Tema 2

Industrial Control System

También conocidos como ICS e IACS son sistemas formados por equipos interconectados que controlan monitorizan y administran grandes sistemas de producción industrial. Algunas formas, de forma no muy correcta se usan como sinónimos:

- PCS (Process Control System) o PLC (Proglamable logic controller)
- DCS (Distributed control System)
- SCADA (Supervisory Control and DAta Acquisition system)

El ICS engloba todo lo aquí definido:

- ICS: Sistema de control que abarca todo esto.
- SCADA: Gran área geográfica
- DCS: Una sola ubicación
- PLC: Una unidad de proceso

PLC

Hardware embebido que controla localmente algún dispositivo, fueron creados para sustituir circuítos lógicos basados en relés. Se caracterizan por:

- Fáciles de programar
- Fáciles de mantener y reparar
- Pequeño Tamaño
- Se pueden comunicar con dispositivos de una planta industrial y con los sistemas remotos de control central

En la actualidad pueden hacer más cosas:

- Mayor potencia de procesamiento
- Soporte para entradas/salidas digitales y analogicas
- Implementan distintas variantes de lazos de control
- Soportes para nuevos protocolos de comunicación

Normalmente se usa un software especializado basado en una interfaz WYSIWYG en la que se pueden ir interconectando las distintas entradas y salidas.

SCADA

Capa de software por encima de los PLC que se limita a realizar tareas de supervisión (Aunque en la actualidad también pueden hacer tareas de control.). Las principales funcionalidades de un SCADA son:

- Adquisición de datos
- Presentación de datos a través de un HMI (Humam-Machine Interface) personalizado
- Control de sistemas dispersos geograficamente.

Los SCADA tienen varios componentes:

- RTU: Remote Terminal Unit, compuestos por sensores y actuadores.
  - Suelen estar dispersos geográficamente
  - No actualizan constantemente debido a que en los ambientes industriales hay muchas interferencias que pueden producir el envío de datos erróneos, por lo que solo suelen indicar al SCADA cambios de estado
  - Se suelen comunicar por protocolo profinet (Siemens) o profibus.

DCS

Similar a un SCADA, con la diferencia de que muestran datos en tiempo real.

Protocolos de comunicación

- SCADA: comunicación con los sitemas de supervisión
- FIELDBUS: Comunicación con sistemas de control
- ModBus: Modicon Communication Bus, protocolo más antiguo y extendido para ICS.
  - Abierto y gratutio
  - Nivel de aplicación
  - Comunicación en texto plano
  - Comunicaciones Request o Reply
  - Problemas de seguridad:
    - Ausencia de autenticación
    - Ausencia de cifrado
    - No hay mecanismos de supresión de broadcast (facilita los ataques DDOS)
    - Los mensajes permiten reprogramar los dispositivos