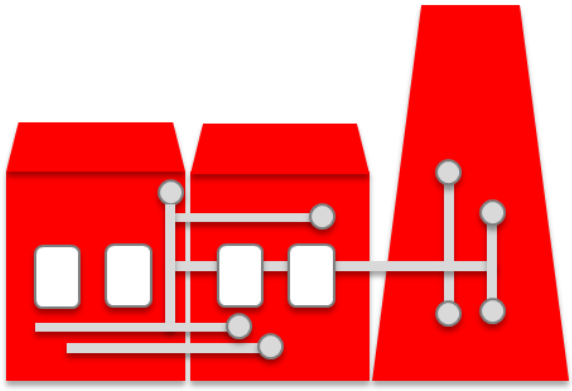
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

TEMA 1. INTRODUCCIÓN A LOS SISTEMAS DE CONTROL Y AUTOMATIZACIÓN Y A LA PROBLEMÁTICA DE SEGURIDAD ASOCIADA

1.1. Evolución histórica y tendencias actuales



Curso avanzado de ciberseguridad en sistemas de control y automatización industrial

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1.1. EVOLUCIÓN HISTÓRICA Y TENDENCIAS ACTUALES

1.1.1 Historia de la automatización. Primeras máquinas

Desde hace siglos, el hombre ha ido construyendo máquinas que facilitasen su trabajo o aumentaran su productividad, realizando trabajos repetitivos o en los que requirieran gran fuerza física.

Hasta la generalización del uso de la electricidad, dichas máquinas fueron aumentando en complejidad mecánica. Palancas, poleas, correas o ruedas dentadas transformaban movimientos de las diferentes partes de la máquina para crear la acción deseada. Ejemplos de este tipo de maquinaria se encuentran principalmente con el desarrollo de la industria textil a finales del siglo XIX, o la máquina de vapor.

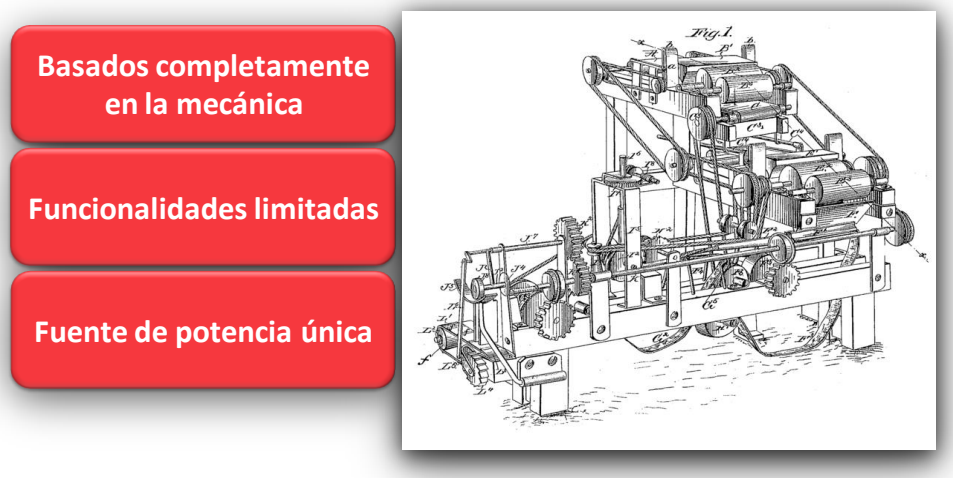


Figura 1. Historia de la Automatización: Máquina para confeccionar cigarros (Siglo XIX). Fuente: www.wikipedia.org

Dichas máquinas, basadas únicamente en la mecánica contaban con una funcionalidad fija y limitada con una sola fuente de potencia (hidráulica, vapor, tracción animal).

1.1.2 Época – Pre PLCs, llegada de la electricidad

El uso de la electricidad no sólo mejoró la generación de potencia para las máquinas, si no que introdujo las bases del control industrial. Contactos accionados por la propia mecánica de la máquina actuaban sobre motores, actuadores… Esta tecnología electromecánica fue ampliándose con la aparición de multitud de componentes individuales que ofrecían nuevas funcionalidades: relés multicontacto, contactores, temporizadores, cajas de levas…

Gracias a estos componentes ya era posible diseñar secuencias de eventos complejos pero que en la práctica simplificaban el diseño mecánico de las instalaciones. Por ejemplo, en la Figura 2 se puede ver cómo, para una sola secuencia de arrancar y parar un

motor con dos pulsadores, se necesitaba un relé de dos circuitos, con un cableado relativamente complejo para una sola actuación.

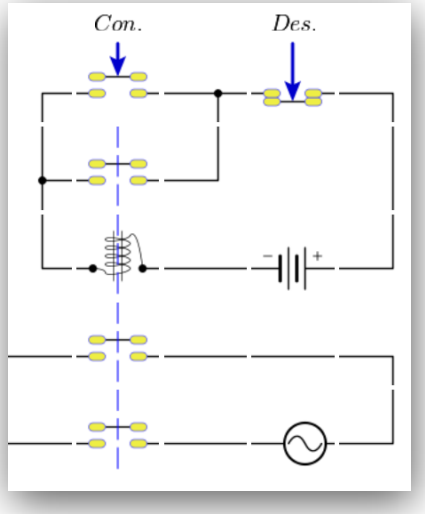


Figura 2. Circuito pulsador Marcha/Paro.
Fuente: www.wikipedia.org

Como se puede ver en la Figura 3, los controles industriales resultantes de esta tecnología estaban compuestos por multitud de pequeños componentes electromecánicos unidos por un cableado complejo. Esto dificultaba enormemente su modificación y mantenimiento.

Figura 3. Época Pre-PLCs.
Fuente: www.wikipedia.org

En este aspecto, la monitorización de las instalaciones se realizaba a través de pilotos, indicadores de aguja, contadores con historizaciones manuales o basados en impresoras de papel continuo.

La monitorización a base de elementos discretos como los indicados anteriormente ha subsistido en el tiempo hasta hace unos pocos años mediante sinópticos de gran tamaño, típicamente en centrales nucleares e infraestructuras.

1.1.3 Hito histórico: Primer PLC- 1970

A instancias de la industria automovilística americana, partió la iniciativa para el diseño de un control programable multiuso que pudiera simplificar el diseño de cuadros eléctricos: una CPU que actuara sobre salidas según un programa preestablecido y los datos proporcionados por las entradas.

Figura 4. Primer PLC. Modicon 084.
Fuente: Lundu University

Es así como, en 1970, aparece el primer PLC (*Programmable Logic Controller*), el MODICON 084. También llamado en español "Autómata Programable", el PLC es un controlador que permite ejecutar programas que tiene como inputs señales eléctricas provenientes de la instalación a controlar y como outputs salidas digitales o analógicas que activan elementos de la misma como motores, válvulas o resistencias.

Las posibilidades de programación del MODICON 084 eran bastante limitadas. La escritura del programa se realizaba a través de un pequeño teclado y un *display* numérico mediante el lenguaje *ladder* (por su semejanza con una escalera de mano, *ladder* en inglés) que intentaba emular los circuitos eléctricos utilizados hasta el momento.

1.1.4 PLC – Características básicas

Las características básicas de ese PLC inicial y que, en general, todavía mantienen todos los dispositivos de campo en la automatización industrial son:

- Robustez: adaptadas para entorno industrial con temperaturas altas, humedad, polvo…
- Arranque rápido: la carga del S.O. y del programa se produce en unos pocos segundos.
- Estabilidad *software*: normalmente con sistema operativo propio, con pocas actualizaciones y diseñado primando la estabilidad software sobre la rapidez de proceso.
- Sin piezas móviles: sin dependencia de discos duros, lectores de CD o componentes susceptibles de avería mecánica.

Figura 5. Resumen características dispositivos de control industrial.

1.1.5 Automatización industrial – Evolución histórica

A partir del hito de la aparición del PLC Modicon 084, la automatización y el control industrial han avanzado ininterrumpidamente saliendo al mercado infinidad de dispositivos y soluciones que abarcan todos los campos de actuación; desde pequeñas unidades con una sencilla configuración, a unidades modulares con inteligencia distribuida capaces de controlar decenas de miles de entradas/ salidas. Aunque se ha centrado el revulsivo en la automatización industria en la aparición del PLC; no se centra sólo en ellos, sino que existen otros dispositivos, aplicaciones o soluciones como RTUs[1], SCADAs[2], DCS[3], EMS[4], MES[5],…, con diferentes funcionalidades como la recogida de datos, control, visualización, *tracking*, que se irán viendo más adelante.

Las capacidades de los dispositivos también han aumentado de una forma exponencial, tanto en cálculo y rapidez, disminuyendo el tiempo de ciclo de ejecución del programa desde unas décimas de segundo a milisegundos; como instaurando nuevas posibilidades

[1] *Remote Terminal Unit*. Unidad terminal remota o unidad de telemetría remota.

[2] *Supervisory Control and Data Acquisition.* Control por supervisión y adquisición de datos.

[3] *Distributed Control System.* Sistema de control distribuido.

[4] *Energy Management System*. Sistema de gestión de la energía.

[5] *Manufacturing Execution System*. Sistema de ejecución de fabricación.

de programación, con nuevos lenguajes de programación; y especialmente en conectividad, sustituyendo los clásicos puertos serie RS-232 por puertos Ethernet o USB.

A continuación, se citan algunos ejemplos de instalaciones automatizadas aumentando en cada caso la complejidad de las prestaciones y, por tanto, las de la solución de control:

- **Montacargas:** un PLC compacto controla, a través de pulsadores y detectores el destino, la posición de las puertas y la posición del montacargas activando las correspondientes salidas de alimentación de motores y pilotos. El motor principal del montacargas es controlado por un variador de frecuencia con funcionamiento autónomo.
- **Máquina de envasado pequeña:** un PLC compacto controla a través de sus entradas y salidas el proceso de envasado. Monitorización a través de una pantalla de operador HMI (*Human Machine Interface*).
- **Depuradora de aguas residuales:** PLC modular con entradas y salidas e instrumentación conectada a través de un bus de campo. Monitorización a través de un programa SCADA.
- **Depuradora de aguas potables:** pareja de PLCs con redundancia de proceso y entradas y salidas a través de buses de campo. Monitorización a través de un programa SCADA. Algunos depósitos remotos se controlan a través de RTUs que transmiten los datos al control central.
- **Línea de envasado de refrescos:** un PLC modular por máquina individual (lavadora de botellas, llenadora, etiquetadora, paletizadora…), que intercambia datos de proceso con los PLCs de las otras máquinas. La monitorización de alarmas se realiza a través de pantallas HMI. Monitorización general del proceso a través de un PC con un programa SCADA y conexión a un sistema MES para control de producción y tiempos de paro de máquina.
- **Planta química:** Un control DCS, que integra en un mismo conjunto diferentes dispositivos de control, instrumentación y control de producción, gestiona todos los aspectos de la automatización: parametrización de dispositivos, control del proceso, recetas, lotes de producción, trazabilidad…

Los diferentes elementos citados en estos ejemplos serán tratados con mayor profundidad en capítulos posteriores.

Los ejemplos anteriores solo muestran un pequeño ámbito de los entornos donde podemos encontrar elementos de automatización industrial.

Hoy en día cualquier proceso productivo o maquinaria es susceptible de incorporar dispositivos de control: desde una empresa de manufactura con producción discreta, como por ejemplo la automovilística; la basada en procesos continuos, como la química o farmacéutica; el control de infraestructuras como plantas potabilizadoras o depuradoras de aguas; La distribución de electricidad agua, gas, o electricidad o en grandes instalaciones como parques de atracciones, aeropuertos o control de edificios.

Figura 6. Automatización industrial – Evolución histórica.

El ámbito de aplicación de la automatización industrial se extiende a todos los sectores industriales e infraestructuras con diferentes soluciones tecnológicas dependiendo del tamaño, complejidad o prestaciones demandadas por la instalación.

1.1.6 Clasificación según la norma ISA-95

Para presentar mejor todos estos elementos se va a utilizar la clasificación realizada por la "*International Society of Automation*" (ISA), organismo que agrupa a más de 30 mil miembros con el objetivo de delimitar los principales estándares industriales, en su norma ISA-95 que regula la automatización industrial.

Figura 7. Norma ISA-95.

Para más información:
International Society of Automation
https://www.isa.org/
http://online.wsj.com/news/articles/SB123914805204099085

1.1.7 Niveles ISA-95

La ISA-95 define 5 niveles de operaciones en la automatización industrial:

- **Nivel 0:** el propio proceso productivo.
- **Nivel 1:** los propios dispositivos que procesan y manipulan el producto en sí (robots, actuadores, instrumentación). Normalmente los dispositivos PLCs y DCS se incluyen en este nivel aunque, dependiendo del grado de automatización de una organización, también es frecuente que se ubiquen en el siguiente nivel. Los DCS se ubican en este nivel, ya que combinan tecnologías de control (los propios controladores) con el software de supervisión ligado a dichos controladores de proceso.
- **Nivel 2:** los dispositivos que monitorizan y controlan el proceso productivo (HMI, SCADAs).
- **Nivel 3:** los dispositivos que controlan el *work flow* y las recetas[6] del proceso productivo y que almacenan toda la información sobre el mismo (MES, Batch, Historian, LIMS [7]).
- **Nivel 4:** el nivel que contiene la infraestructura de logística, inventario, ERP [8] o planificación.

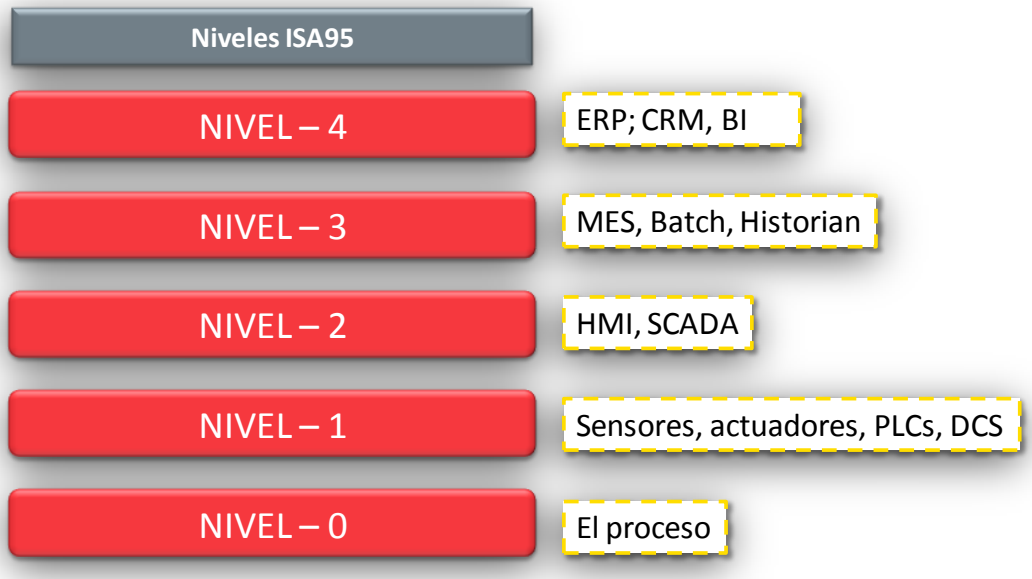


Figura 8. Niveles ISA-95

1.1.7.1 Nivel 0

Engloba el propio proceso productivo.

[6] Recetas: Conjunto de parámetros y procesos necesarios para la producción de un producto y que lo diferencian de otro producido con la misma instalación.

[7] LIM: Laboratory Information Management System.

[8] ERP: *Enterprise Resource Planning.*

1.1.7.2 Nivel 1

En este nivel se encuentran los elementos que adquieren los datos de planta y los que actúan sobre la cadena. Dependiendo de su complejidad, pueden disponer de una sencilla conexión a la entrada de un PLC; como por ejemplo, un simple pulsador, o necesitar de una compleja parametrización vía un bus de campo, como un sensor de presión avanzado. Dentro del apartado de sensórica se pueden encontrar dispositivos para la medida de cualquier unidad: niveles de líquido en un tanque, temperaturas del producto en un reactor, presión del aire en el circuito, luminosidad, caudal, presencia de impurezas. El coste de la instrumentación utilizada en una instalación industrial, como en el caso de una planta química, puede ser muy superior al de los dispositivos de control.

Figura 9. Instrumento para el control de temperatura.

A este nivel también pertenecen los PLCs y DCS que mediante programas de control procesan los datos de entrada. Mientras que los PLCs son dispositivos compactos, los DCS suelen disponer de una arquitectura distribuida con diferentes CPUs de control.

Los dispositivos de este nivel requieren de una programación específica. En su diseño prima la robustez contra las duras condiciones ambientales de la industria.

Figura 10. PLC compacto.

También se incluyen en este nivel las RTUs que permiten la adquisición remota de datos para traspasarlos a los elementos de Nivel 2.

Figura 11. RTU con múltiples opciones de comunicación.

1.1.7.3 Nivel 2

Aunque ya se ha citado que se pueden encontrar PLCs en este nivel, habitualmente el nivel 2 se identifica con la capa de supervisión y control de proceso, bien localmente (es decir, desde los interfaces de operador que incluyen las máquinas) como centralizadamente (a través de centros de control que se construyen sobre lo que se llama soluciones SCADA).

Cuando se realiza una supervisión y control local, se utilizan normalmente las pantallas HMI. Aparatos compactos para la visualización de procesos.

Figura 10. Pantalla HMI de 5.4 pulgadas.

Cuando se realiza una supervisión centralizada, se utilizan los programas SCADA, con base en ordenadores, que además de la simple visualización del proceso de los HMI pueden incorporar funcionalidades avanzadas como *Data Logging*, control de alarmas, gestión de usuarios o comunicación con los sistemas del siguiente nivel.

1.1.7.4 Nivel 3

Desde este nivel se controla el flujo de la producción, recetas y cantidades. También el almacenamiento de la información de producción como lotes, trazabilidad, productividad, calidad… Se sitúan en este nivel los controladores *Batch*, que realizan parte del control del proceso de recetas, principalmente en industrias químicas y farmacéuticas.

Figura 11. PCs en control industrial.

1.1.7.5 Nivel 4

Este nivel corresponde al nivel más alto de la gestión, controlando la programación de la producción de una o varias plantas de una empresa, el uso de materiales, inventario y logística. Desde este nivel, la dirección ejecutiva obtiene una visión general del funcionamiento de las mismas a todos los niveles (eficiencia, económicos, logísticos) de forma que puede tomar las decisiones oportunas sobre su funcionamiento.

1.1.8 Comunicación entre niveles

La comunicación entre los diferentes niveles y elementos se realiza a través de diversos medios físicos, protocolos y estilos de integración. Algunos ejemplos de estos protocolos, que se analizarán con detalle en próximos capítulos, son: Profibus, que proporciona su propio *hardware* de transmisión para comunicar entradas y salidas remotas con el PLC; Modbus, soportado por diferentes medios (RS-232. RS-485, encapsulado TCP) para una comunicación entre PLC y SCADA o, en el caso de los estilos de integración, la que se realiza mediante *middleware* orientado a mensajes (MOM) o servicios (SOA). En capítulos posteriores se profundizará sobre los diferentes medios de comunicación, tanto físicos como lógicos que se encuentran dentro de un proceso de automatización industrial: desde los protocolos de comunicación entre la instrumentación y los PLCs, como Profibus o Ethercat; hasta los protocolos de comunicación entre PLCs y SCADAs, como OPC (que también puede utilizarse para integrar información entre los niveles 2, 3 y 4) o los propietarios de cada fabricante (S7 messaging, Ethelway, Controlnet, etc.).

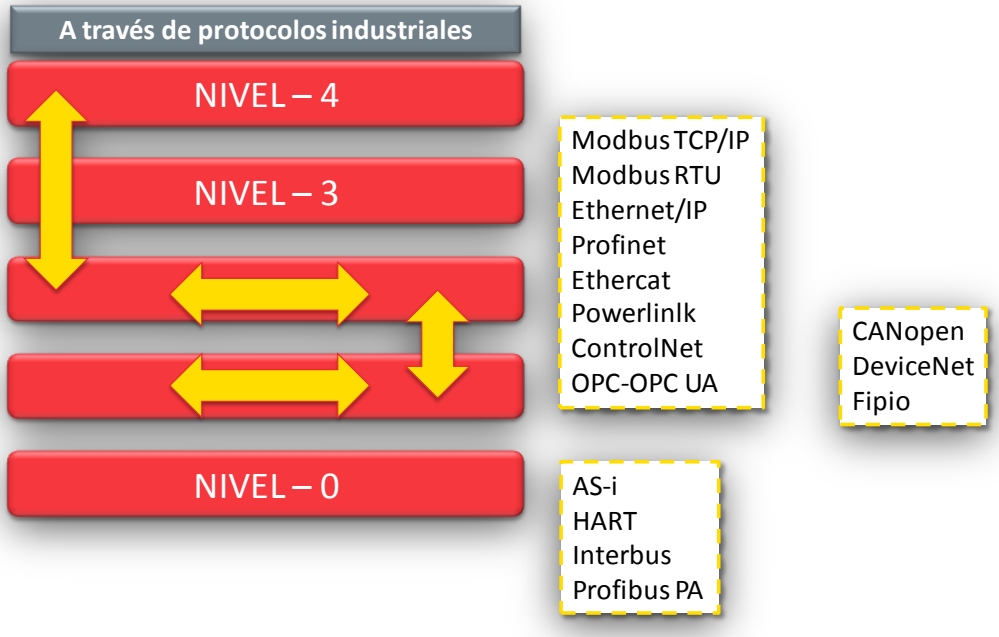


Figura 12. Protocolos industriales.

En el capítulo 3 de este curso profundizaremos sobre los diferentes protocolos utilizados dentro del entorno industrial y su ámbito de aplicación.

REFERENCIAS TÉCNICAS

PLCs y pantallas

http://www.automation.siemens.com/

Clasificación ISA

http://www.isa-spain.org/

Modicon 084 historia

http://www.plcdev.com/schneider_electric_modicon_history

Programas SCADA

http://www.isa-spain.org/

http://www.wonderware.es/

Autómatas programables y sistemas de automatización. Enrique Mandado y otros. Editorial Marcombo. ISBN: 9788426715753

http://www.marcombo.com/Automatas-programables-y-sistemas-de-automatizacion_isbn9788426715753.html

INSTITUTO NACIONAL DE CIBERSEGURIDAD