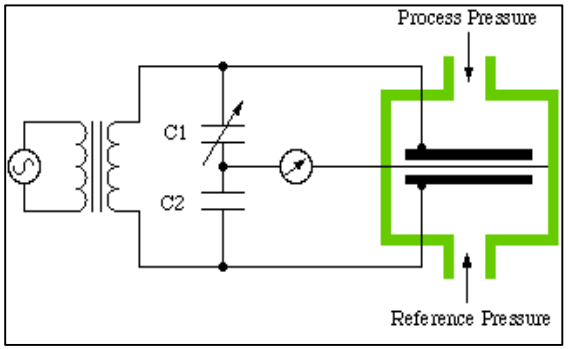
Ejemplos

Fuente: Izantux, Wikipedia



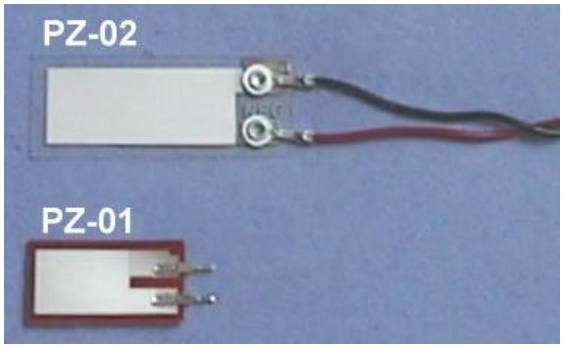
Resistivo

Fuente: Charles D. H. Williams



Capacitivo

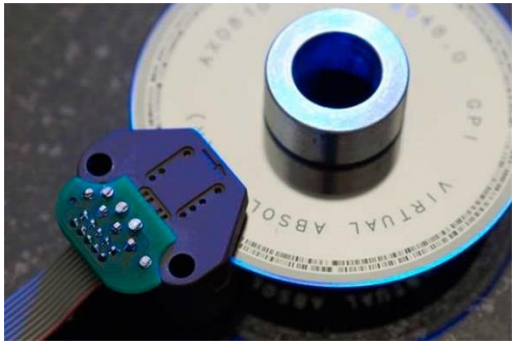
Fuente: Images Scientific Instruments



Piezoeléctrico

Fuente: www.ecvv.com

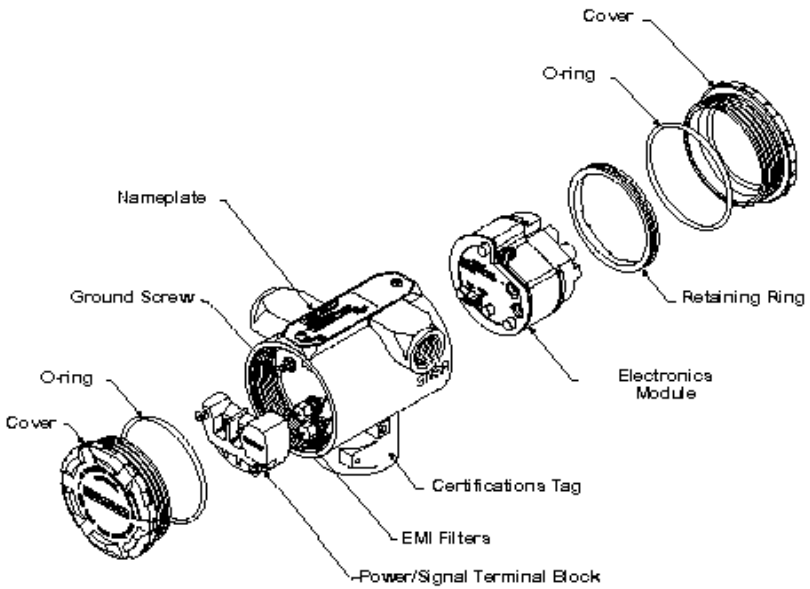
Fuente: Schmersal



ELEMENTOS DE CAMPO: TRANSMISORES

- **Elementos del transmisor:**
  - El sensor puede estar separado o integrado
  - Tienen un bloque de tratamiento de señal y una etapa de salida que generalmente amplifica la señal
- **Tipos de salida del transmisor:**
  - Analógica
    - La señal estándar es generalmente de 4-20mA (bucle de corriente) o 0-10V (bucle de tensión) de corriente continua
  - Digitales todo-nada,
  - Con señal codificada
    - Usando protocolos de bus de campo específicos
    - El transmisor debe realizar la modulación, conversión a digital, etc.
- **Los transmisores en la actualidad pueden también permitir: corregir no linealidades, realizar cálculos, autocalibrarse o autodiagnosticarse, etc.**

ELEMENTOS DE CAMPO: TRANSMISORES



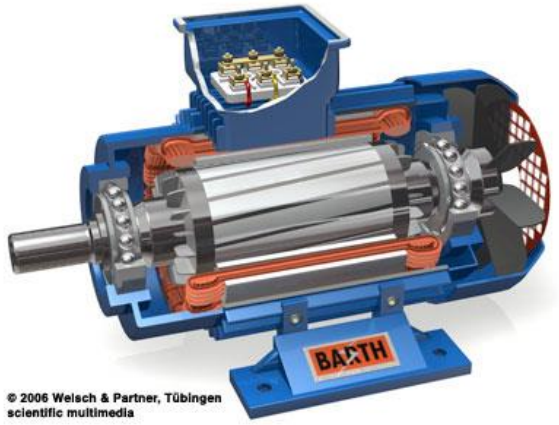
ELEMENTOS DE CAMPO: ACTUADORES

- **Deben responder de manera rápida y precisa**
- **Incluyen a menudo un servo-motor, es decir, un motor que cuenta con un sensor y la posibilidad de obtener un comportamiento estable, rápido y fácil de controlar**
- **Pueden presentar limitaciones como saturación o zona muerta**
- **Eléctricos, neumáticos o hidráulicos**

Fuente: Jesús Esparza y Gustavo Baños

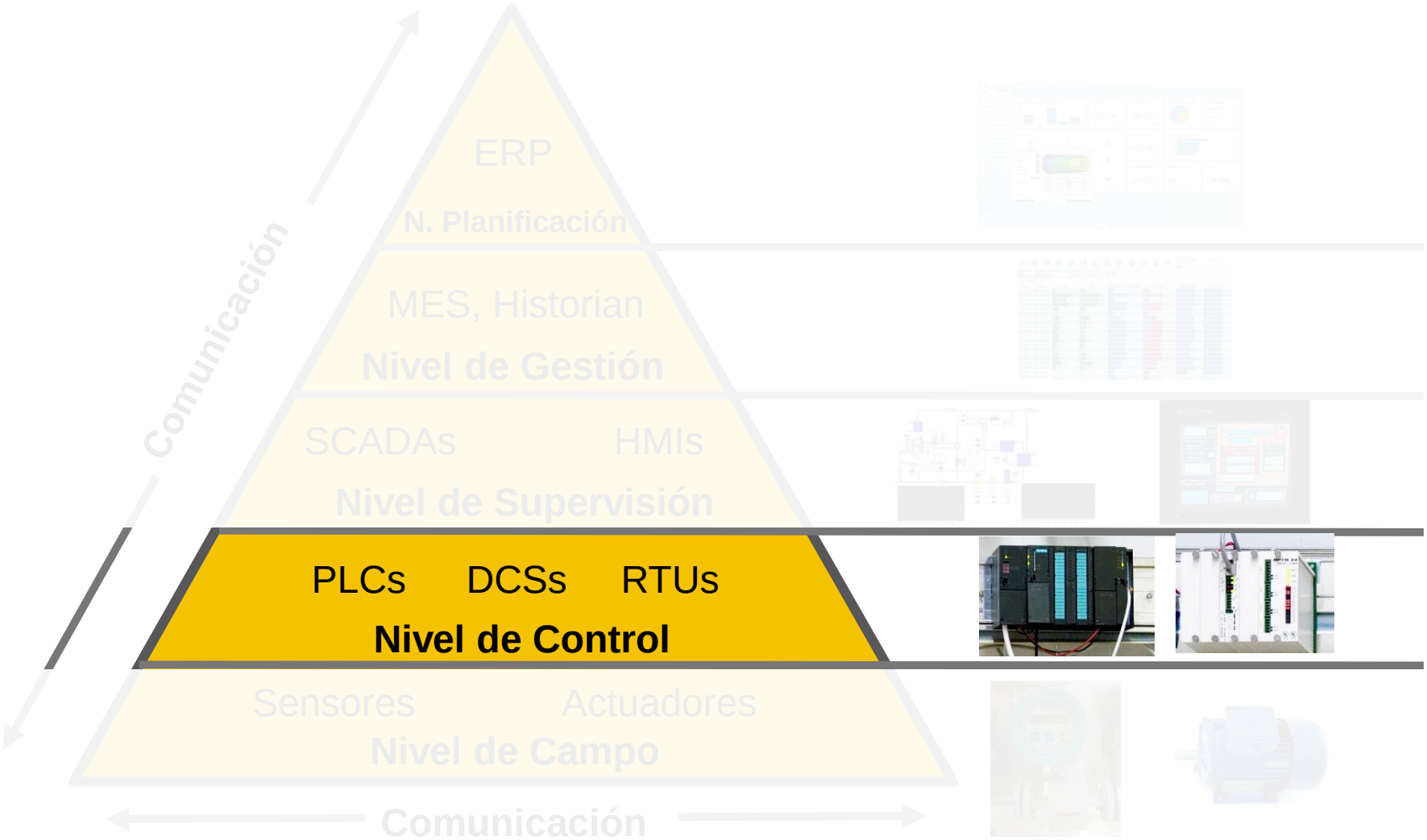
ELEMENTOS DE CAMPO: ACTUADORES

- **Actuadores Eléctricos**
  - Motores de corriente continua
    - Con escobillas (tradicionales)
    - Sin escobillas y paso a paso
  - Motores de corriente alterna
    - Síncronos
    - Asíncronos o de inducción



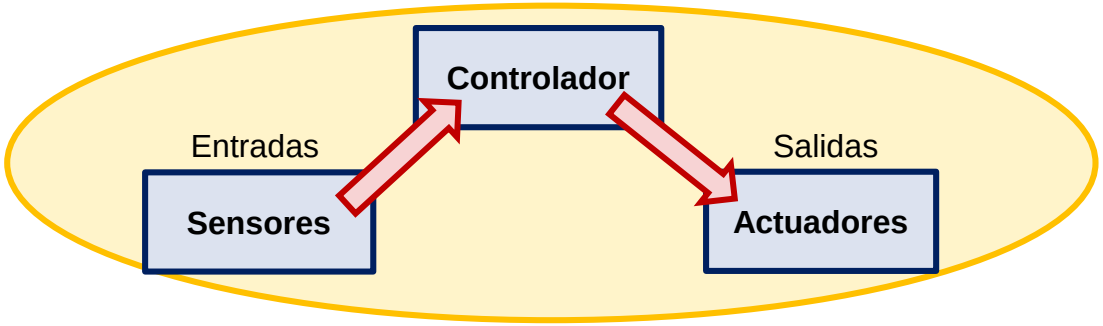
- **Actuadores Neumáticos/Hidráulicos**
  - Cilindros
  - Motores

ELEMENTOS DE CONTROL



ELEMENTOS DE CONTROL

- **Autómatas programables (PLCs, *programmable logic controllers*) y su periferia**
- **Sistemas de control distribuido (DCSs)**
- **Unidades terminales remotas (RTUs)**
- **PCs industriales**
- **Microcontroladores y máquinas dedicadas**



AUTÓMATAS PROGRAMABLES

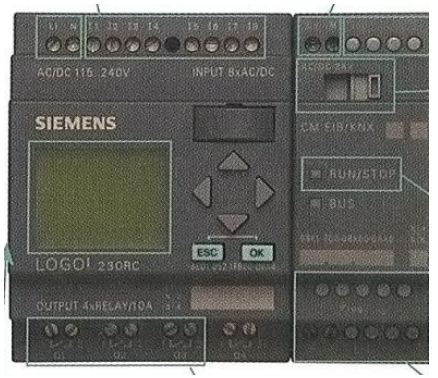
- **Un autómata programable es un sistema electrónico programable diseñado para el control de procesos y máquinas**
- **Destaca por:**
  - La gestión de las entradas y salidas, digitales y analógicas
  - Facilitar operaciones específicas como lógica combinacional y secuencial, temporización, recuento y funciones aritméticas.

AUTÓMATAS PROGRAMABLES

- **Características básicas de un autómata programable:**
  - Robustez
    - Adaptado a entornos industriales hostiles
    - Diseñado para funcionar de forma continua durante años
  - Modularidad
  - Potente interfaz de Entrada/Salida
    - Las entradas son los canales que le permiten adquirir señales al autómata, unas de mando y otras de realimentación (sensores)
    - Las salidas son los canales que permiten al PLC enviar órdenes a los actuadores del proceso e información de estado al sistema de supervisión
  - Determinismo
  - Software estable y de arranque rápido

AUTÓMATAS PROGRAMABLES

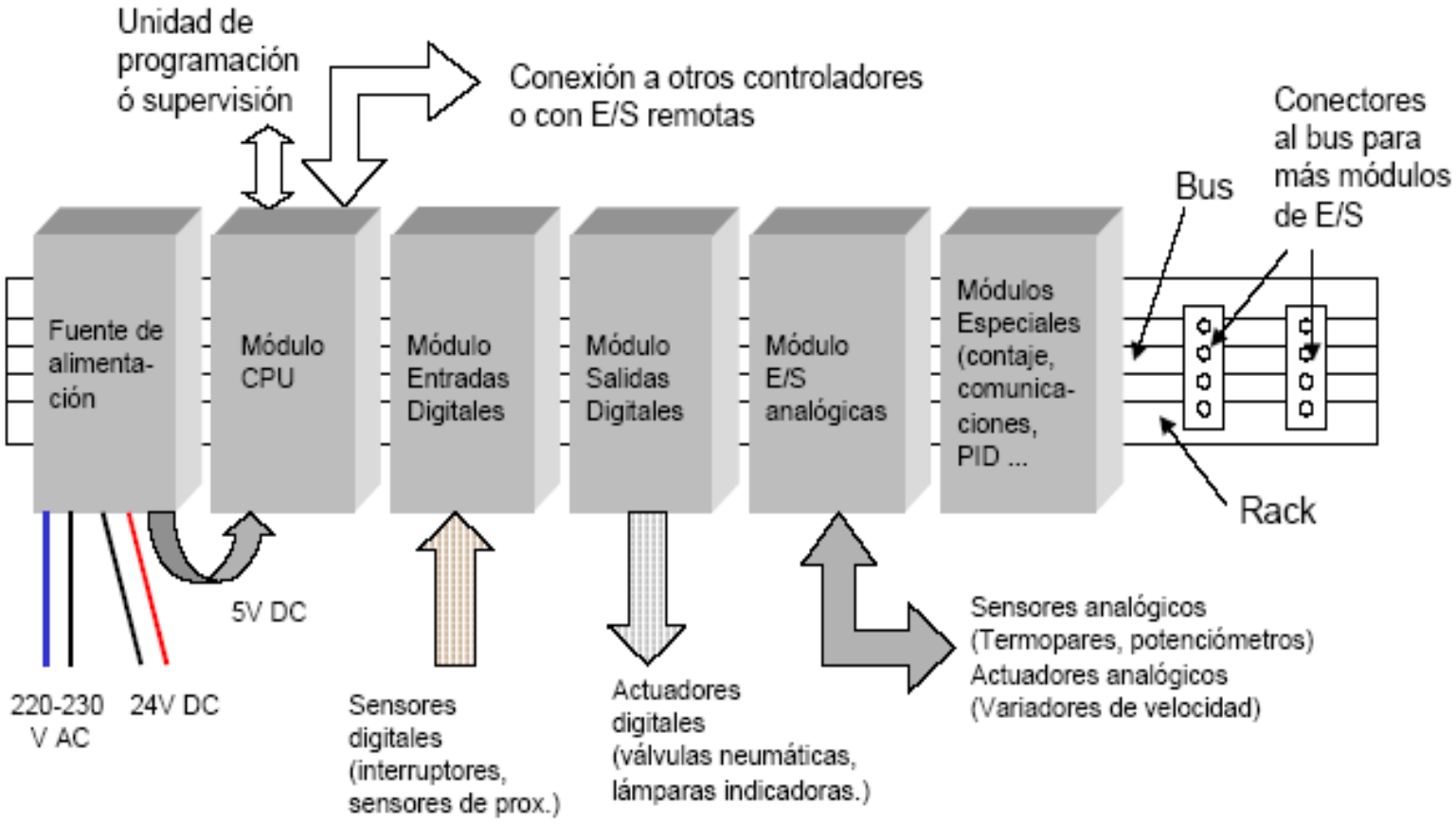
- **Tipos de autómatas programables:**
  - Microautómatas o autómatas compactos



  - Autómatas modulares

AUTÓMATAS PROGRAMABLES

- **Arquitectura típica de un autómata programable modular**



AUTÓMATAS PROGRAMABLES

- **Funcionamiento:**
  - Cuando el PLC está en modo de ejecución, el programa de control se ejecuta de manera indefinida
  - Esa ejecución es cíclica, describiendo lo que se ha dado en llamar “Ciclo de Scan”:
    - Lectura de las entradas del PLC, que a partir de este instante trabajará con una “imagen” en memoria hasta el próximo ciclo
    - Ejecución del programa de control almacenado en la memoria del PLC, de forma secuencial aunque no necesariamente lineal
    - Escritura en las salidas del PLC
    - Tareas internas del PLC, de comprobación de errores, almacenamiento de información interna, etc.

AUTÓMATAS PROGRAMABLES

- **PERIFERIA**
  - Módulos de E/S remotos que suponen una alternativa a la conexión directa de entradas y salidas al PLC
  - Generalmente cableados a transmisores y actuadores
  - Conectados con el autómata por medio de un bus de campo
  - Actúan simplemente como esclavos del PLC principal

SISTEMAS DE CONTROL DISTRIBUIDO

- **Conjunto de dispositivos que se comunican entre sí para controlar de forma coordinada un proceso productivo generalmente extenso**
- **Cada equipo dispone de autonomía propia y sólo intercambian los datos necesarios para el control y supervisión del proceso.**
- **Incorporan funcionalidades adicionales como:**
  - gestión de eventos y alarmas del proceso (cubren en parte el nivel de supervisión),
  - optimización de recursos,
  - control de activos (para un mantenimiento programado) y reemplazo en caliente de módulos
- **Ámbito de utilización típico: instalaciones industriales con gran cantidad de procesos interrelacionados, como en la industria petroquímica**

SISTEMAS DE CONTROL DISTRIBUIDO

Fuente: José Carlos Villaluca

UNIDADES TERMINALES REMOTAS

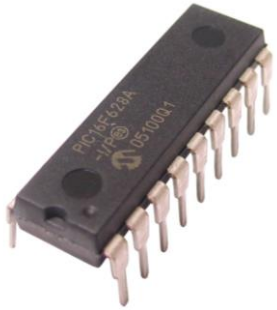
- **Los RTUs son dispositivos diseñados para la adquisición y transmisión de datos a un sistema de control remoto**
- **Se encuentran situados en emplazamientos remotos y permiten el control de la planta desde una localización centralizada**
- **Elemento típico en instalaciones de distribución y suministro de electricidad, agua, etc.**
- **Es habitual la capacidad simultánea de comunicación por diferentes medios físicos**
- **También se utilizan para la concentración de datos y la conversión de protocolos**

PCS INDUSTRIALES

- **Mayor flexibilidad y facilidad de ampliación**
- **Aprovechar la potencia de la CPU de un computador**
  - Virtualización
  - Algoritmos avanzados
  - Posibilidad de comunicar en diversos protocolos por software
- **Es necesario que sea robusto y que incorpore potentes interfaces de E/S**
- **Más inaccesible para personal con baja formación**

MICROCONTROLADORES Y MÁQUINAS DEDICADAS

- **Microcontroladores**
  - Para el control de ciertas máquinas se utilizan sistemas embebidos, es decir, sistemas informáticos con una función dedicada
  - Están optimizado para coordinar el flujo de información entre la memoria y la periferia
  - Bajo coste y reducido tamaño
  - No muy potentes, pero lo suficiente para, cada vez más, permitir funcionalidad “IoT”



- **Máquinas dedicadas**
  - Robots
  - Máquinas tipo CNC (Control numérico computerizado), también denominadas "máquinas-herramienta

ELEMENTOS DE SUPERVISIÓN

ERP

N. Planificación

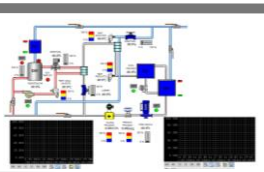
MES, Historian

Nivel de Gestión

Comunicación

SCADAs HMIs

Nivel de Supervisión



PLCs DCSs RTUs

Nivel de Control

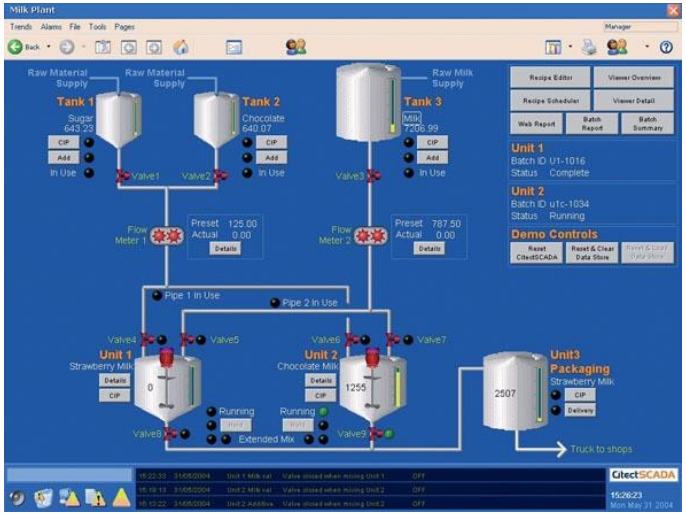
Sensores Actuadores

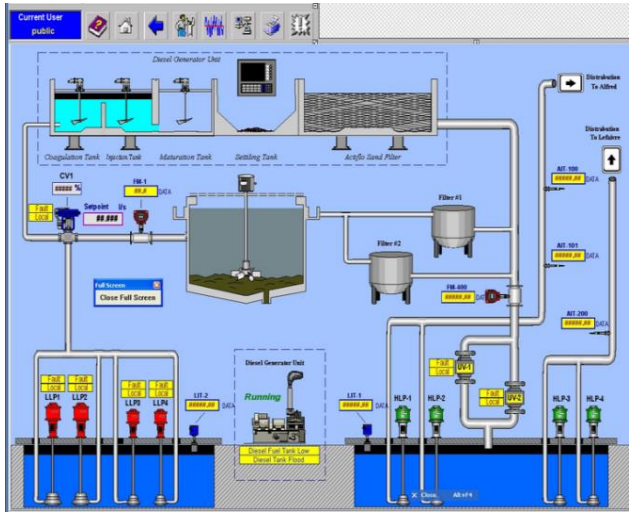
Nivel de Campo

Comunicación

SCADA

- ***Supervisory Control And Data Adquisition***
  - Software especializado para la monitorización en tiempo real de procesos industriales mediante una interfaz gráfica
  - También permiten el control remoto de instalaciones y equipos
  - En otros ámbitos, *Building/Energy/… management system*
  - Diferentes arquitecturas: *stand-alone*, cliente servidor, …

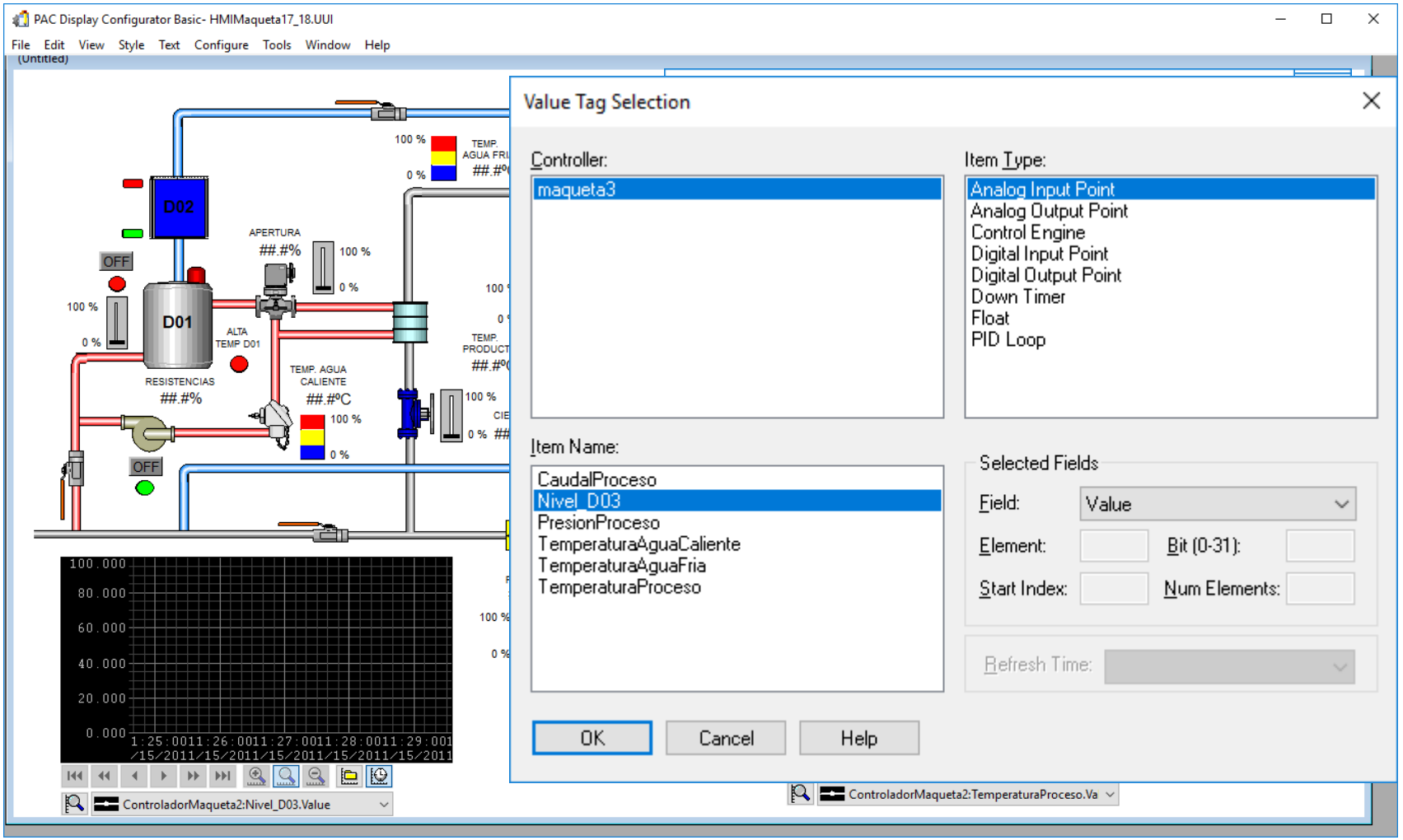




SCADA

- **Funciones principales:**
  - **Supervisión remota de instalaciones y equipos:** permite conocer el estado, detectar fallos y registrar estadísticas
  - **Control remoto de instalaciones y equipos:**
    - Se pueden enviar consignas, por ejemplo para activar o desactivar los equipos, de manera automática o manual
    - Es posible ajustar/reprogramar parámetros, valores de referencia, algoritmos de control, etc.
  - **Procesamiento y almacenamiento de datos:** que se pueden analizar y comparar con los anteriores o con otras referencias
  - **Visualización gráfica:**
    - Imágenes en movimiento que representan de forma esquemática el comportamiento del proceso
    - Gráficas de evolución
    - Representación de señales de alarma

SCADA


PAC Display Configurator Basic- HMIMaqueta17_18.UUI
File Edit View Style Text Configure Tools Window Help
(Untitled)
D02
D01
OFF
APERTURA
##.#%
RESISTENCIAS
##.#%
ALTA TEMP D01
TEMP. AGUA CALIENTE
##.#ºC
TEMP. PRODUCT
100 %
0 %
100.000
80.000
60.000
40.000
20.000
0.000
ControladorMaqueta2:Nivel_D03.Value
ControladorMaqueta2:TemperaturaProceso.Va
Value Tag Selection
Controller:
maqueta3
Item Type:
Analog Input Point
Analog Output Point
Control Engine
Digital Input Point
Digital Output Point
Down Timer
Float
PID Loop
Item Name:
CaudalProceso
Nivel_D03
PresionProceso
TemperaturaAguaCaliente
TemperaturaAguaFria
TemperaturaProceso
Selected Fields
Field:
Value
Element:
Bit (0-31):
Start Index:
Num Elements:
Refresh Time:
OK
Cancel
Help

HMI

- **Interfaces hombre-máquina o paneles de supervisión y control**
- **Dispositivos que permiten la visualización rápida de las variables del sistema industrial, las alarmas o introducción de consignas**
- **Se trata esencialmente de un sistema SCADA limitado y local, para cuya configuración se utiliza generalmente un software similar pero más flexible y restringido**
- **La pérdida de su operatividad conllevaría la falta de visibilidad del proceso.**

COMUNICACIONES: BUSES DE CAMPO

- **Inicialmente, se usaban solamente conexiones punto a punto entre los elementos de campo y los PLCs, que se comunicaban mediante señales analógicas (niveles de tensión/ corriente)**
- **Se ha evolucionado a utilizar en mayor medida un único medio de transmisión para comunicarlos: el BUS DE CAMPO**
- **Se trata de una comunicación digital en serie, utilizando unas ciertas características determinadas por una pila de protocolos**
- **Generalmente: tramas pequeñas y periódicas, bajas latencias, determinismo**

COMUNICACIONES: BUSES DE CAMPO

- **La implantación de buses de campo ha supuesto:**
  - Modularidad y mejora de prestaciones por la descentralización de dispositivos inteligentes
  - Ahorro y mejoras en mantenimiento por la supresión de cableado
  - Interconexión de equipos heterogéneos
  - Acceso fácil/rápido a la información. Integración con otros sistemas

- **Los protocolos utilizados en los buses de campo generalmente no son enrutables, ya que solamente implementan los niveles 1, 2 y 7 de OSI**

- **Diversas tecnologías compiten por el mercado, pero son generalmente estándares abiertos: IEC 61158, IEC 61784**

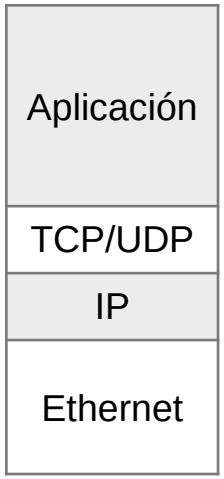
COMUNICACIONES: BUSES DE CAMPO

- La capa física más habitual es el par trenzado, aunque en ocasiones podría utilizarse cable coaxial, fibra óptica o comunicación inalámbrica

- RS-485 es una configuración muy extendida en buses de campo, ya que permite una conexión multipunto
- No obstante, también se utilizan en algunos casos RS-232 o USB (para las conexiones punto a punto) u otras capas físicas específicas (p. ejemplo, es el caso de ASI)

COMUNICACIONES: PROTOCOLOS INDUSTRIALES A NIVEL DE CONTROL

- **Generalmente sobre TCP/IP y por tanto enrutables**
  - Mensajes generalmente no periódicos y más grandes que a nivel de campo
  - Requisitos de tiempos menos estrictos



- **Por lo general, para cada familia de protocolos de automatización, se suelen definir protocolos para el bus de campo y el nivel de control**
- **En algunos casos, el protocolo de nivel de control se limita a encapsular las tramas del protocolo de bus de campo en paquetes TCP/IP**

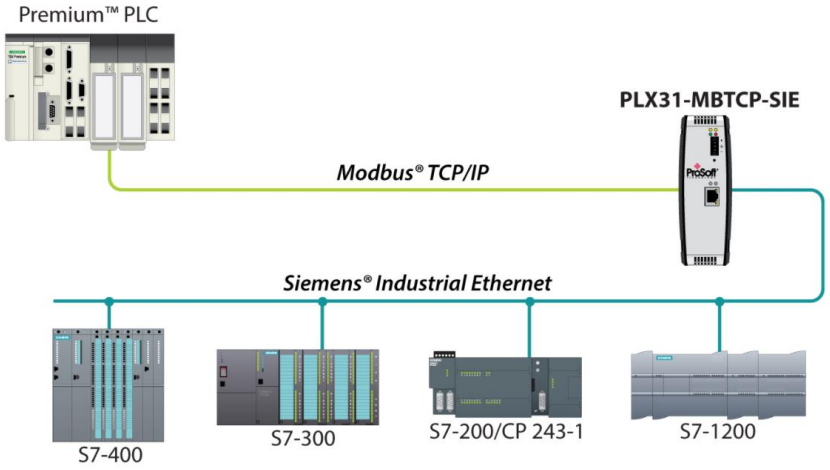
ELEMENTOS DE COMUNICACIÓN

- ***Switches* industriales**
  - Deben cumplir unas condiciones de robustez
  - Generalmente un número reducido de puertos
  - Pueden implementar protocolos de redundancia que garantizan la llegada de los mensajes ante el fallo de un nodo en una topología en anillo:
    - PRP (*Parallel Redundancy Protocol*), MRP (*Media Redundancy Protocol*) o HSR (*High-availability Seamless Redundancy*)

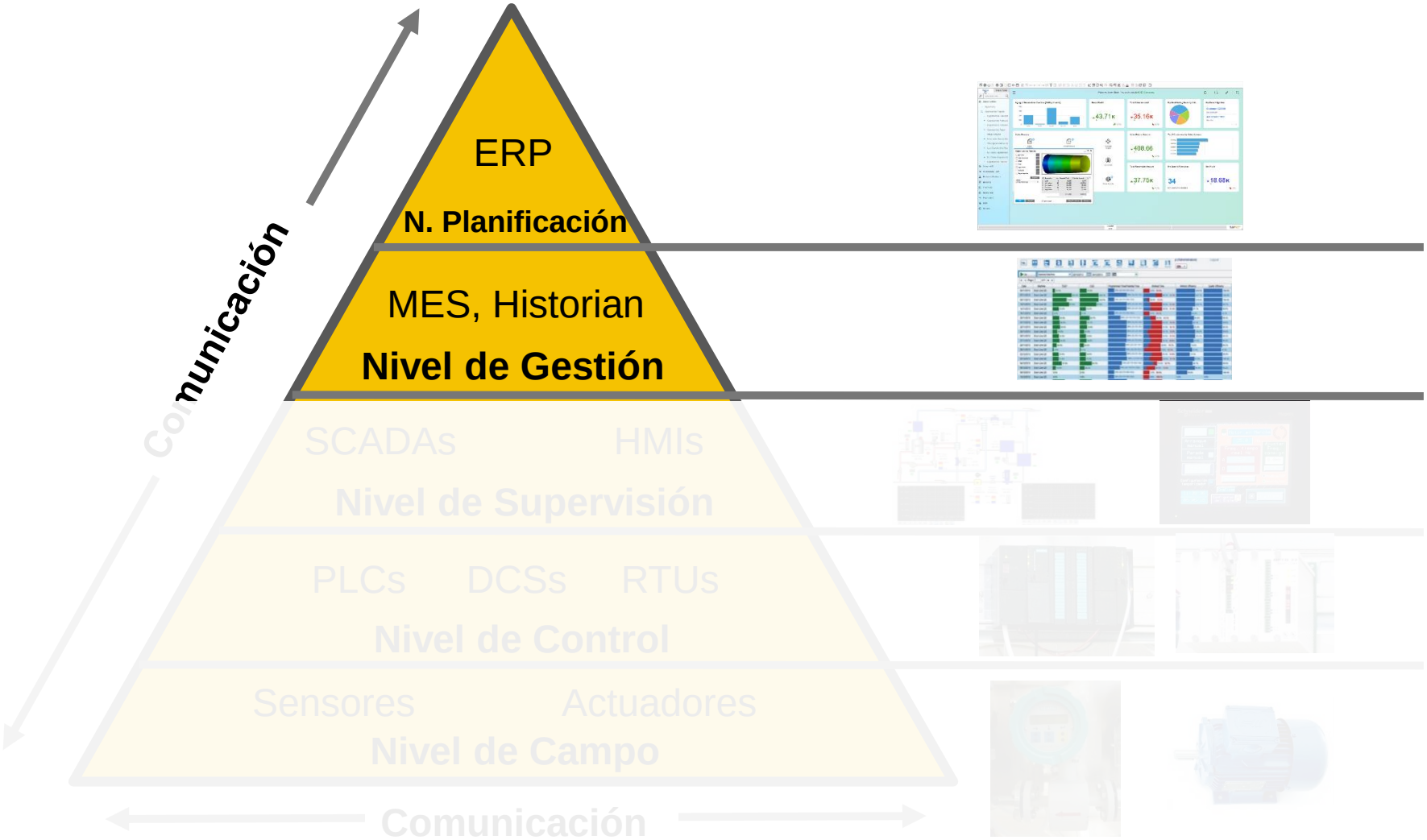
- ***Routers* industriales**
  - De nuevo, deben ser dispositivos robustos
  - Cada vez más incorporan opciones de seguridad, como la posibilidad de realizar túneles VPN

ELEMENTOS DE COMUNICACIÓN

- **Pasarelas de comunicación:**
  - Permiten adaptar diferentes medios físicos o protocolos a capas superiores para establecer una comunicación
  - A menudo se usan para aumentar la distancia útil o unir diferentes segmentos serie remotos por medio de una red TCP/IP

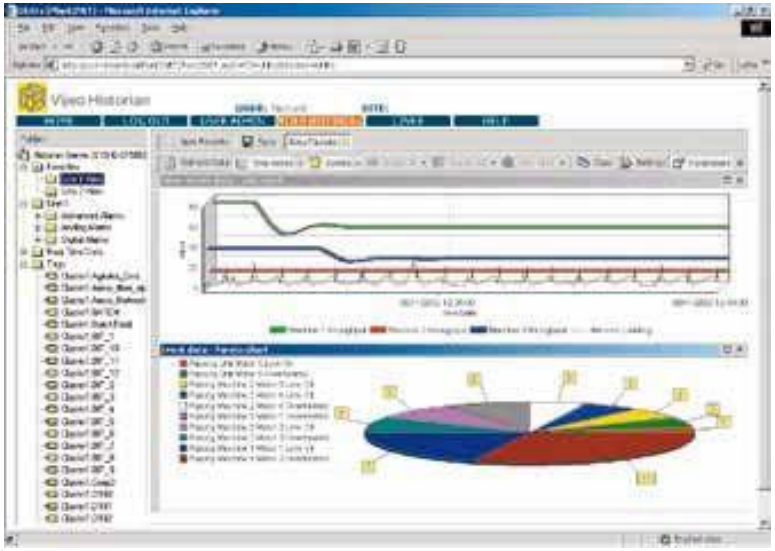


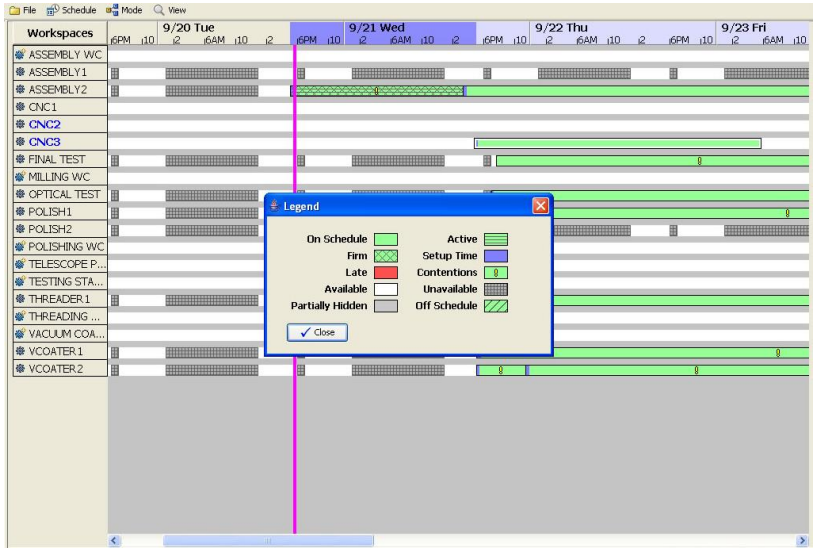
ELEMENTOS DE GESTIÓN Y PLANIFICACIÓN



ELEMENTOS DE GESTIÓN

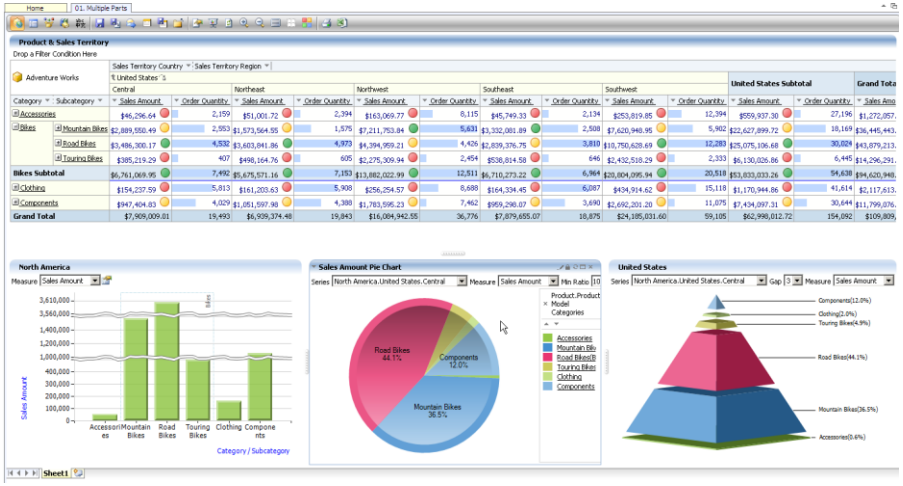
- **Historizador o gestor de históricos:**
  - Software específico que salvaguarda todos los datos y estados del proceso para permitir su estudio *off-line*, la generación de informes, etc.
  - Pueden manejar grandes volúmenes de información
- **MES (*Manufacturing Execution System*)**
  - Gestión y optimización de la actividad de la industria





ELEMENTOS DE PLANIFICACIÓN

- ***Enterprise Resource Planning***
  - Sistemas de planificación de recursos empresariales que fusionan la información proporcionada por el MES con otros aspectos necesarios para la gestión de la empresa (logística, inventario, contabilidad, etc.)
  - A menudo proporcionan herramientas de *Business Intelligence* orientadas al procesamiento de los datos para la obtención de conocimiento utilizando análisis estadístico, minería de datos, etc.



DUALIDAD SEGURIDAD OPERACIONAL-CIBERSEGURIDAD

- **Los programas de ciberseguridad en sistemas de control deben integrarse en programas más amplios que también consideren la seguridad física y la seguridad operacional**
- **La ciberseguridad es, a día de hoy, esencial para la operación segura y confinable de cualquier proceso**

- **Se debe trabajar para alcanzar, en el ámbito de la ciberseguridad, niveles semejantes de sistematización a los que se utilizan en seguridad operacional:**
  - Métodos de detección, evaluación y mitigación de riesgos
  - Definición de niveles de seguridad aceptables y de indicadores de desviación,…
  - Capacidad de trabajar aún en modo degradado ante un fallo