SCADA: OVERVIEW

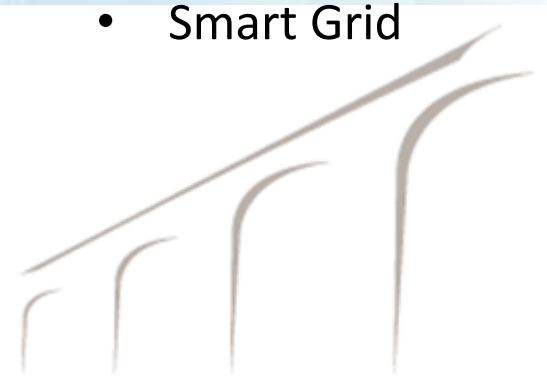
Dr. César Cárdenas
ccardena@itesm.mx

EVOLUCIÓN DEL INTERNET INDUSTRIAL

Dr. César Cárdenas
ccardena@itesm.mx

Agenda

- Redes de control industrial
- Redes comerciales vs. redes industriales
- Sistemas de control industrial
- Orígenes, evolución y tendencias
- Olas de Internet
- Smart Planet
- Internet Industrial
- Cyber-Physical Systems
- Smart Grid



Redes de Control Industrial

- Al inicio de la era industrial, el control de la manufactura y las plantas de procesos fue hecho de manera mecánica (**manual o hidráulico**).
- Luego los controles mecánicos fueron remplazados por lazos de **control electrónico** empleando transductores, relevadores y circuitos de control alambrados.
- Enseguida, los **controladores digitales** empezaron a sustituir los controles análogos aunque las comunicaciones al campo de trabajo seguía siendo mediante **señales análogas**.
- El movimiento hacia sistemas digitales demandó nuevos protocolos de comunicación en el campo de trabajo (llamados **protocolos de campo de trabajo o *fielbus protocols***) así como entre los microcontroladores.
- Más recientemente, los sistemas digitales de control incorporan **redes en todos los niveles** del control industrial, así como la interconexión de equipos de oficina y equipos industriales **usando el estándar Ethernet** por lo que los requisitos de estas últimas han cambiado.

Redes de Control Industrial

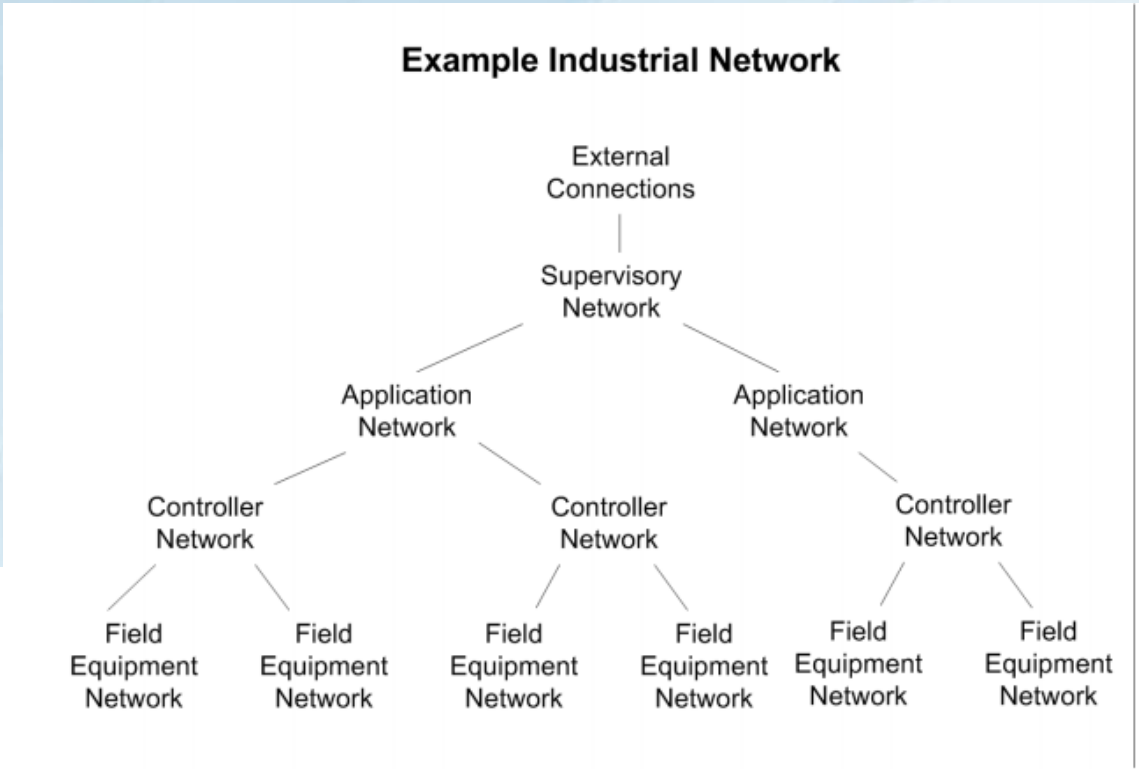
- La interconexión de equipo industrial (***industrial networking***) se refiere a la implementación de protocolos de comunicación entre equipo industrial, controladores digitales, herramientas computacionales y sistemas externos en el campo de trabajo.
- En la actualidad, las redes industriales son muy importantes para los sectores de **manufactura y generación de electricidad** pero también son usadas en las industrias de **alimentos, transporte, distribución de agua, petroléo y gas** entre otras.
  - Estas redes son altamente especializadas y usan varios protocolos que han sido adaptados para cumplir los estrictos requisitos para implementar control en tiempo real de equipo físico.
- Debido a la importancia de las redes industriales estás se han **empezado a integrar también con Internet**.
- **La principal diferencia entre las redes comerciales e industriales es que estas últimas se conectan a equipo físico y son usadas para controlar y monitorear acciones y condiciones de la realidad.**

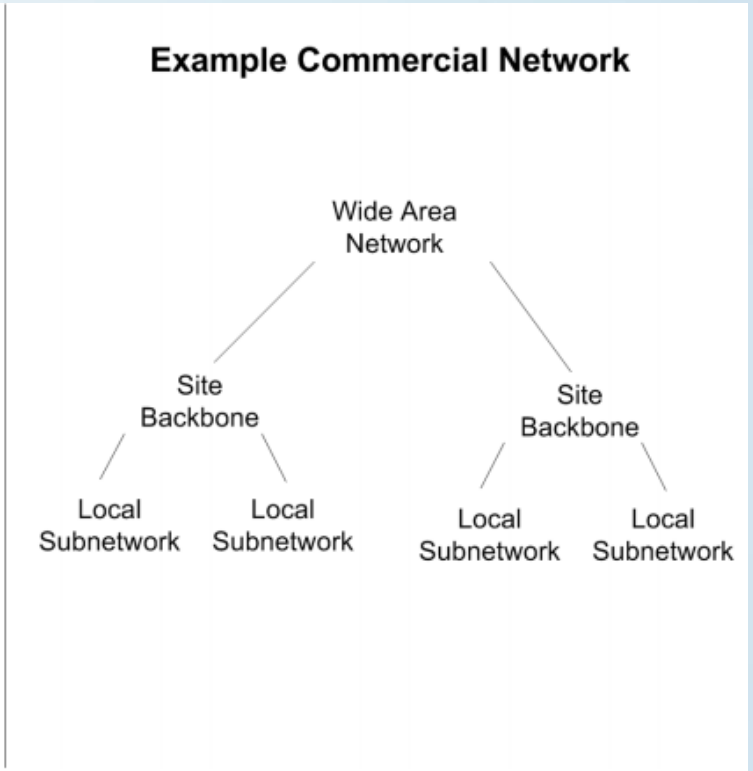
Redes de Control Industrial

- **La calidad de servicio (QoS) es muy diferente en las redes industriales.**
  - **Más aún si se integra con el tráfico de Internet.**
- Implementación:
  - Cada industria requiere su propio conjunto de pequeñas diferencias pero con requisitos muy similares los cuales pueden ser agrupados en los siguientes sectores:
    - **Manufactura discreta, control de procesos, automatización de edificios, distribución de servicios públicos (agua, gas, electricidad, etc.), transporte y sistemas embebidos**.
- Arquitectura:
  - Las redes industriales tienen una arquitectura más profunda (3 o 4 niveles) que las redes comerciales. **Primer nivel:** conexión entre instrumentos y controladores. **Segundo nivel:** interconexión de controladores. **Tercer nivel:** Interfaces Hombre-Máquina. **Cuarto nivel:** una red de recolección de datos y comunicaciones externas.

Redes de Control Industrial

- Las redes industriales son **muy heterogéneas y no muy planas**.



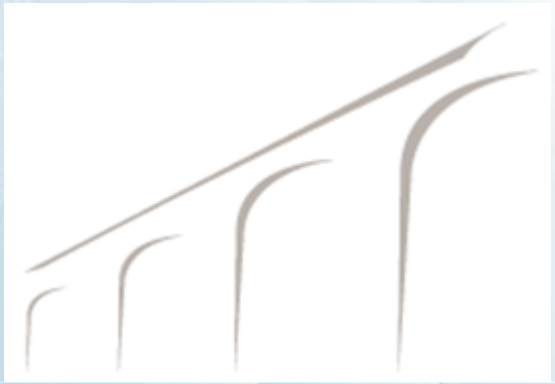


Redes de Control Industrial

- Requisitos de tiempo:
  - Regla general: **el tiempo de respuesta debe ser menor el tiempo de muestreo**.
  - Los **retrasos** en la entrega de la información pueden impactar de manera muy severa el **desempeño de los lazos de control**, especialmente en sistemas de control de lazo cerrado.
  - Las **jerarquías altas** de las redes industriales tienen casi los **mismos requisitos que las redes comerciales**.
- Determinismo
  - Las **variaciones en el tiempo impactan los controles de lazos cerrados**, especialmente las proporciones integrales y derivativas.
  - La telefonía por Internet requiere también de esta propiedad.
- Tamaño de paquetes
  - Especialmente **pequeños a jerarquías bajas**.
  - En Internet se tiene el efecto de “ratones y elefantes”.

Redes de Control Industrial

- Tipos de información en redes industriales:
  - **De control** (requerimientos de tiempo real y determinismo), **de diagnóstico o monitoreo** (requerimientos menores a la de control pero mantiene consistencia temporal y mínima pérdida de datos), y **de seguridad** (requiere de tiempo real y alta confiabilidad).



Redes Comerciales vs. Redes Industriales

	Industrial	Comercial
Función primaria	Control de equipo físico	Procesamiento y transferencia de datos
Dominio de aplicación	Manufactura, procesamiento y distribución de información para servicios públicos	Ambientes caseros y corporativos
Jerarquía	Profunda, jerarquías de funcionalidad separadas con muchos protocolos y estándares físicos	Superficial, jerarquías integradas con uniformidad de protocolos y uso de estándares físicos
Gravedad de fallas	Alta (ejemplo planta nuclear)	Baja
Confiabilidad requerida	Alta	Moderada
Tiempos de ida y vuela	250us – 10ms	50+ ms
Determinismo	Alta	Baja
Composición de datos	Paquetes pequeños de tráfico periódico y aleatorios	Paquetes aleatorios y grandes
Consistencia temporal y orden de eventos	Necesaria y muy importante	No necesaria
Ambiente de operación	Condiciones hostiles, con altos niveles de contaminación, calor y vibración	Ambientes limpios, pensados para equipo sensible

Componentes de una Red Industrial

- Los componentes de las redes industriales son:
  - SCADA
  - DSC
  - PLC
- Las redes industriales se ocupan de las comunicaciones entre estos tres componentes.
- A estos componentes **también se les conoce como sistemas de control industrial** (*Industrial Control Systems o ICSs*).
- Las **diferencias** entre los tres sistemas se **desvanecen conforme evoluciona la tecnología**.
  - La **integración de los tres conceptos recibe el nombre de PAC** (*Programmable Automation Controller o Process Automation Controller*).

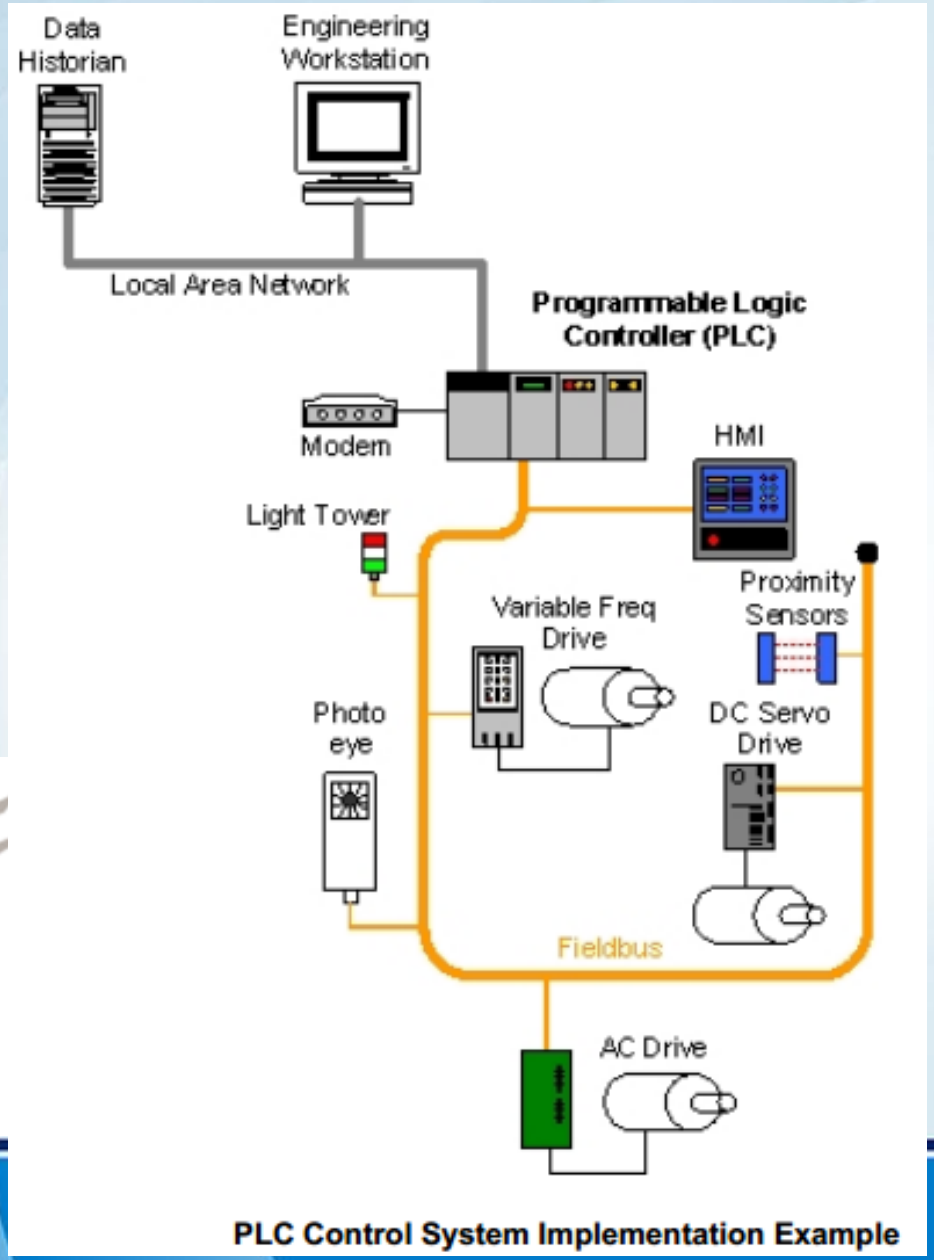
Sistemas de Control Industrial

- **SCADA:** *Supervisory Control And Data Acquisition*, Supervisión, Control y Adquisición de Datos, Control de supervisión y adquisición de datos, adquisición de datos y control de supervisión.
  - Nacen en aplicaciones industriales distribuidas: energía, tubos de gas y de agua, etc. donde hay una necesidad para extraer datos de lugares remotos a través de enlaces no confiables, intermitentes, de bajo ancho de banda y alta latencia.
- **DCS:** Sistemas de Control Distribuido
  - Nacen de la necesidad de obtener información y controlar sistemas en tiempo real, con ancho de banda alto y baja latencia en las redes de datos en una zona geográfica amplia. Se usan en plantas de procesos industriales.
- **PLC:** Controlador Lógico Programable
  - Nacen de la necesidad de remplazar relevadores organizados en forma de escalera que presentaban muchos problemas derivados de los cableados.

PLC

- **Computadora especializada para la industria.**
- También se le conoce como Controlador Programable (PCs).
  - Para evitar confusión se le ha llamado PLC.
- Desarrollados para cumplir los requerimientos de la División de Hydramatic de General Motors en 1968.
- Fáciles de programar y reprogramar, de mantener y reparar.
- Tamaño pequeño y baratos, modulares.
- Capaces de comunicarse con una unidad central.
- Estándares:
  - **IEC 61131**: define 5 languajes de programación: diagramas de escalera, cartas de secuencia funcional, diagrama de bloques fucionales, texto estructurado y lista de instrucciones.
  - **IEC 61499**: define diferentes bloques de funciones, sus interconexiones y sus aplicaciones en el diseño de un programa.

Ejemplo PLC



PLC Control System Implementation Example

SCADA

- Un sistema SCADA **se compone solamente de la capa de soporte de código** (*software*) .
- Se aplica normalmente **arriba de la capa del soporte físico** (*hardware*) de control.
- Los sistemas SCADA **no ejecutan ningún control** y su función es solo de supervisión.
- El **enfoque** de los sistemas SCADA es la **adquisición de datos y** la presentación de la interfaz humano-máquina (***HMI***).
- También **ejecutan comandos de alto nivel** para ser enviados mediante el soporte físico de control.
- Se enfocan al **monitoreo de soporte físico de control distribuido geográficamente en distancias largas**.
- El soporte físico que se comunica con el SCADA se le llama Unidad Terminal Remota (**RTU**). El RTU es un PLC especializado.
- La topología considera el **MTU** (*Master Terminal Unit*).

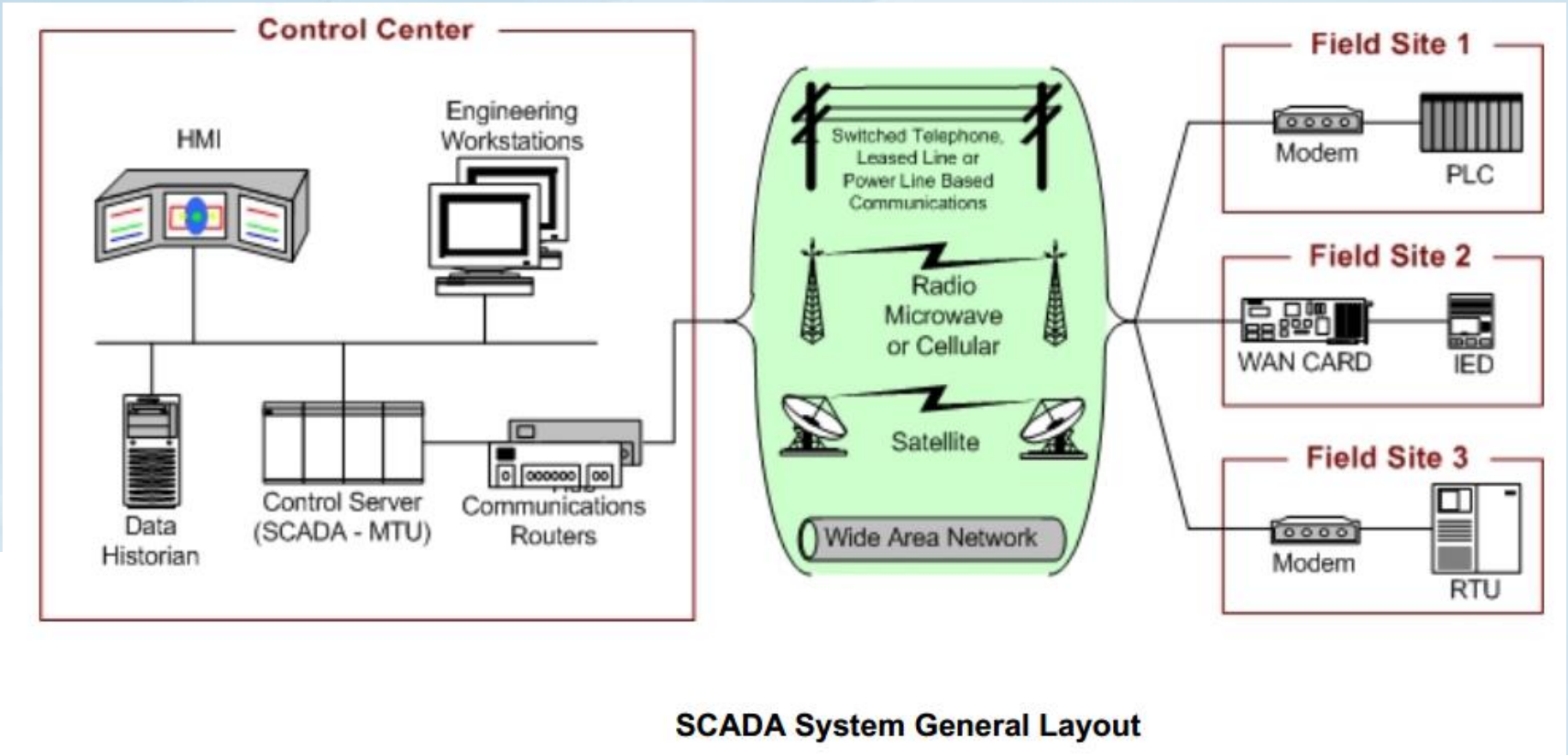
SCADA

- Los sistemas SCADA tienden a ser **manejados por eventos** (*event-driven*) en lugar de por procesos (*process-driven*).
- También **solo reportan los cambios** en lugar de toda la información.
  - Por lo tanto se deben modelar como sistemas híbridos.
- Los **RTUs usan de manera muy eficiente la potencia**.
- Los sistemas SCADA consisten de **dos capas de aplicación-cliente** las cuales presentan **el HMI y el servidor de aplicaciones**.
- El **servidor funciona como MTU** o puede comunicarse con MTUs dedicados.
- Las **funciones de red** pueden ser también **implementadas de manera redundante** para aumentar la confiabilidad.
- Las **aplicaciones cliente-servidor pueden comunicarse usando Ethernet implementado en los modos: cliente-servidor, servidor-servidor o productor-consumidor**.

SCADA

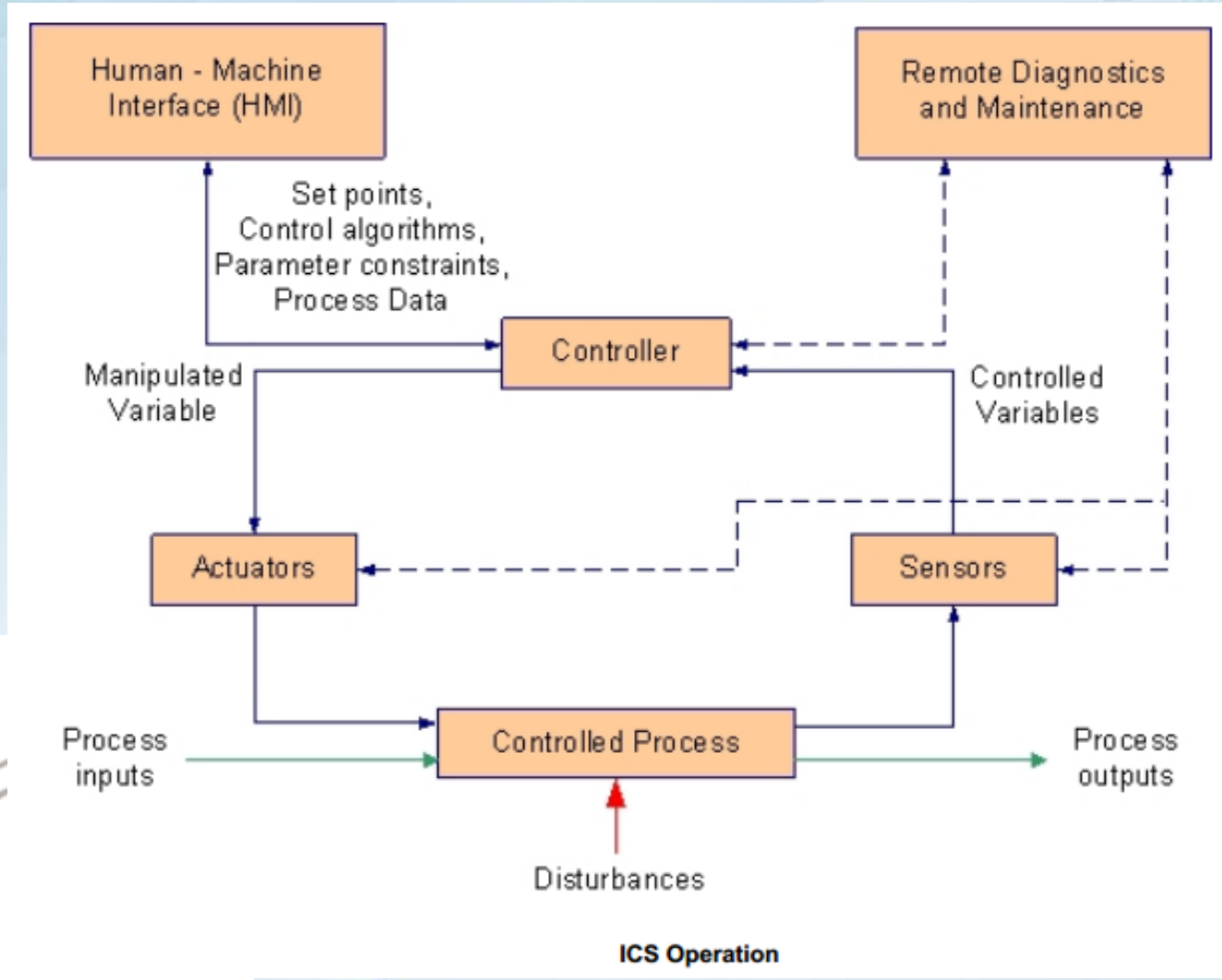
- Los sistemas SCADA también contienen **otras herramientas** de soporte de código:
  - Herramientas **de ingeniería** para configurar o para solucionar problemas.
  - Métodos **para re-enviar datos a otras aplicaciones**: **OLE** (*Open Linking Embedding*) para control de procesos (**OPC**).
- Los sistemas SCADA son **afectados por las tendencias en tecnologías de información**.
  - Avances en los sistemas operativos
  - Avances en el soporte físico de las computadoras
  - Problemático porque ambos tienen ritmos de evolución diferentes
- **El ciclo de vida** del sistema SCADA completo es una **consideración importante**.
- Existe una **preocupación creciente por la seguridad de la información y de la red**.

Sistema SCADA



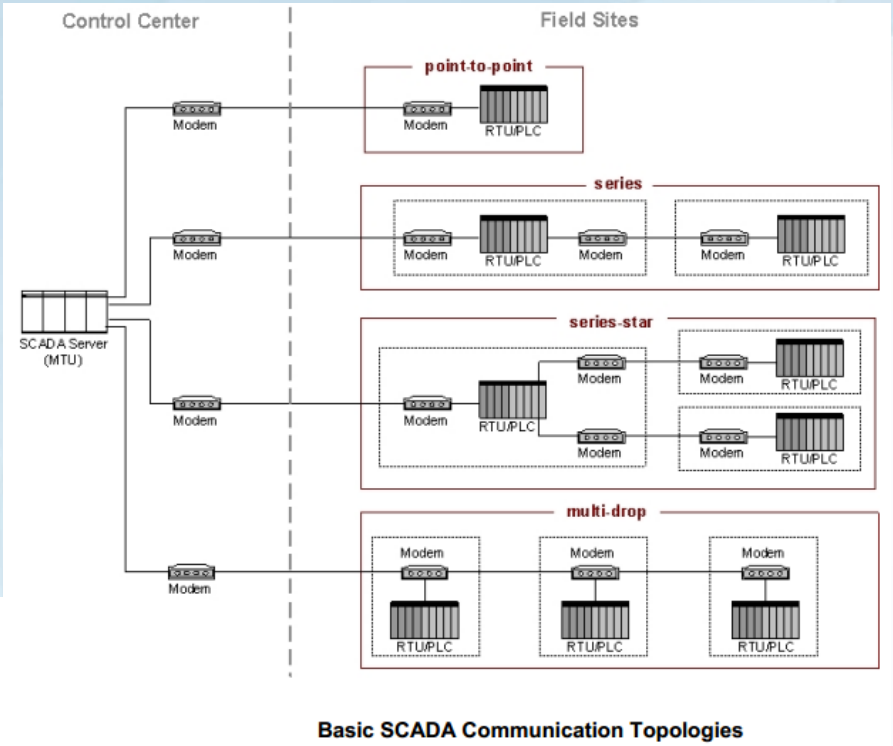
SCADA System General Layout

SCADA Components

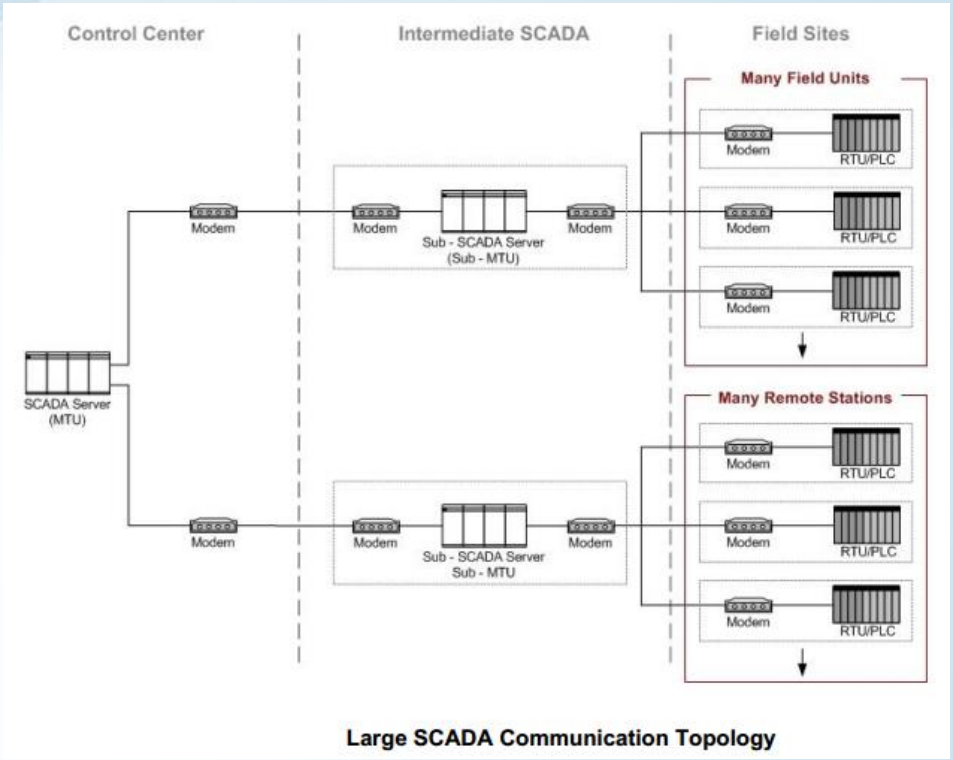


ICS Operation

Topologías SCADA

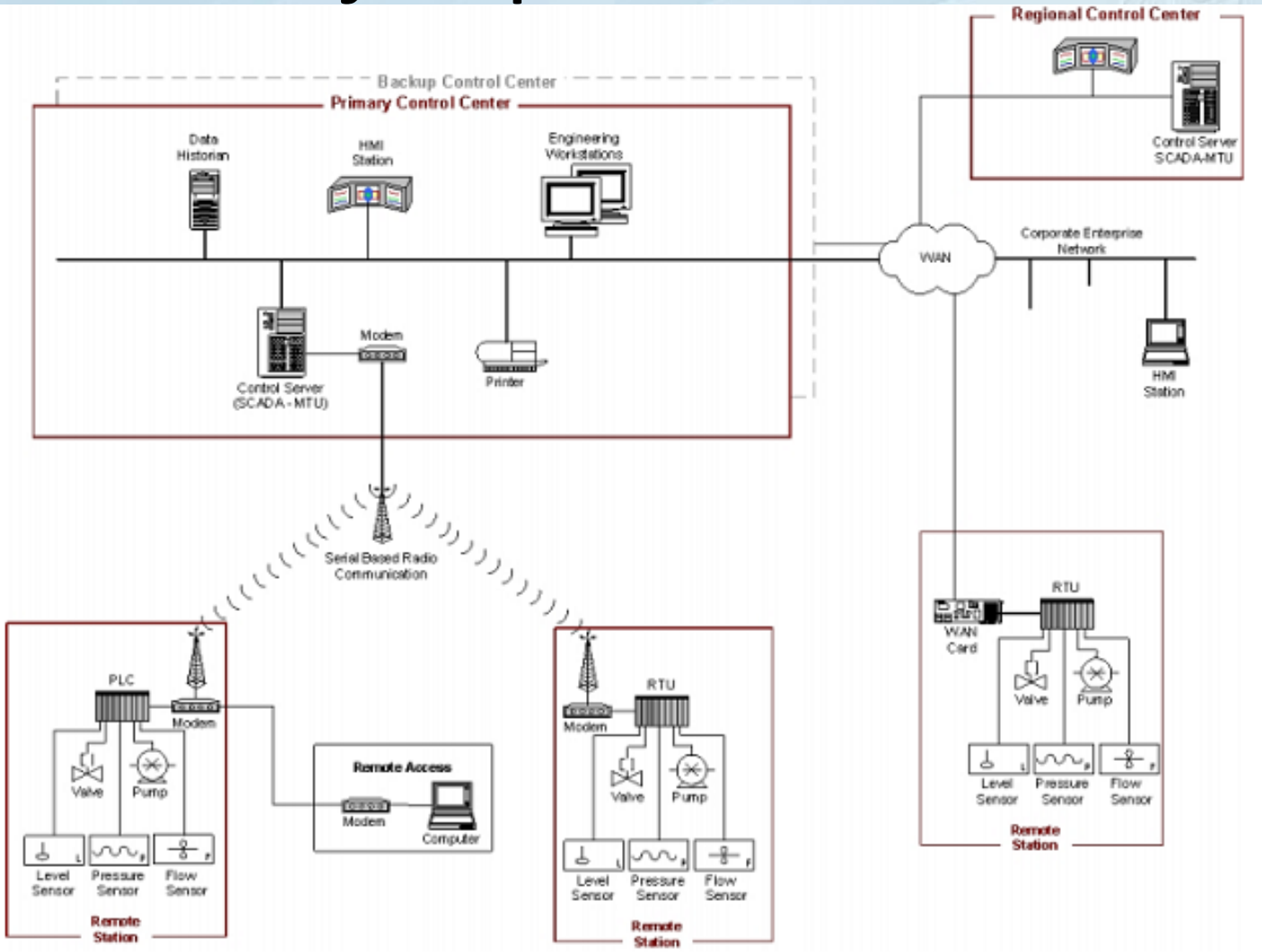


Basic SCADA Communication Topologies



Large SCADA Communication Topology

Ejemplo SCADA

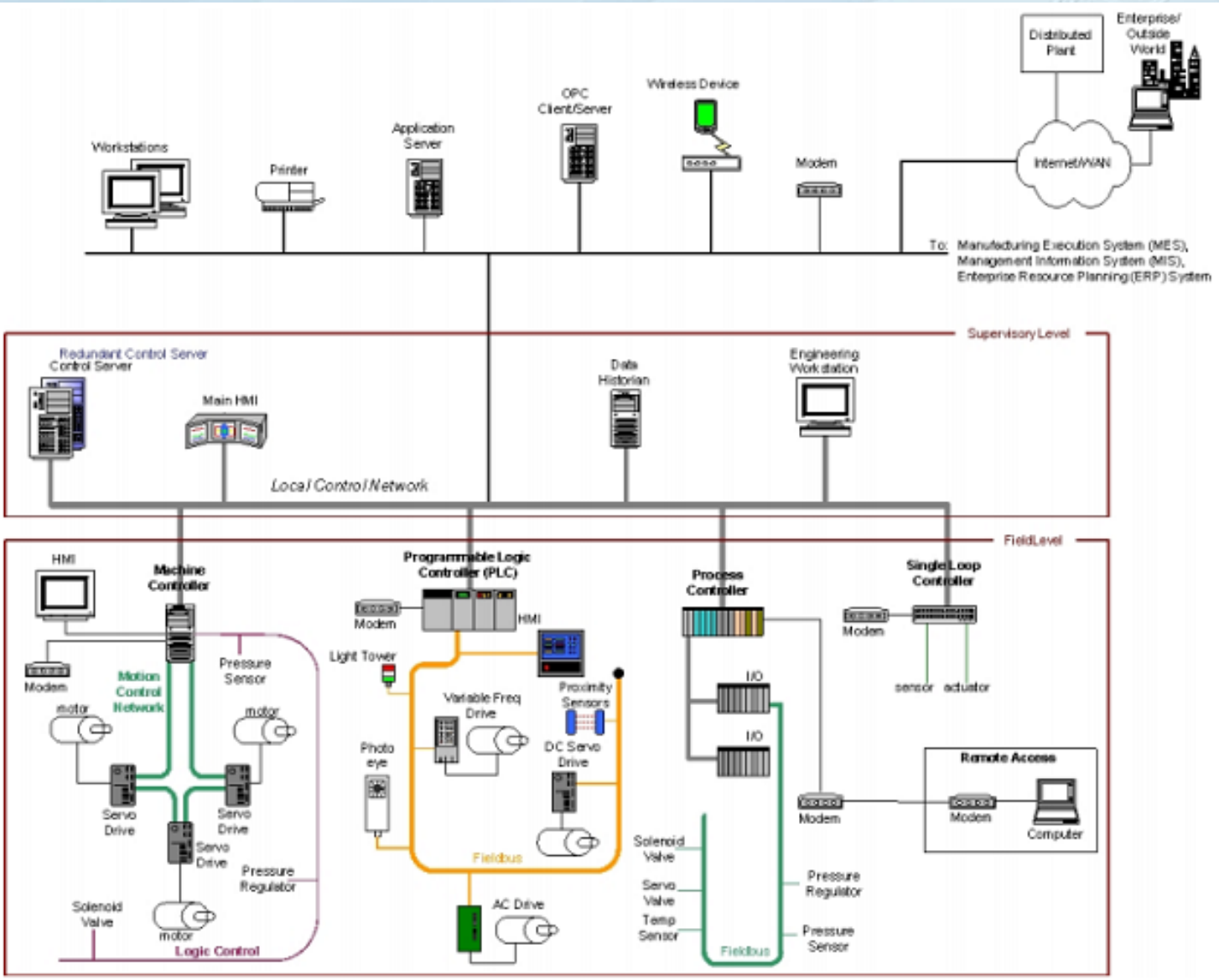


SCADA System Implementation Example (Distribution Monitoring and Control)

DCS

- DCS es **manejado por procesos** (*process-driven*).
- DCS se **enfoca en presentar un flujo estable de procesamiento de información**.
- Un DCS tiene un **nivel mayor de interconexión entre la capa de soporte de código y el soporte físico de control así como entre controladores**.
- Los DCS no **se preocupan por la calidad de los datos** debido a que la comunicación con el soporte físico de control es más confiable.
- El **soporte físico de control consiste de PLCs** tradicionales frecuentemente con procesadores muy potentes implementando múltiples controles de lazo cerrado.
- Los DCSs **no se recomiendan para zonas geográficamente distantes pero si para plantas locales altamente interconectadas** (refinerías, estaciones de potencia, etc.)
- Muy **similares a SCADA con arquitecturas similares en las capas altas**.
- Mismas afecciones por evolución de TI y mismos requisitos de seguridad que los sistemas SCADA.

Ejemplo DCS



DCS Implementation Example

DCS vs. SCADA

DCS	SCADA
Manejado por procesos	Manejado por eventos
Para áreas geográficas pequeñas	Para áreas geográficas grandes
Para sistemas largos e integrados tales como procesamientos químicos y generación de energía eléctrica	Para múltiples sistemas independientes tales como manufactura discreta y distribución de servicios públicos
Buena calidad de datos y confiabilidad media	Pobre calidad de datos y confiabilidad media
Soporte físico de control de lazo cerrado muy potente	Soporte físico eficiente en potencia, a menudo enfocado a detecciones de señales binarias.

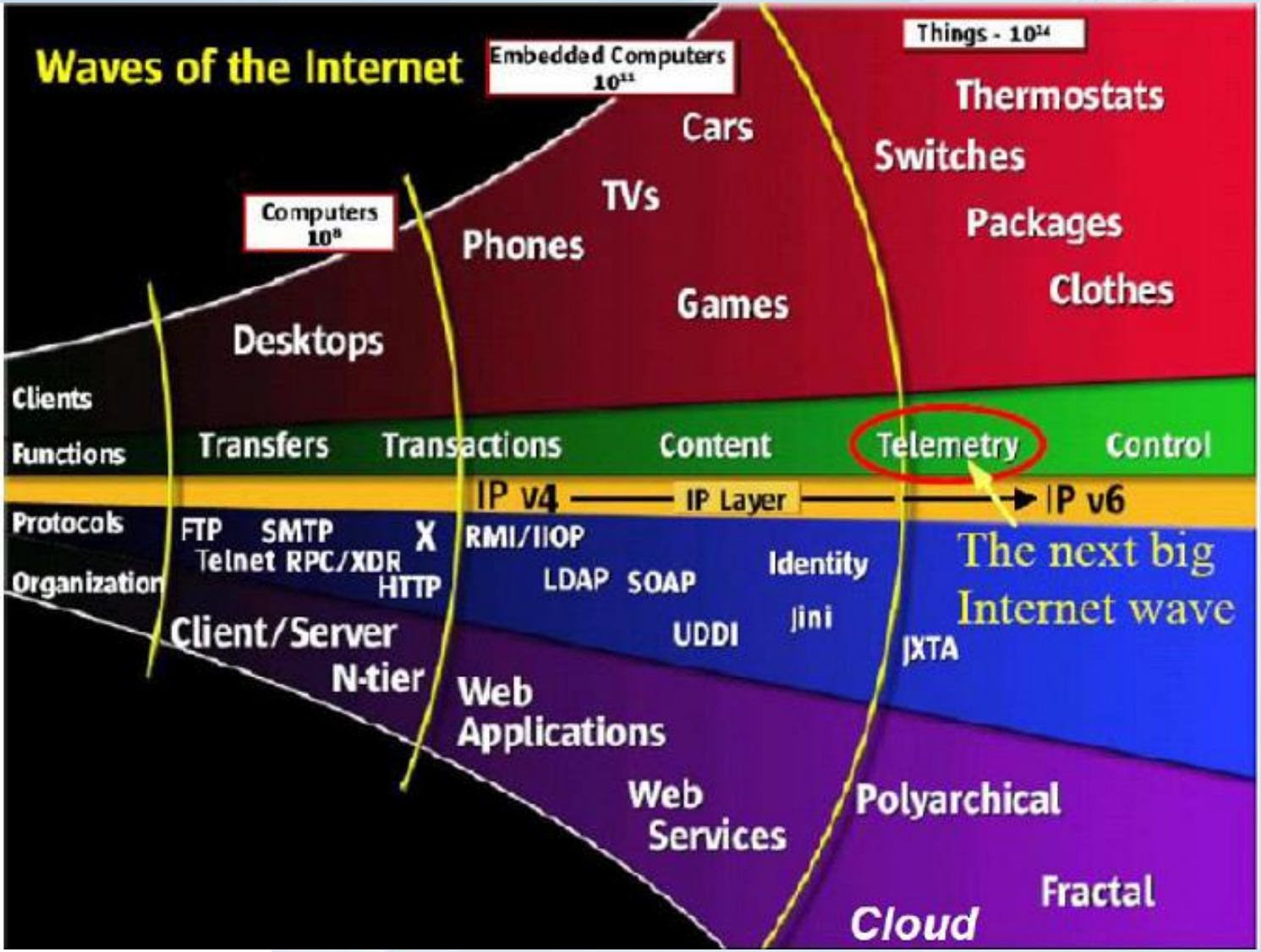
Orígenes y Evolución

- Manufacturing Automation Protocol (MAP).
  - Se enfoca en las comunicaciones entre controladores de fábrica y celdas de control.
- Technical and Office Protocol (TOP).
  - Perfiles de comunicación en la jerarquía de CIM.
  - Los perfiles facilitan la comunicación entre oficinas de negocios y técnicas.
- Mini-MAP o MAP/EPA (Enhanced Performance Architecture)
  - Incorporó la especificación de la interconexión de la fábrica automática al definir perfiles de comunicaciones entre celdas de control.
- Manufacturing Message Specification (MMS) se desarrolló como parte del proyecto MAP.
- La los bajos niveles de las jerarquías se necesitaba de un protocolo que redujera los requerimientos de alambrado de la señalización tradicional. Lo que dio como resultado el nacimiento del protocolo Fieldbus.

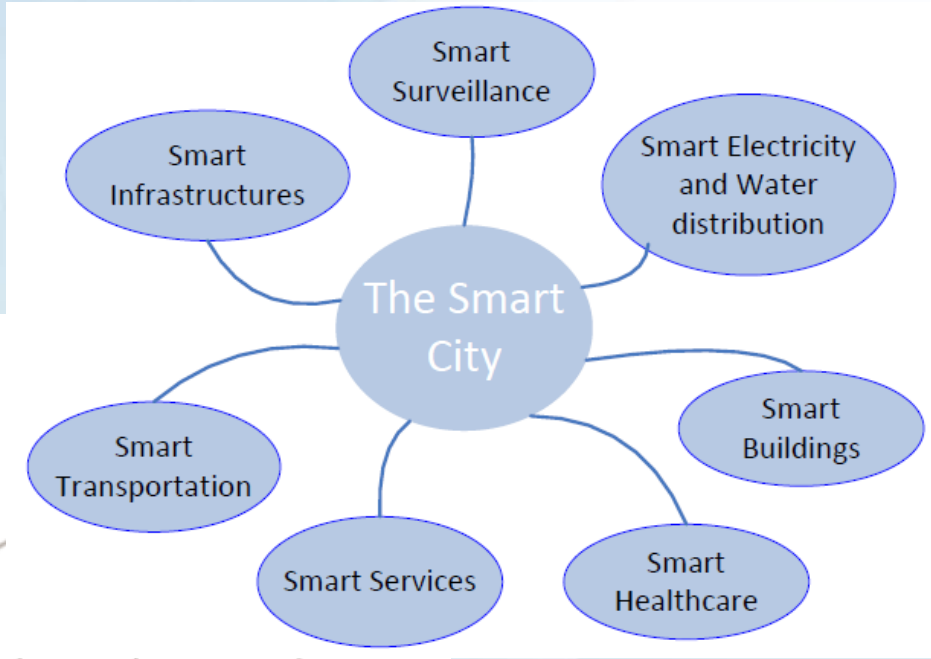
Orígenes y Evolución

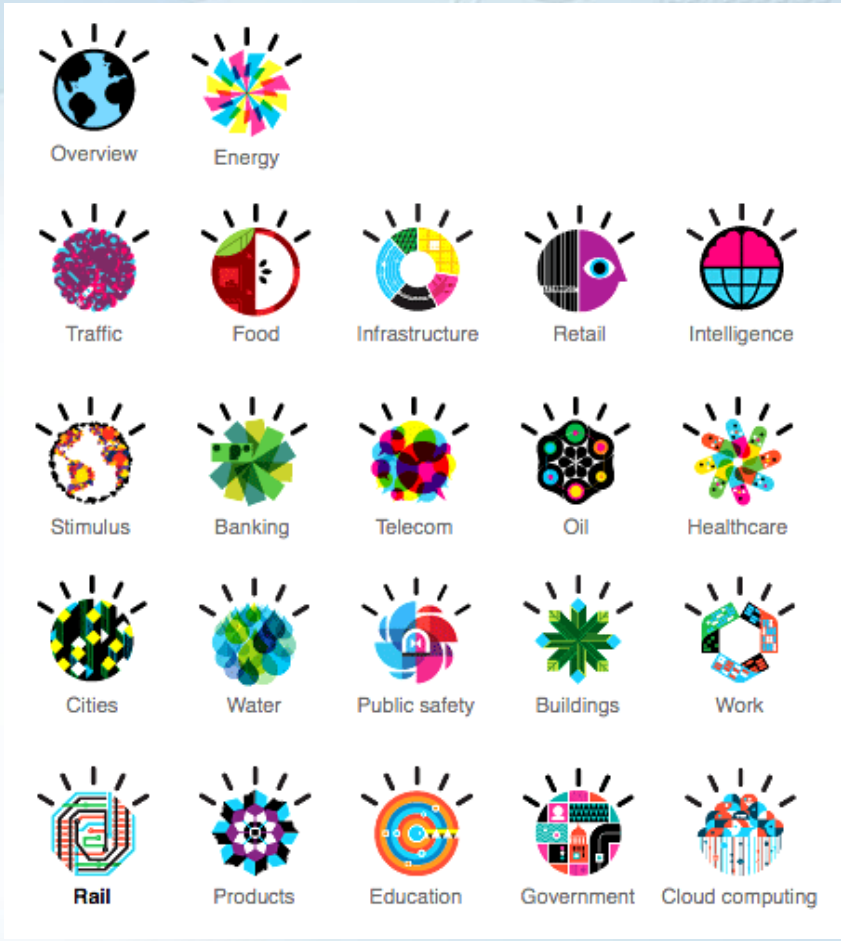
- La base son los protocolos **Fieldbus (IEC 61158)**, IEC61784 en proceso.
  - Bus digital, serial, multisalida de datos para comunicaciones con control industrial y dispositivos de instrumentación (transductores, actuadores y controladores locales).
  - Los precursores empezaron en 1970s. PROFIBUS (Alemania), FIP (Francia), P-Net (Dinamarca), **etc.**. **El proceso de convertirse en estándar en IEC**.
  - Manufactura Integrada por Computadora (**CIM**): define una estructura jerárquica para el uso de las computadoras en todos los niveles de la automatización industrial.
- Fieldbus fue concebido para remplazar las técnicas de señalización a dos alambres (4-20 mA y 0-10 V) usados en los niveles de jerarquías bajas en el control industrial.
- **Generaciones de redes industriales de control**:
  1. Protocolos Fieldbus en serie (de monolíticas -> distribuidas -> en red).
  2. Protocolos basados en Ethernet: **Ethernet Fieldbus, etc.**
  3. Incorporación de tecnologías inalámbricas y seguridad: **IEC: ISA 100.11a, WirelessHART, WIA-PA (Wireless Networks for Industrial Automation – Process Automation). Estándares abiertos: 62734, 62591 y 62601. Casi compatibles con IEEE 802.15.4 (ZigBee). Seguir evolución de ZigBee-IP así como 6LoWPAN.**

Olas de Internet



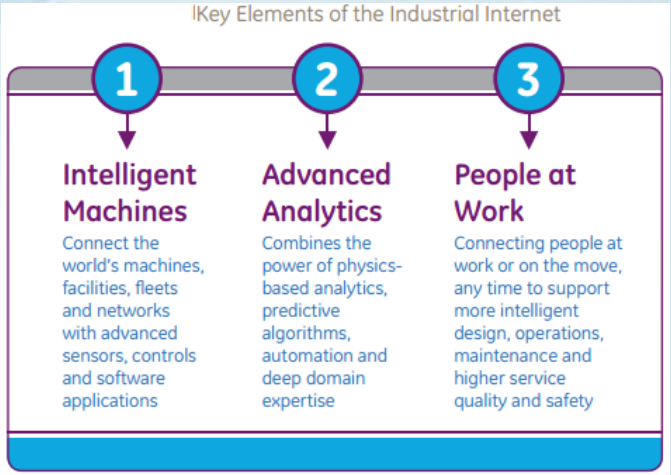
Smart Planet (IBM)

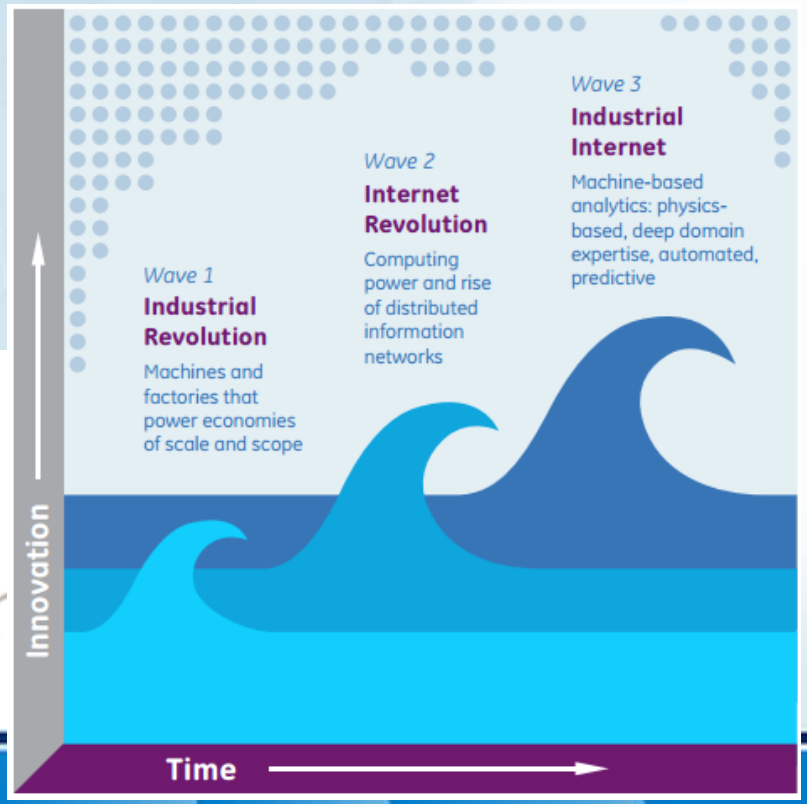


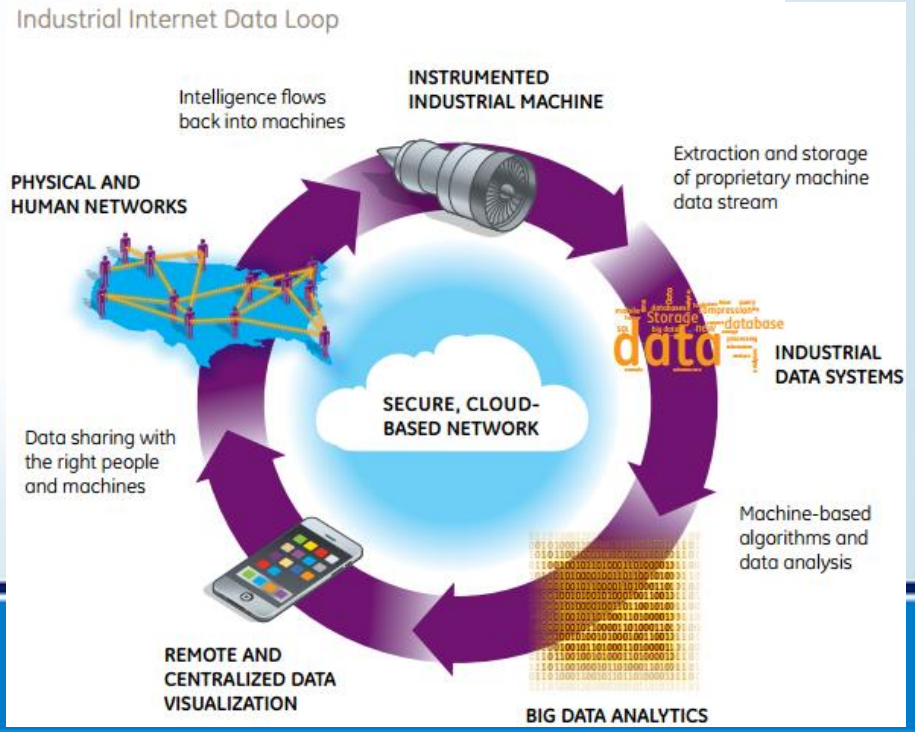


Internet y WEB Industrial

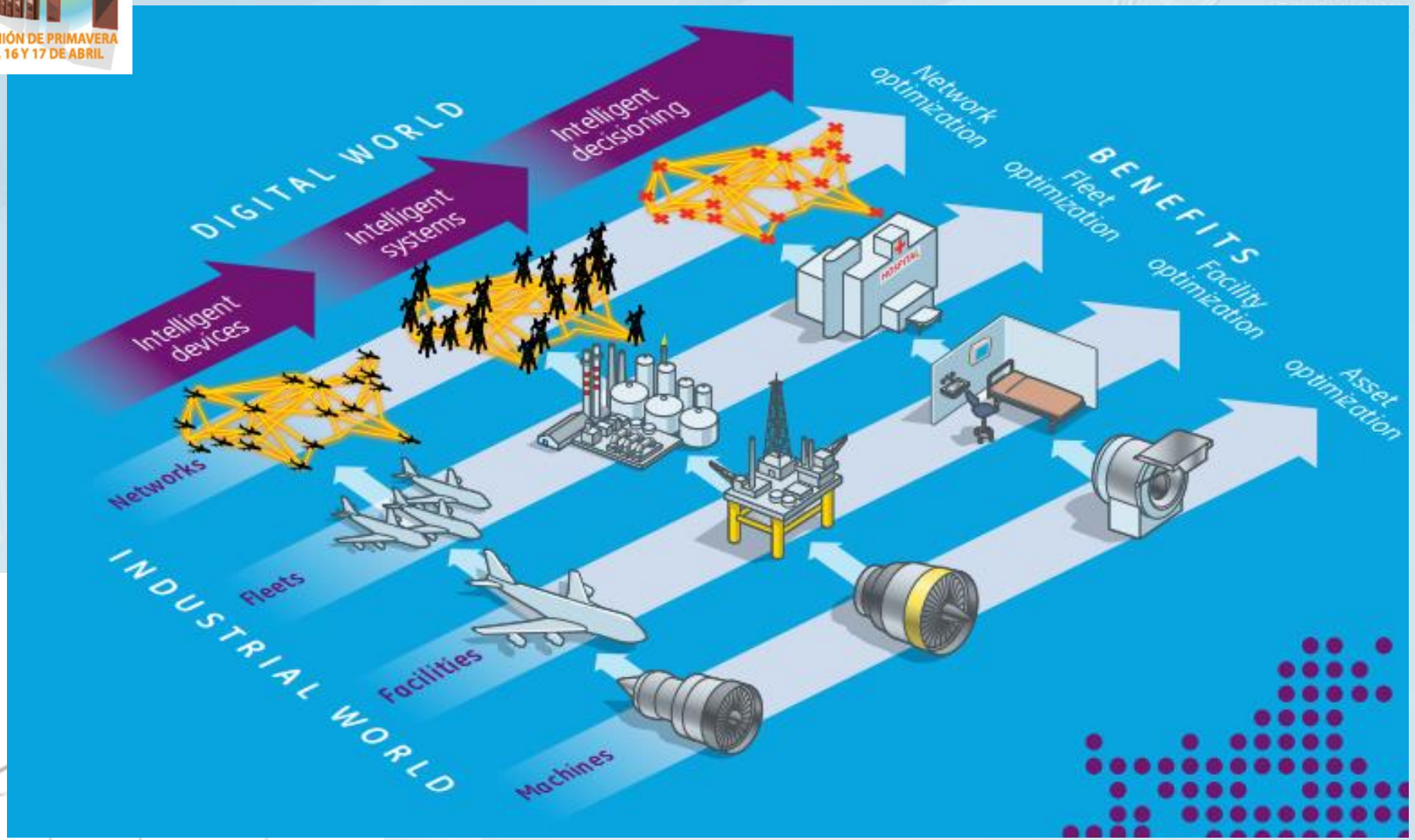
- Integración de maquinas complejas con sensores en red y soporte de código. Integra los siguientes dominios:
  - Machine learning
  - Big data
  - Internet of things
  - M2M communications







Industrial Internet (GE)



Cyber-Physical Systems (CPSs)

- Son sistemas que tienen una integración (combinación de, y una coordinación entre) del sistema computacional, de redes y de los procesos físicos.
- Son computadoras embebidas y redes que monitorean y controlan los procesos físicos con lazos de retroalimentación donde los procesos físicos afectan los cálculos y viceversa.
- Los CPSs integran la dinámica de los procesos físicos con los de soportes de código, de redes, proporcionando abstracciones y modelado, diseño, y técnicas de análisis para una integración total de las tres disciplinas.
- El precursor de los CPSs son los sistemas embebidos.
- Los CPSs son una red de elementos que interactúan con entradas y salidas físicas.
- Se piensa que esta integración incrementará en los CPSs la:
  - Adaptabilidad
  - Autonomía
  - Eficiencia
  - Funcionalidad
  - Confiabilidad
  - Seguridad
  - Usabilidad
- Potenciando sus aplicaciones:
  - Intervención
  - Precisión
  - Operación en ambientes peligrosos
  - Coordinación
  - Eficiencia
  - Aumento de capacidades humanas

Smart Grid

- Es una red eléctrica que usa TICs para obtener y actuar con base en la información.
  - Los protocolos más conocidos son el *Power Line Communications* (PLC), X-10, BPL (*Broadband over Power Line*) o tecnologías inalámbricas.
- La información puede ser sobre comportamientos de proveedores y consumidores.
- La información puede ser transferida de manera autónoma para mejorar la eficiencia, la confiabilidad, la economía, y la sustentabilidad de la producción y distribución de electricidad.
- El término se uso por primera vez en un artículo publicado en 2005: Amin and Wollenberg, “Towards A Smart Grid”.
- El crecimiento en la demanda en los últimos años así como el esperado (de ~200 TWh en 2010 a ~400TWh en 2025) requiere administrar mejor este servicio público lo que ha captado el interés por el término “Smart Grid”
- Hay un proyecto Europeo para transmitir Internet por la red eléctrica a 200 Mbps.

Smart Grid

- Algunas tecnologías se refieren a: control electrónico, medición y monitoreo.
- Se han desarrollado electrodomésticos o equipo de uso en el hogar que se adaptan con base en la demanda y las tarifas.
- Características:
  - Confiabilidad
  - Flexibilidad en topología de red
  - Eficiencia
  - Ajuste local
  - Reducción y nivelación de picos y tarificación por uso
  - Sustentabilidad
  - Habilitación de mercado
  - Soporte de respuesta a la demanda
  - Plataforma para servicios avanzados
  - Aprovisionamiento de Megabits , control de potencia con Kilobits, venta del resto.

Smart Grid

- Tecnología:
  - Comunicaciones integradas
  - Medición y sensado
  - Medidores inteligentes
  - Medidores de fase
  - Componentes avanzados
  - Control avanzado
  - Mejora de interfaces y soporte a la toma de decisiones
  - Generación inteligente de potencia
- Proyectos de Investigación
  - IntelliGrid
  - Modern Grid Initiative
  - Grid 2030
  - GridWise
  - GridWise Architecture Council
  - GridWorks
- Retos de implementación:
  - Modelos de negocios
  - **Los sistemas SCADA han sido desarrollados con estándares propietarios por lo que no son compatibles para estas aplicaciones.**

Estándares para Smart Grid

- IEEE Smart Grid Initiative
- IEEE 2030.2: extensión del trabajo de almacenamiento de servicios públicos para redes de transmisión y distribución.
- IEEE P2030: Nuevas guías para el desarrollo de interfaces entre TICs y la red eléctrica que también incluye:
  - Baterías, supercapacitores y volantes generadores de energía.
- IEEE P2030.1: Guías para integrar vehículos eléctricos
- IEC TC57: Familia de estándares internacionales que pueden ser usados como parte de e incluyen:
  - IEC61850: Arquitectura de para automatización de subestaciones
  - IEC61970/61968: Modelo de información común (CIM), semántica común para convertir datos en información.
- OpenADR: estándar de comunicación abierto para ser usado en aplicaciones de respuesta a la demanda.
- MultiSpeak: Especificación que soporta funcionalidad de distribución.
- Hay tendencia en usar TCP/IP: CISCO, etc.
- NIST incluyó ITU-T G.hn: comunicaciones de alta velocidad sobre líneas eléctricas, telefónicas y cable coaxial.

PREGUNTAS Y RESPUESTAS

Dr. César Cárdenas
ccardena@itesm.mx

GRACIAS!

MARTES DE 16H00 A 17H40: ARQUITECTURAS DE PENSAMIENTO DE INNOVACIÓN PARA LA EDUCACIÓN

MIÉRCOLES DE 9H00 A 10H40: MANUFACTURA INTERACTIVA

Dr. César Cárdenas
ccardena@itesm.mx