



Proyecto de Investigación:

SEGURIDAD EN REDES INDUSTRIALES

CLAVE PARA LA CIBERSEGURIDAD DE LAS INFRAESTRUCTURAS CRITICAS

Integración de las tecnologías
IT - OT

Mg. Lic. Jorge Kamlofsky

Introducción:

Resumen

El nuevo paradigma de Industria 4.0 pregoná la confluencia entre la tecnología corporativa e industrial, lo que ha abierto agujeros de seguridad.

Los sistemas de Control industrial están presentes tanto en los complejos industriales como en las infraestructuras críticas de las naciones.

En 2010 las plantas de enriquecimiento de uranio de Irán fueron atacadas por un virus llamado “Stuxnet” dejando expuesto el problema de seguridad en estos sistemas.

El presente trabajo presenta avances y resultados de las investigaciones tendientes a implementar de soluciones de Seguridad Informática con criptografía e inteligencia artificial a los sistemas de control industrial.

Introducción:

Importancia de estas investigaciones

El mejoramiento de la seguridad en las redes industriales permitiría evitar daños o sabotajes causados por ciber-ataques hacia los bienes de las industrias. Evitaría también, el robo de las recetas de producción de algunos productos industriales.

Podría evitar (o dificultar) la concreción de ciber-ataques terroristas a infraestructuras críticas de las naciones que pudieran ocasionar efectos catastróficos en una nación, o quizás, a nivel mundial.

Contenido de esta Presentación

Una Introducción a Industria 4.0

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

Seguridad en Tecnologías Operacionales

Resumen de Nuestro Proyecto

Contenido de esta Presentación

Una Introducción a Industria 4.0

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

Seguridad en Tecnologías Operacionales

Resumen de Nuestro Proyecto

Una Introducción a Industria 4.0

Hacia adónde vamos...

Fuente: Montagut Contreras, Eduardo. "La transición demográfica en la Revolución Industrial", Los ojos de hipatía, ISSN: 2341-0612, (2017)

Una Introducción a Industria 4.0

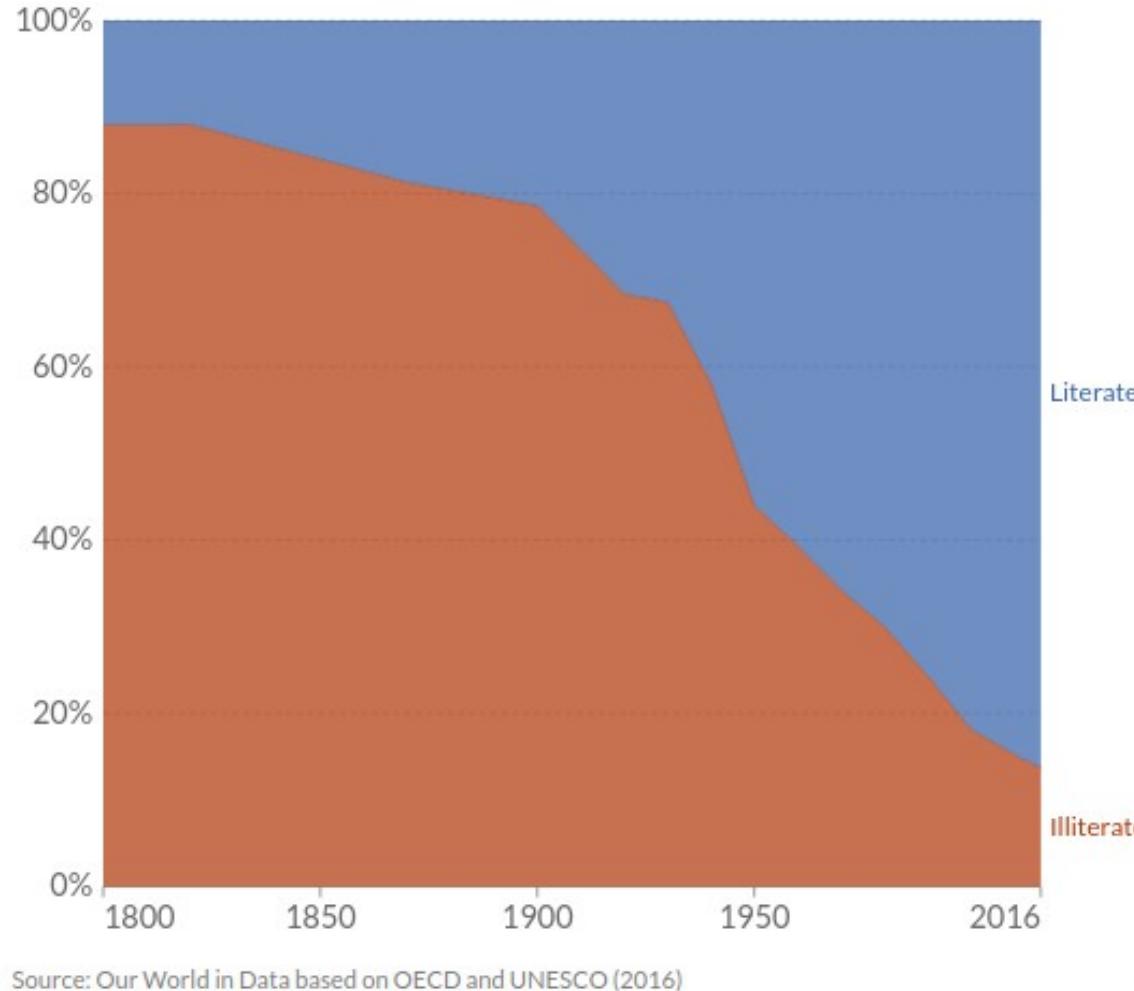
Breve reseña histórica:

Desde mediados del siglo XVIII hasta la fecha las revoluciones industriales han producido una explosión demográfica: Creció fuertemente la esperanza de vida y se redujo notoriamente la pobreza. Estos cambios se lograron gracias al incremento de la disponibilidad de bienes y de alimentos, el incremento de la necesidad de mano de obra y mejoras permanentes en las condiciones sanitarias.

Fuente: Montagut Contreras, Eduardo. "La transición demográfica en la Revolución Industrial", Los ojos de hipatía, ISSN: 2341-0612, (2017)

Una Introducción a Industria 4.0

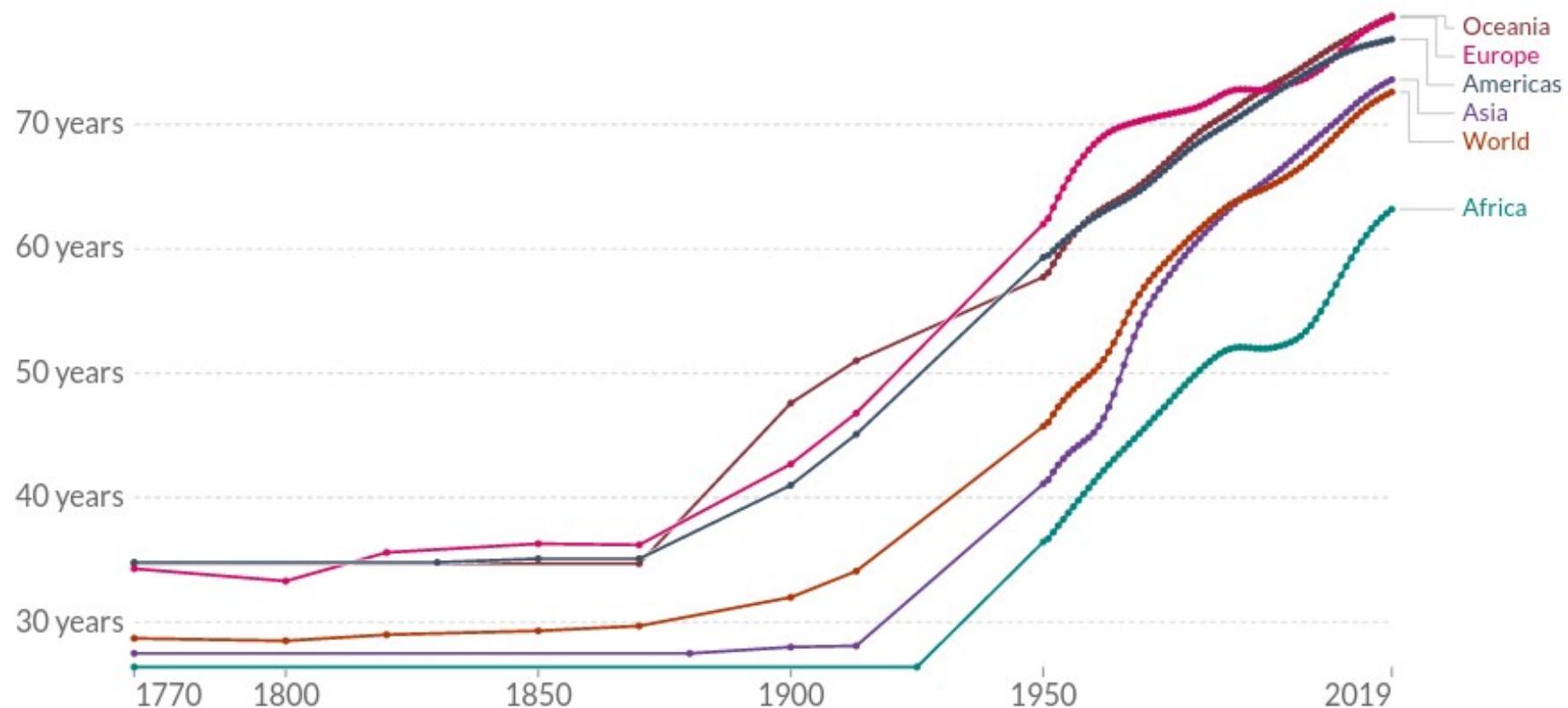
Breve reseña histórica: La disminución del analfabetismo



Fuente: https://verne.elpais.com/verne/2018/01/23/articulo/1516705169_487110.html

Una Introducción a Industria 4.0

Breve reseña histórica: La mayor expectativa de vida



Source: Riley (2005), Clio Infra (2015), and UN Population Division (2019)

Note: Shown is period life expectancy at birth, the average number of years a newborn would live if the pattern of mortality in the given year were to stay the same throughout its life.

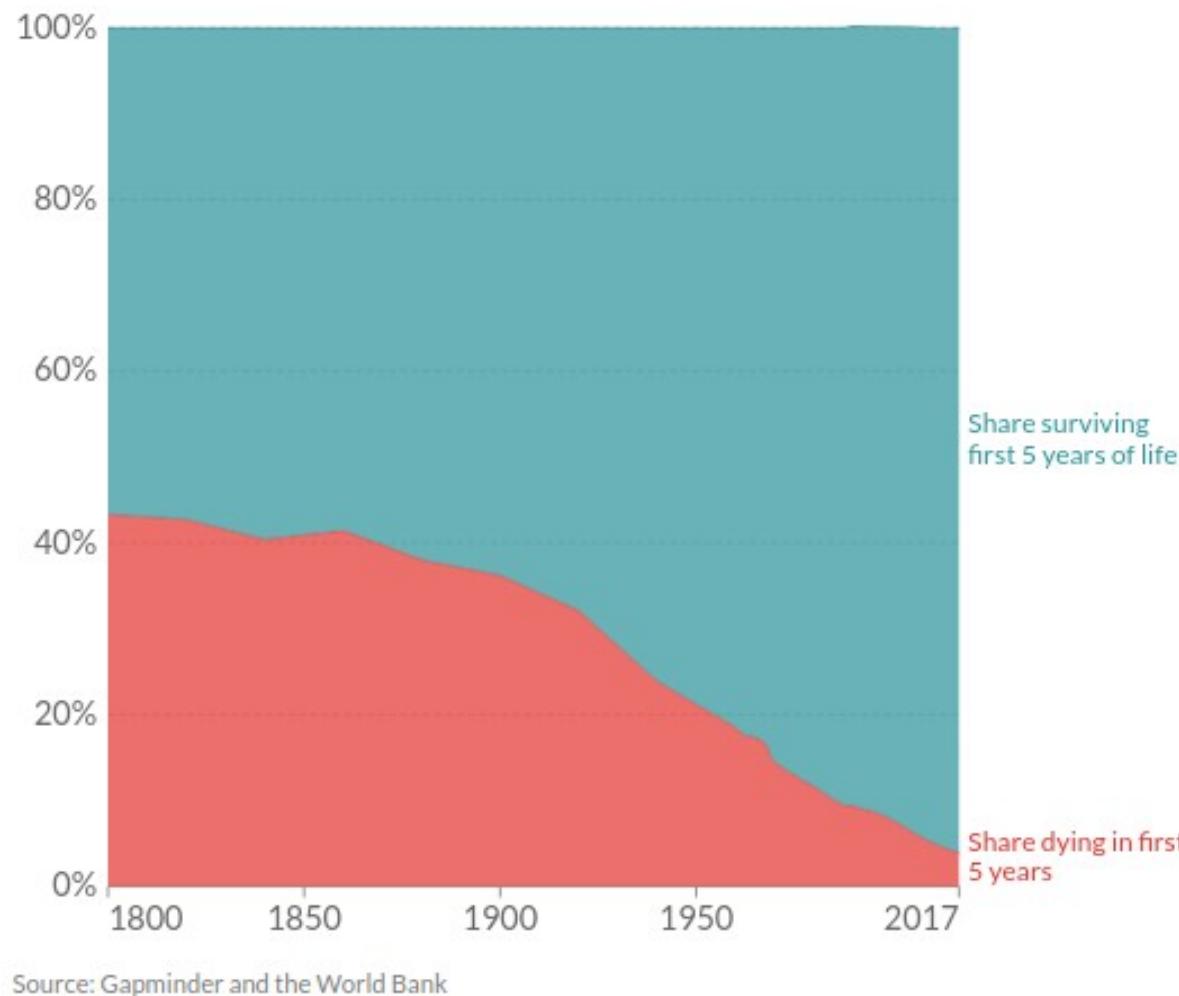
OurWorldInData.org/life-expectancy • CC BY

La expectativa de vida subió de 28,5 años en 1880 a 72,2 años en 2019

Fuente: Our World in Data - <https://ourworldindata.org/life-expectancy>

Una Introducción a Industria 4.0

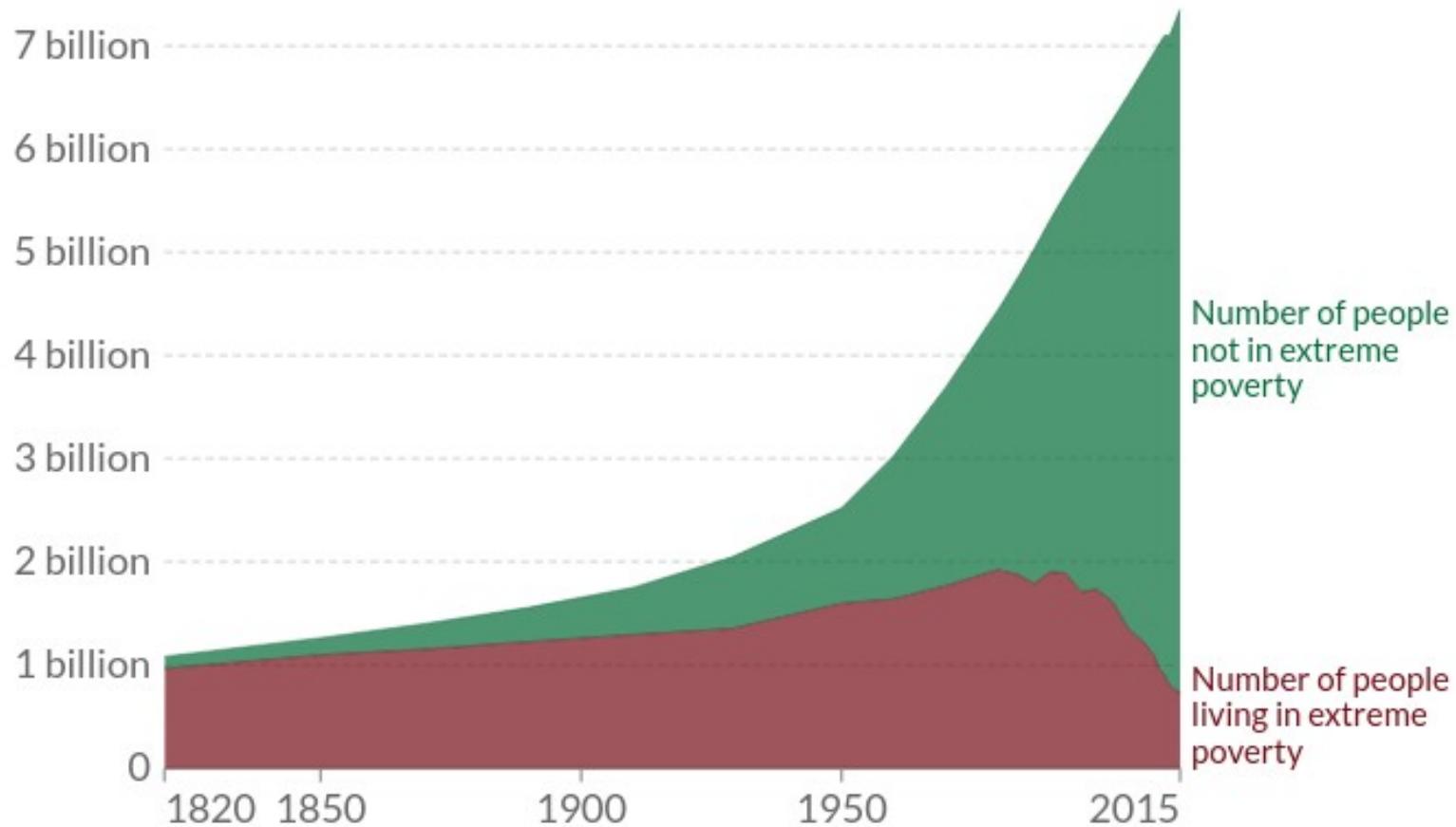
Breve reseña histórica: La disminución de la mortalidad infantil



Fuente: Our World in Data - <https://ourworldindata.org/child-mortality>

Una Introducción a Industria 4.0

Breve reseña histórica: La disminución de la pobreza extrema mundial



Fuente: https://verne.elpais.com/verne/2018/01/23/articulo/1516705169_487110.html

Una Introducción a Industria 4.0

Breve reseña histórica:

- 1) La primera revolución industrial se basó en la mecanización de la producción.
- 2) La segunda (estimada desde 1870 a 1970), se caracterizó por el uso intensivo de energía (eléctrica y petróleo).
- 3) La tercer revolución industrial (1970 - actualidad) se basó en la incorporación de dispositivos electrónicos, informáticos y redes de comunicaciones para la automatización de la producción.

Fuente: Kamlofsky J, Trigo S, Gonzalez G. Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. WICC, 2021.

Una Introducción a Industria 4.0

Breve reseña histórica

La automatización de la producción a gran escala se realiza con los ICS (del inglés: Industrial Control Systems). Los ICS consisten en sistemas de tele-mando y tele-control de procesos.

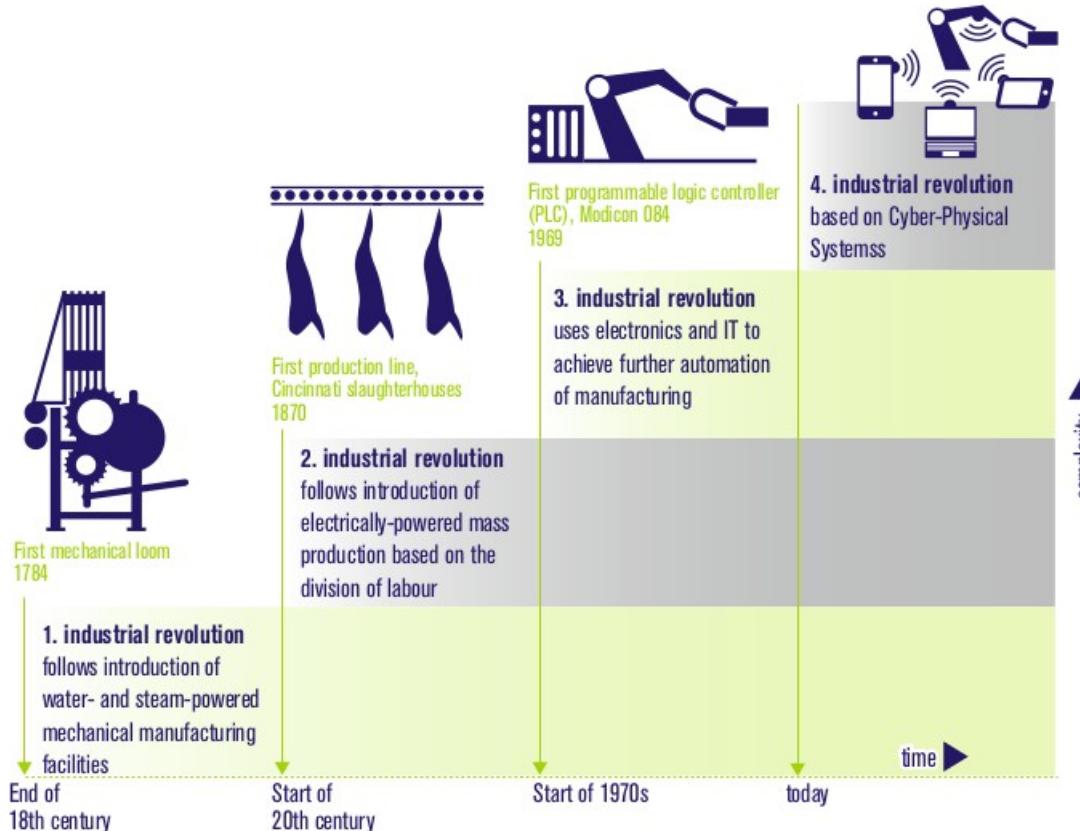
Están compuestos por:

- Autómatas industriales: RTU, PLC, DCS, etc. Poseen procesadores de pequeño porte y lógica determinista, lo cual favorece a la alta disponibilidad, esencial en el ambiente industrial (Nivel 2).
- Elementos de Campo: entradas y salidas, discretas y/o analógicas como ser: micro-switches, sensores de temperatura, actuadores para encendido de motores, llaves, etc. (Nivel 1)
- Los ICS se supervisan y controlan en tiempo real desde sistemas informáticos llamados SCADA (Nivel 3)

Fuente: Kamlofsky J, Trigo S, Gonzalez G. Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales. WICC, 2021.

Una Introducción a Industria 4.0

Breve reseña histórica

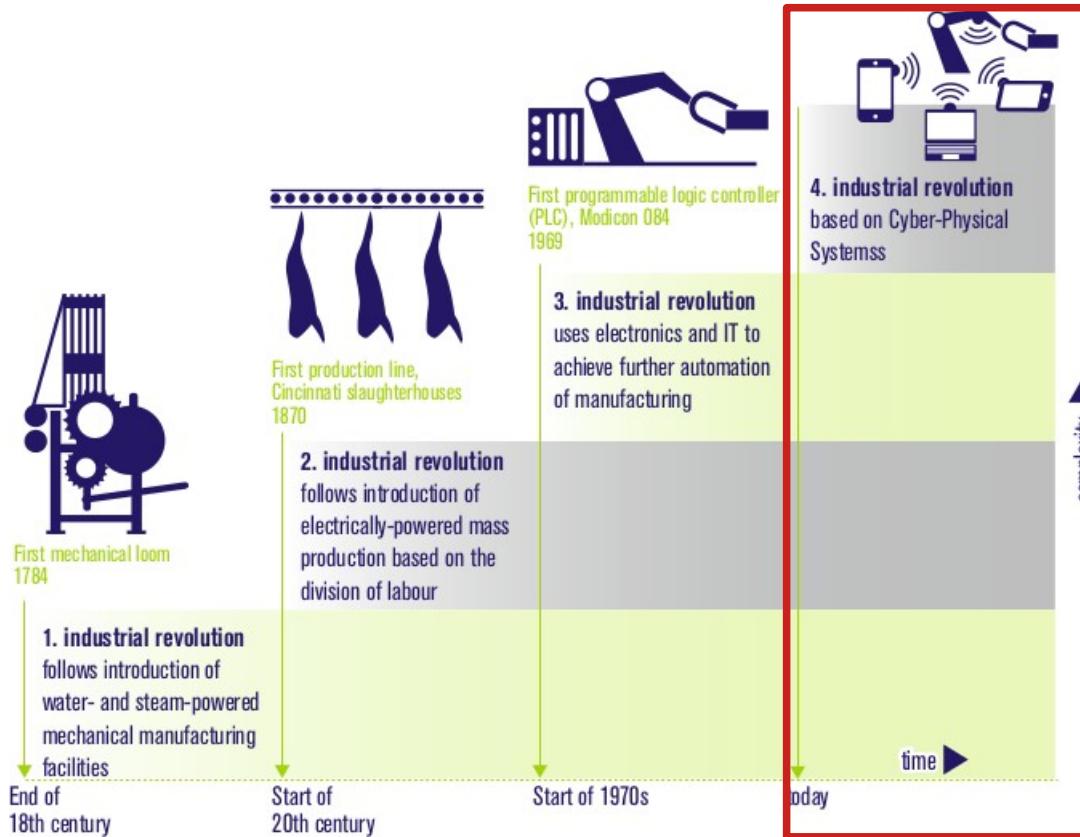


Las cuatro revoluciones industriales

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

Presentación



Las cuatro revoluciones industriales

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

Presentación

Industria 4.0 es considerada ya como la “Cuarta Revolución Industrial”, debido a su potencial y beneficios relacionados con la integración, innovación y autonomía de los procesos.

Los conceptos de industria 4.0 y manufactura inteligente, son relativamente nuevos y ***contemplan la introducción de las tecnologías digitales en la industria de la fabricación.*** Es decir, la incorporación al ambiente de manufactura de tecnologías como el internet de las cosas, cómputo móvil, la nube, el big data, redes de sensores inalámbricos, sistemas embebidos y dispositivos móviles, entre otros.

Fuente: Ybzunza Cortes C. y otros. El Entorno de la Industria 4.0: Implicaciones y Perspectivas Futuras. “Conciencia Tecnológica” nº54, 2017.

Una Introducción a Industria 4.0

Algunos Objetivos

- Optimización de los factores de decisión.
- Trazabilidad de la producción desde el inicio del proceso.
- Creación de nuevos productos y modelos de negocio.
- Producción personalizada.
- Facilitará el lanzamiento de pequeños emprendimientos.

Adicionalmente, Industria 4.0 ayudará a resolver algunos desafíos mundiales como ser: la eficiencia energética, producción urbana y el cambio demográfico.

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

El problema de la Integración

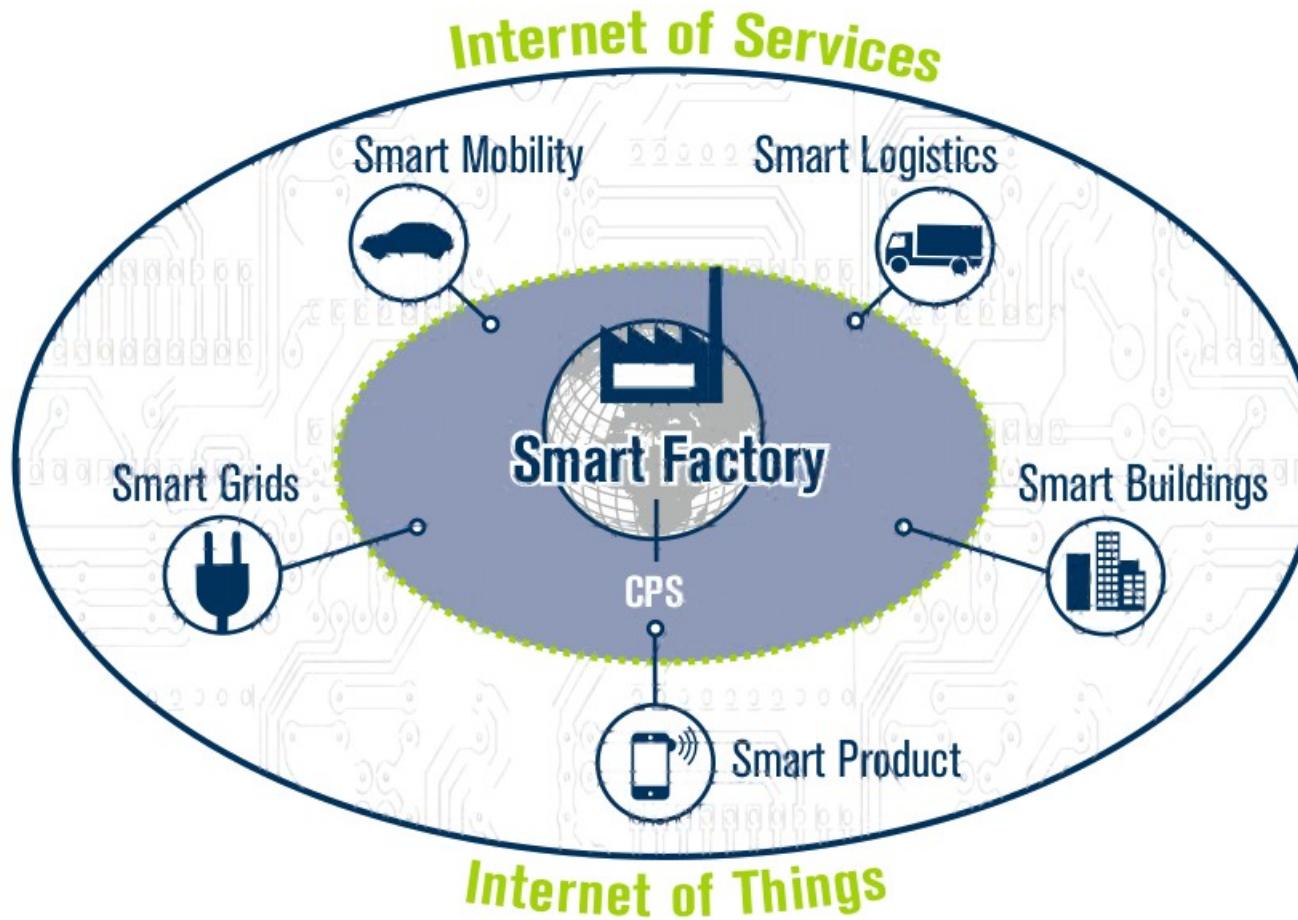
Se busca lograr:

- Integración Horizontal: de las redes de toda la cadena de valor de la producción
- Integración Vertical: de las redes de producción.

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

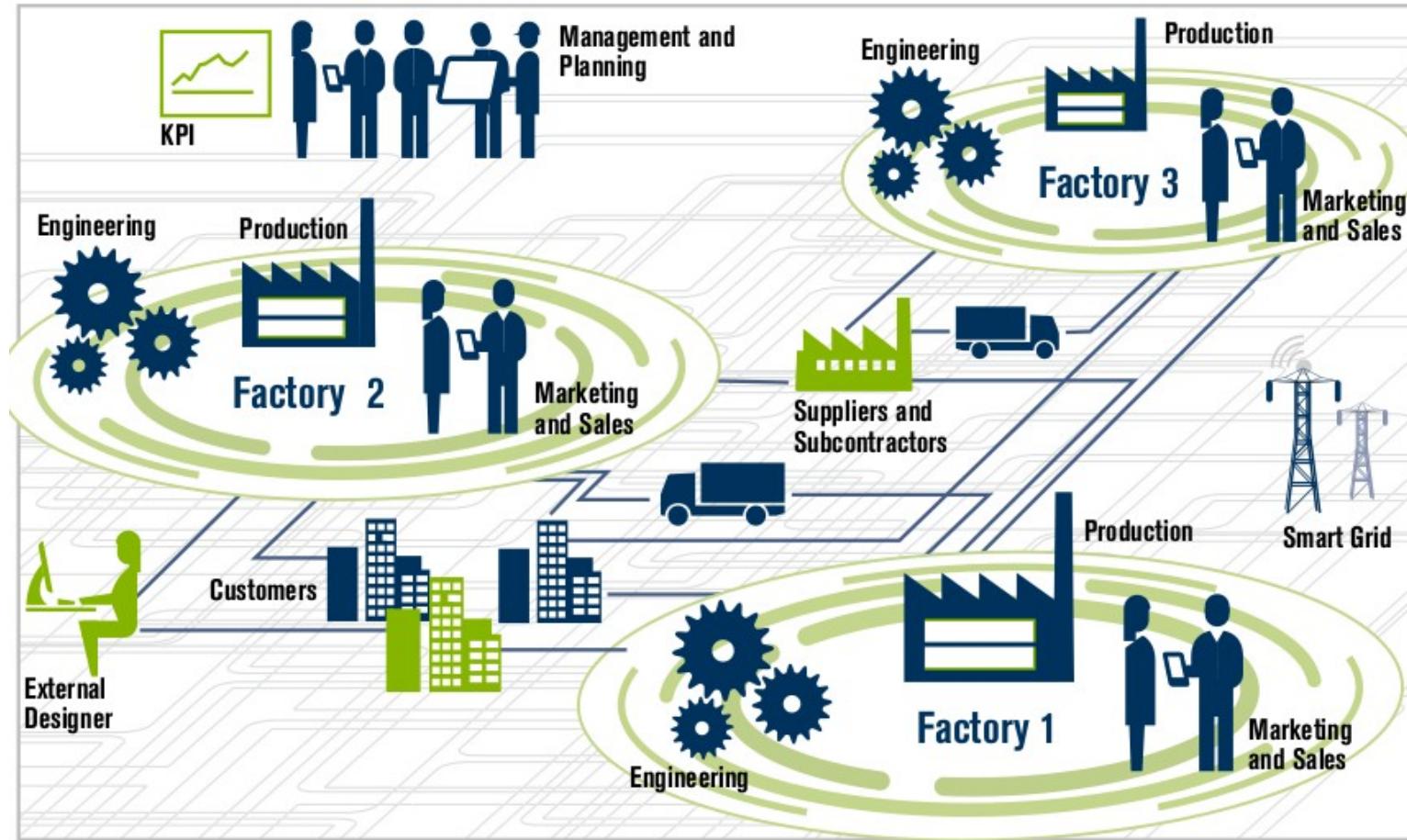
Integración de Fábricas con IoT e IoS



Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

Integración con diferentes sectores de la producción



Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

El problema de la Integración

El grupo de trabajo de Industria 4.0 cree que se requiere mucha **investigación** en los siguientes aspectos:

- 1)Estandarización y arquitecturas de referencia.
- 2)Supervisión de sistemas complejos.
- 3)Necesidad de una completa y más veloz infraestructura de comunicación de banda ancha.
- 4)Seguridad de la información y de los sistemas.
- 5)Diseño y Organización eficiente del trabajo.
- 6)Entrenamiento y desarrollo profesional continuo.
- 7)Diseño de marco regulatorio.
- 8)Eficiencia de recursos.

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

El problema de la Integración:

El grupo de trabajo de Industria 4.0 cree que se requiere mucha **investigación** en los siguientes aspectos:

- 1)Estandarización y arquitecturas de referencia.
- 2)Supervisión de sistemas complejos.
- 3)Necesidad de una completa y más veloz infraestructura de comunicación de banda ancha.
- 4)Seguridad de la información y de los sistemas.** → Nuestro Interés
- 5)Diseño y Organización eficiente del trabajo.
- 6)Entrenamiento y desarrollo profesional continuo.
- 7)Diseño de marco regulatorio.
- 8)Eficiencia de recursos.

Fuente: Kagerman H, Wahlster W, Johannes Helbig J. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group. Acatech – National Academy of Science and Engineering, 2013.

Una Introducción a Industria 4.0

El problema de la Integración: Seguridad de la Información y de los sistemas

Resumidamente, el grupo de trabajo de Industria 4.0 sugiere la hiperconectividad de los ICS con:

- Internet.
- Redes corporativas.
- IoT.
- IoS.

Una Introducción a Industria 4.0

El problema de la Integración: Seguridad de la Información y de los sistemas

Pero el ICS CERT de USA sugiere el aislamiento de los ICS para la mitigación de la gran mayoría de las Alertas presentadas en su sitio:

MITIGATION

ICS-CERT is attempting to coordinate with the vendor and security researcher to identify mitigations.

ICS-CERT recommends, as quality assurance, that users test the update in a test development environment that reflects their production environment prior to installation. In addition, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are **not accessible from the Internet**.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Una Introducción a Industria 4.0

El problema de la Integración: Seguridad de la Información y de los sistemas

Pero el ICS CERT de USA sugiere el aislamiento de los ICS para la mitigación de la gran mayoría de las Alertas presentadas en su sitio:

MITIGATION

ICS-CERT is attempting to coordinate with the vendor and security researcher to identify mitigations.

ICS-CERT recommends, as quality assurance, that users test the update in a test development environment that reflects their production environment prior to installation. In addition, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are **not accessible from the Internet**.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Mientras que quienes tratan los problemas de ciberseguridad en ICS sugieren su aislamiento físico, quienes pregan Industria 4.0 proponen su hiper-conexión.

Fuente: Sitio US-ICS CERT. Link: <https://www.cisa.gov/uscert/ics/alerts>

Universidad FASTA: Ciberseguridad y Análisis Forense de entornos Industriales - 1/7/2022

Jorge.kamlofsky@uai.edu.ar



Una Introducción a Industria 4.0

El problema de la Integración: Seguridad de la Información y de los sistemas

Pero el ICS CERT de USA sugiere el aislamiento de los ICS para la mitigación de la gran mayoría de las Alertas presentadas en su sitio:

MITIGATION

ICS-CERT is attempting to coordinate with the vendor and security researcher to identify mitigations.

ICS-CERT recommends, as quality assurance, that users test the update in a test development environment that reflects their production environment prior to installation. In addition, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are [not accessible from the Internet](#).
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Mientras que quienes tratan los problemas de ciberseguridad en ICS sugieren su aislamiento físico, quienes pregonan Industria 4.0 proponen su hiper-conexión.

Este es un problema abierto de gran importancia.



Contenido de esta Presentación

Una Introducción a Industria 4.0

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

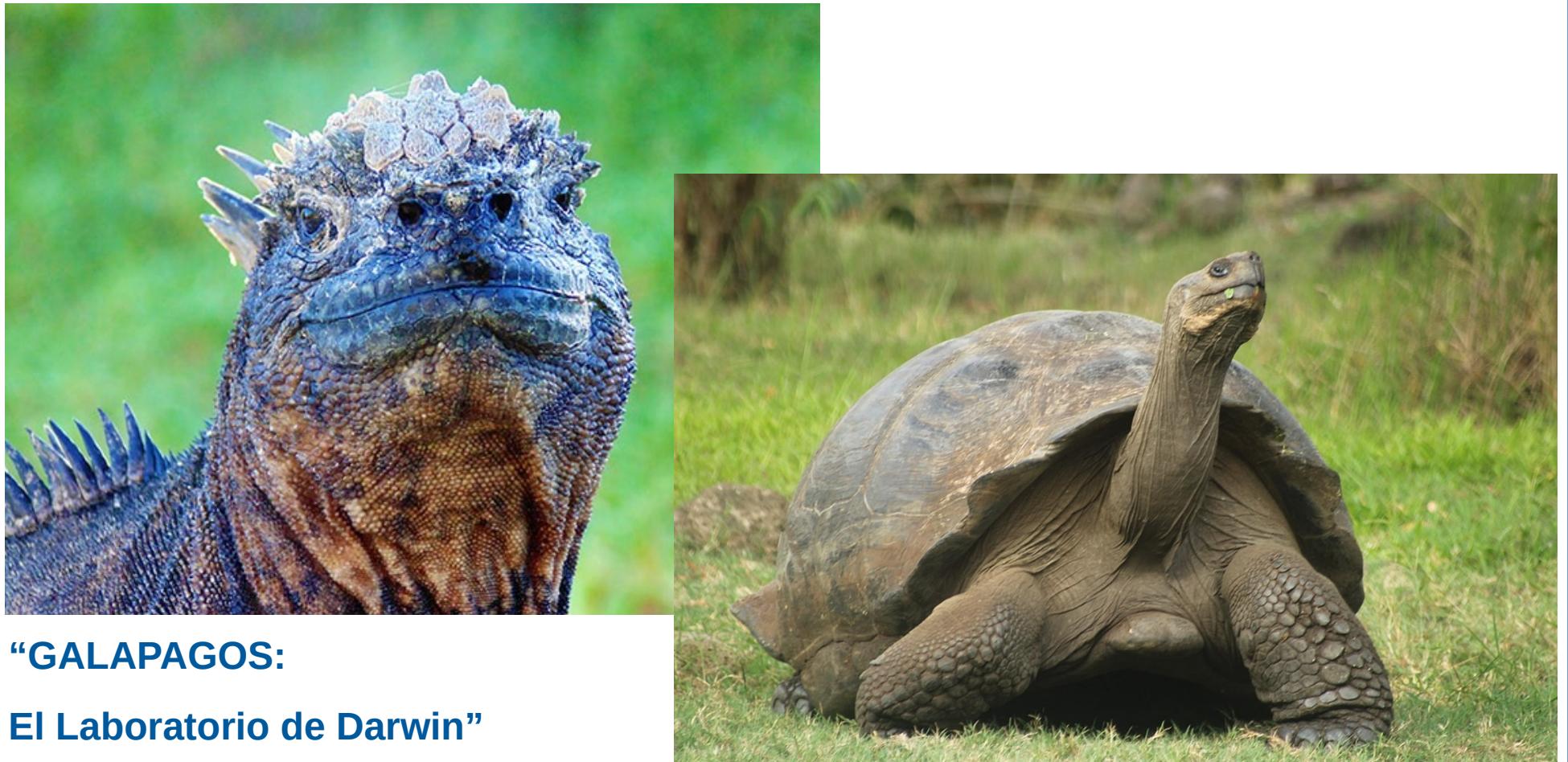
Seguridad en Tecnologías Operacionales

Avances de Nuestro Proyecto

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Dónde estamos...

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales



**“GALAPAGOS:
El Laboratorio de Darwin”**

Imágenes obtenidas de:

https://es.wikipedia.org/wiki/Archivo:Tortuga_Islands_Gal%C3%A1pagos_2.jpg

<https://www.unccruise.com/destinations/galapagos-cruise>

Universidad FASTA: Ciberseguridad y Análisis Forense de entornos Industriales - 1/7/2022

Jorge.kamlofsky@uai.edu.ar

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

OT: ni mejor, ni peor que IT. Es diferente.



**“GALAPAGOS:
El Laboratorio de Darwin”**

Imágenes obtenidas de:

https://es.wikipedia.org/wiki/Archivo:Tortuga_Islands_Gal%C3%A1pagos_2.jpg

<https://www.uncruise.com/destinations/galapagos-cruise>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

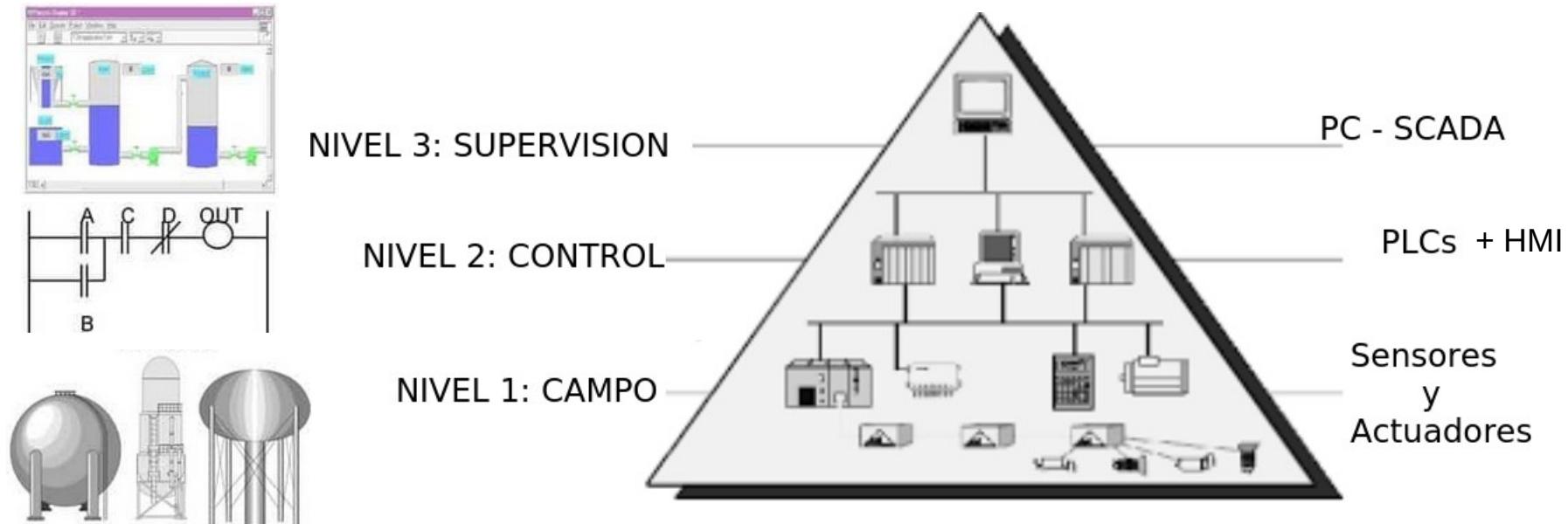
La Automatización en una Industria



Imagen de una planta automotriz

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Los niveles de un Sistema de Control Industrial clásico



Esquema con los niveles de un Sistema de Control Industrial clásico

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Entradas Digitales

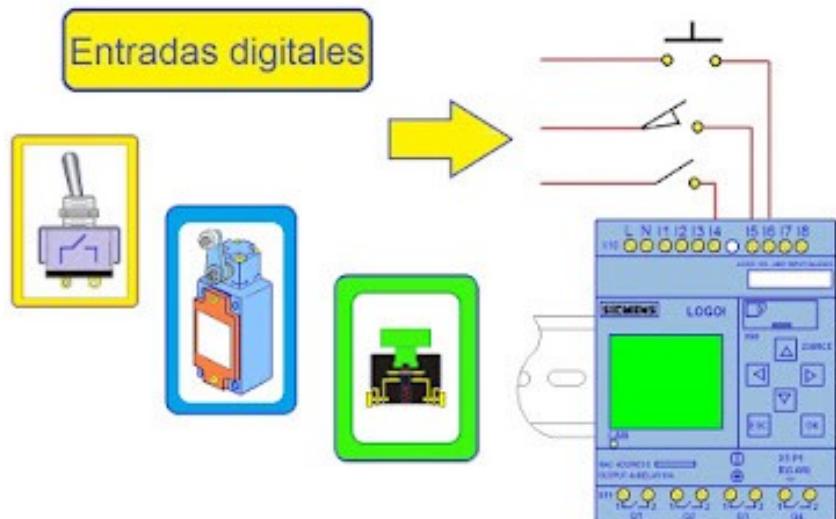
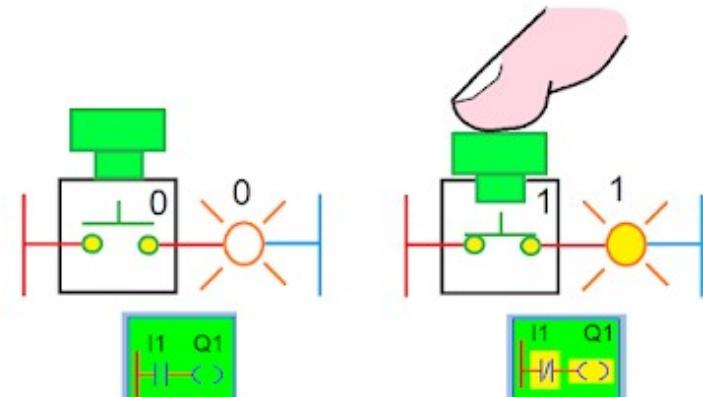


Diagrama de Conexión



La entrada en el programa

Parámetro	Condición	Mínimo	Máximo	Unidades
Tensión de entrada		10	30	Vdc

Tabla de tensiones

Fuentes:

- (1) <https://coparoman.blogspot.com/2019/08/entradas-digitales-en-equipo-de-control.html>
- (2) https://www.exemys.com/beta/docs/spanish/GRD_UM/ApendiceC.html

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Entradas Digitales



Microswitch fin de carrera (1)



Sensores ópticos (2)



Sensores magnéticos (3)

Imágenes obtenidas de:

- (1) <https://www.abcelectronica.net/productos/interruptores/microswitch/>
- (2) <https://madera-sostenible.com/maquinaria/sensores-opticos-distancia-siko-lat170-la060/>
- (3) <https://www.nortechcontrol.com/products/vehicle-detection-and-parking/inductive-loop-detectors/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Entradas Analógicas

Uso de 4 – 20 mA:

Estándar industrial hace más de 50 años, gran variedad de equipos en el mercado

Considerando la 1º ley de Kirchhoff, la corriente medida en cualquier punto del lazo siempre es la misma. Por lo tanto un lazo 4-20 mA tendrá mayor precisión que cualquier señal de tensión

Es más estable en largas distancias y más inmune a los ruidos eléctricos, interferencias electromagnéticas o de radio frecuencia

Considerando al valor 4 mA como 0% de la señal, es muy fácil detectar fallas en el cableado o circuito abierto.

Fuente: <https://www.cpi.com.ar/notas/por-que-4-20-ma/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Entradas Analógicas



Sensores de Temperatura (1)



Caudalímetros (2)



Sensores de Presión (2)

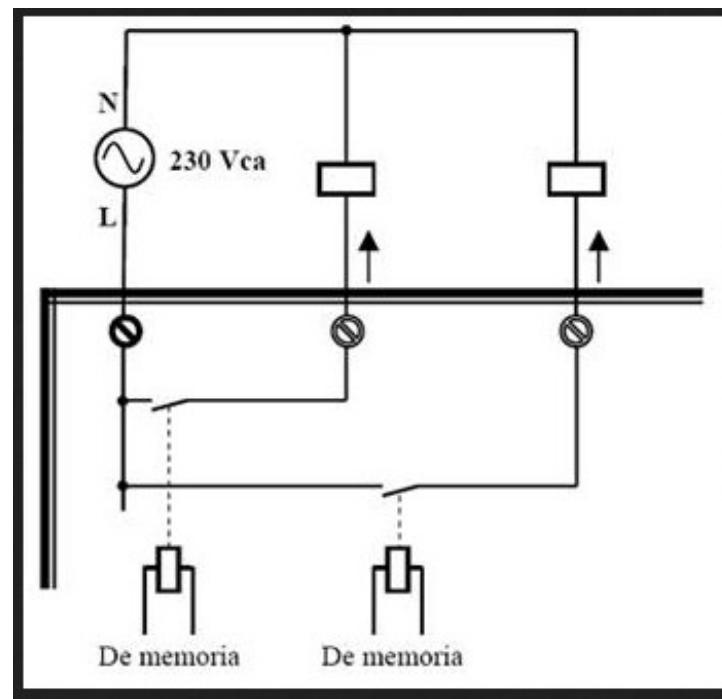
Imágenes obtenidas de:

- (1) http://www.infopl.net/noticias/item/106463-balluf-sensores-temperatura-robustos-procesos-pequena-escala_
- (2) http://www.phelectronica.com.ar/lista_productos.php?cat=11&tipo=Caudalimetros
- (3) <https://www.dycor.com/what-do-we-do/process-control-data-acquisition/sensors/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Salidas Digitales

Las Salidas a relé son las más utilizadas, libres de tensión, pudiendo gobernar cualquier actuador, ya sea a corriente continua o alterna.



Fuente: <https://www.enerxia.net/portal/index.php/i-auto/941-automatismos-partes-de-un-plc-salidas-digitales>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Salidas Digitales



Relé o Relevador Omron



Válvulas Industriales

Imágenes obtenidas de:

<https://cpi.com.ar/nuevos-productos/rele-my-omron/>

Industrias Belg-W: <https://www.belg-w.com/actuadores>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Salidas analógicas

Las Salidas Analógicas son valores de parámetros principalmente eléctricos que interactúan desde el PLC hacia una Carga que se transmite en Corriente 4-20mA ó en la forma más común por Voltaje 0-10V, se escala el valor de la salida en el PLC en valor Voltaje.



**FUENTE
220/24VCC**



PLC LOGO 220VAC



MODULO AM2-2AQ

Fuente: <https://www.electricalchile.cl/plclogosiemens6.php>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 1: Campo – Salidas Analógicas



Actuador Neumático



Actuador Proporcional (y cable)



Imágenes obtenidas de:
<http://jjbcn.com/producto/i/>
<https://www.electricalchile.cl/plclogosiemens6.php>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs

¿Qué es un PLC?

Es una computadora industrial que usa la ingeniería para la automatización de procesos y tiene como finalidad, que las máquinas desarrollen efectivamente todos los sistemas que la componen.

Gracias a estas bondades los PLC se han convertido en una herramienta fundamental para el desarrollo tecnológico de las industrias y todo el entorno social.

Fuente: <https://industriasmgl.com/blogs/automatizacion/que-es-un-plc-y-como-funciona>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs



Un tablero de Control Industrial

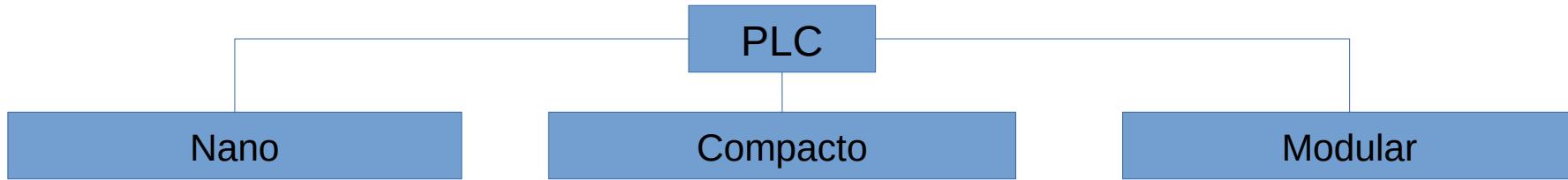
Imagen obtenida de: <https://new.abb.com/low-voltage/products/wire-cable-management/tnb-europe/panel-builder>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs. Clasificación

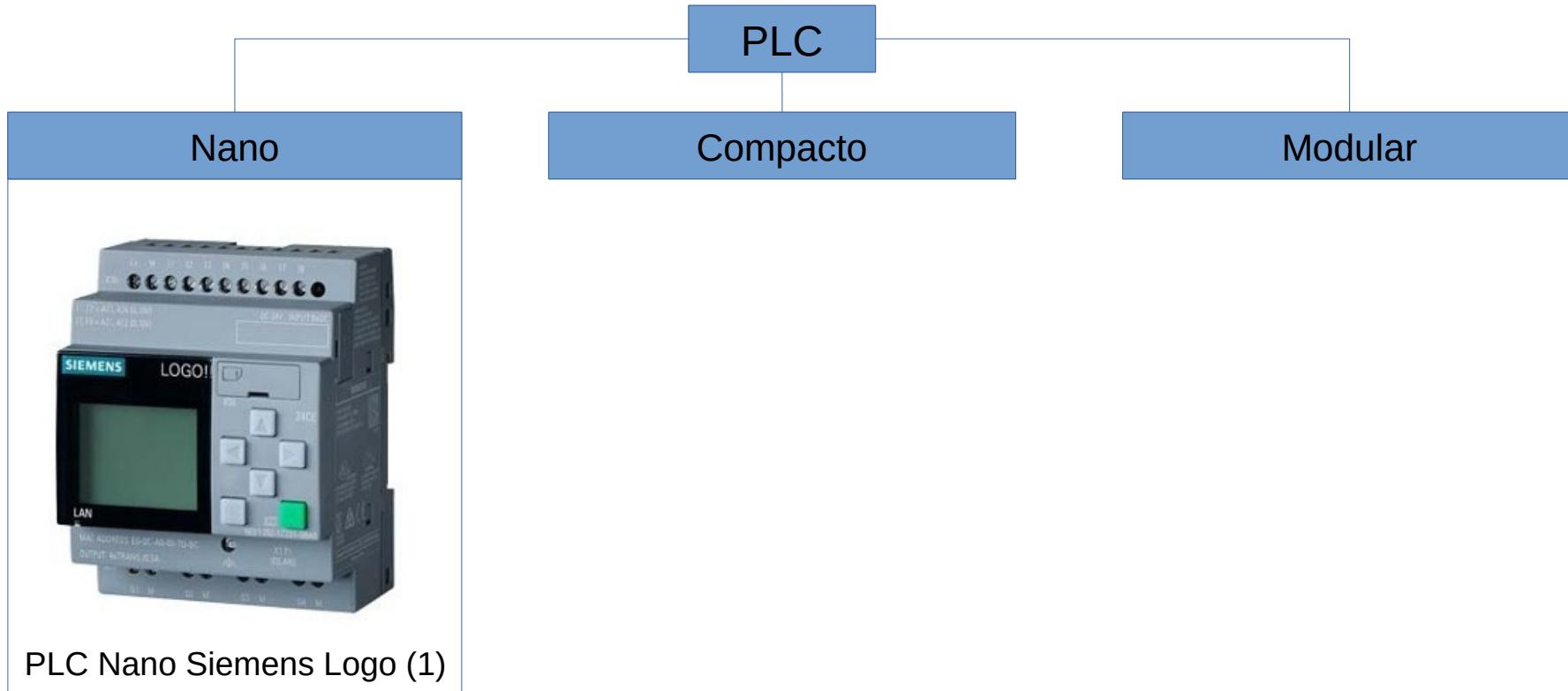
Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs. Clasificación



Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs. Clasificación



Imágenes obtenidas de:

- (1) <https://listado.mercadolibre.com.ar/plc-logo-8-siemens>
- (2) <https://www.interempresas.net/HCAV/Companies-Products/Product-PLC-Compact-Omron-Sysmac-CP1-53246.html>
- (3) <https://www.indiamart.com/proddetail/quantum-cpu-modicon-plc-4690961088.html>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs. Clasificación

PLC

Nano

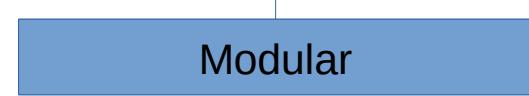


PLC Nano Siemens Logo (1)

Compacto



Modular



PLC Compacto Omron CP1 (2)

Imágenes obtenidas de:

- (1) <https://listado.mercadolibre.com.ar/plc-logo-8-siemens>
- (2) <https://www.interempresas.net/HCAV/Companies-Products/Product-PLC-Compact-Omron-Sysmac-CP1-53246.html>
- (3) <https://www.indiamart.com/proddetail/quantum-cpu-modicon-plc-4690961088.html>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Los PLCs. Clasificación



Imágenes obtenidas de:

- (1) <https://listado.mercadolibre.com.ar/plc-logo-8-siemens>
- (2) <https://www.interempresas.net/HCAV/Companies-Products/Product-PLC-Compact-Omron-Sysmac-CP1-53246.html>
- (3) <https://www.indiamart.com/proddetail/quantum-cpu-modicon-plc-4690961088.html>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Interfaz Hombre / Maquina (HMI)

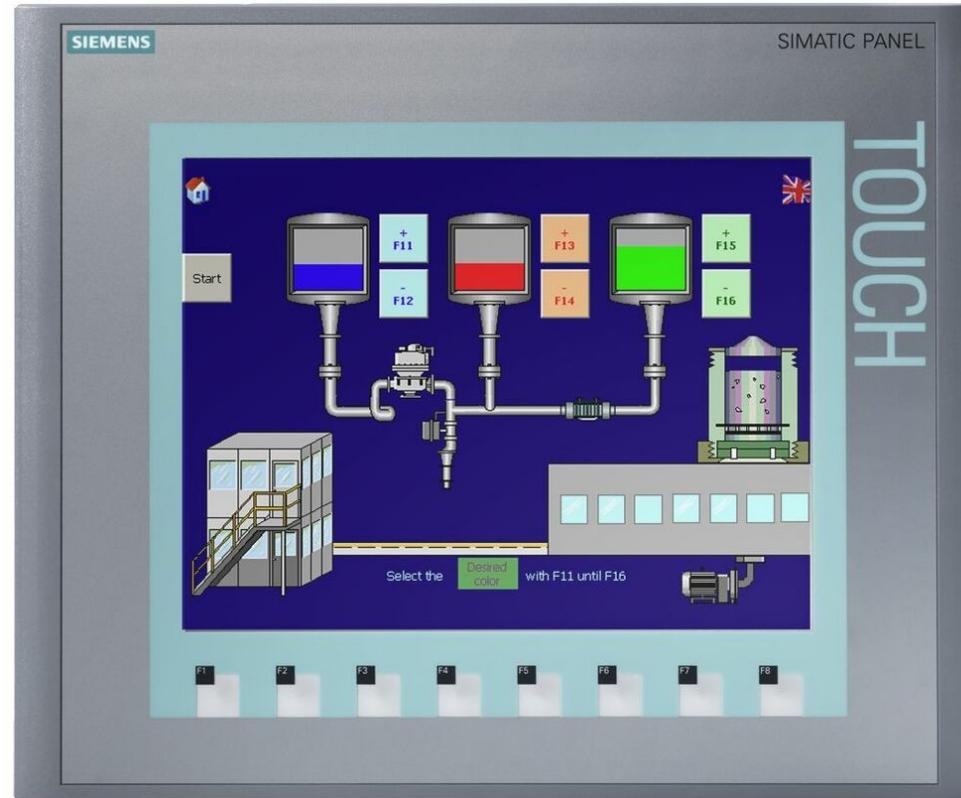


Interfaz de operación de equipos industriales: botones, llaves y lámparas.

Imagen obtenida de: <http://indpanels.com/spark-conversation-electrical-code-safety-meet-greet-st-joe-missouri/control-panel-with-switches-and-lamps/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Interfaz Hombre / Maquina (HMI)



Panel Táctil Siemens Simatic

Imagen obtenida de: <https://www.ebay.es/item/Siemens-6AV6647-0AE11-3AX0-SIMATIC-HMI-KTP1000-BASIC-COLOR-DP-KEY-TOUCH-/260992728442>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 2: Control – Interfaz Hombre / Maquina (HMI)



HMI de campo con Pantalla

Imagen obtenida de: <http://buffaloadv.com/asa/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – La Supervisión de los Sistemas de Control Industrial

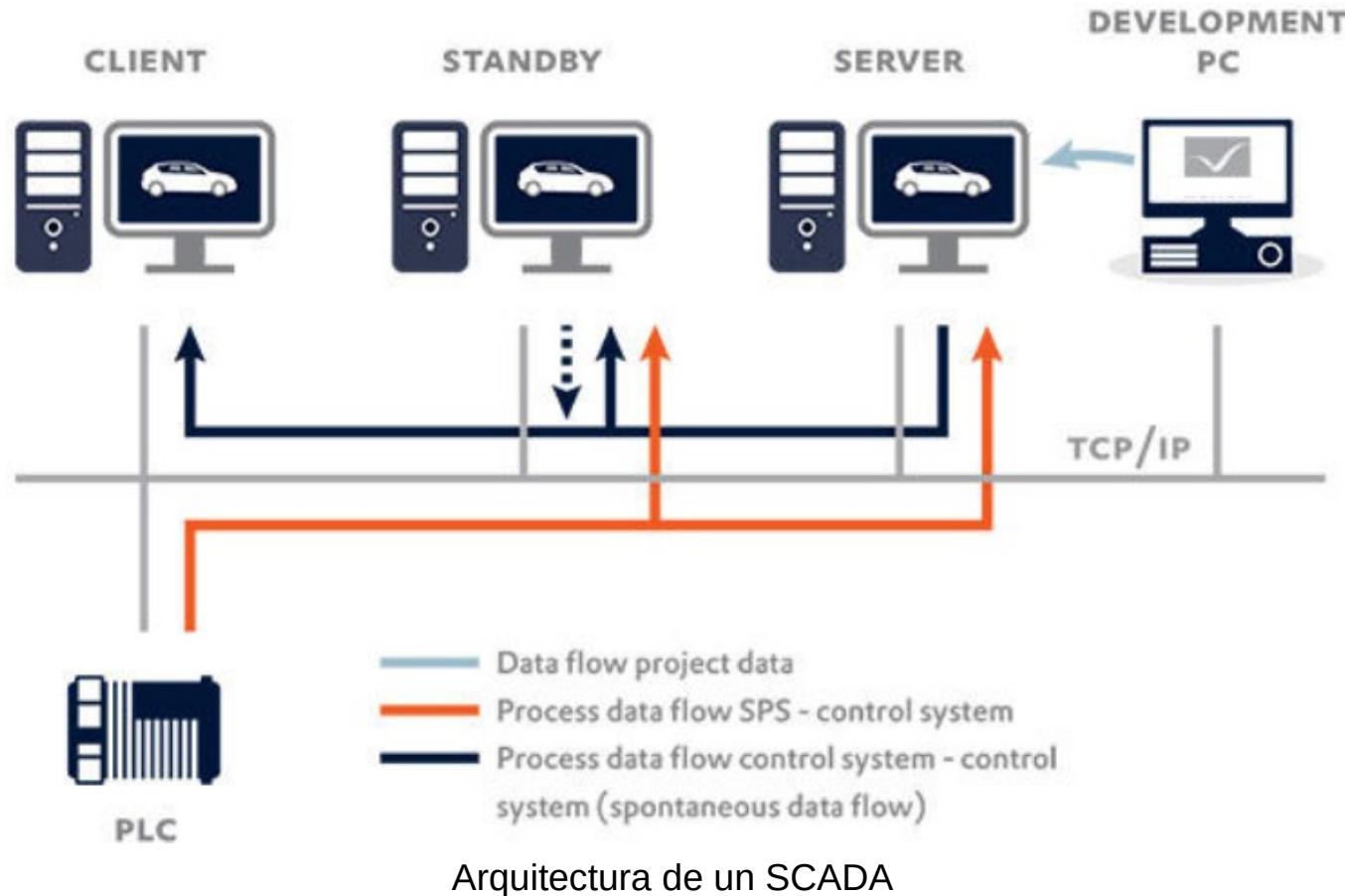


Imagen: <https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – La Supervisión de los Sistemas de Control Industrial

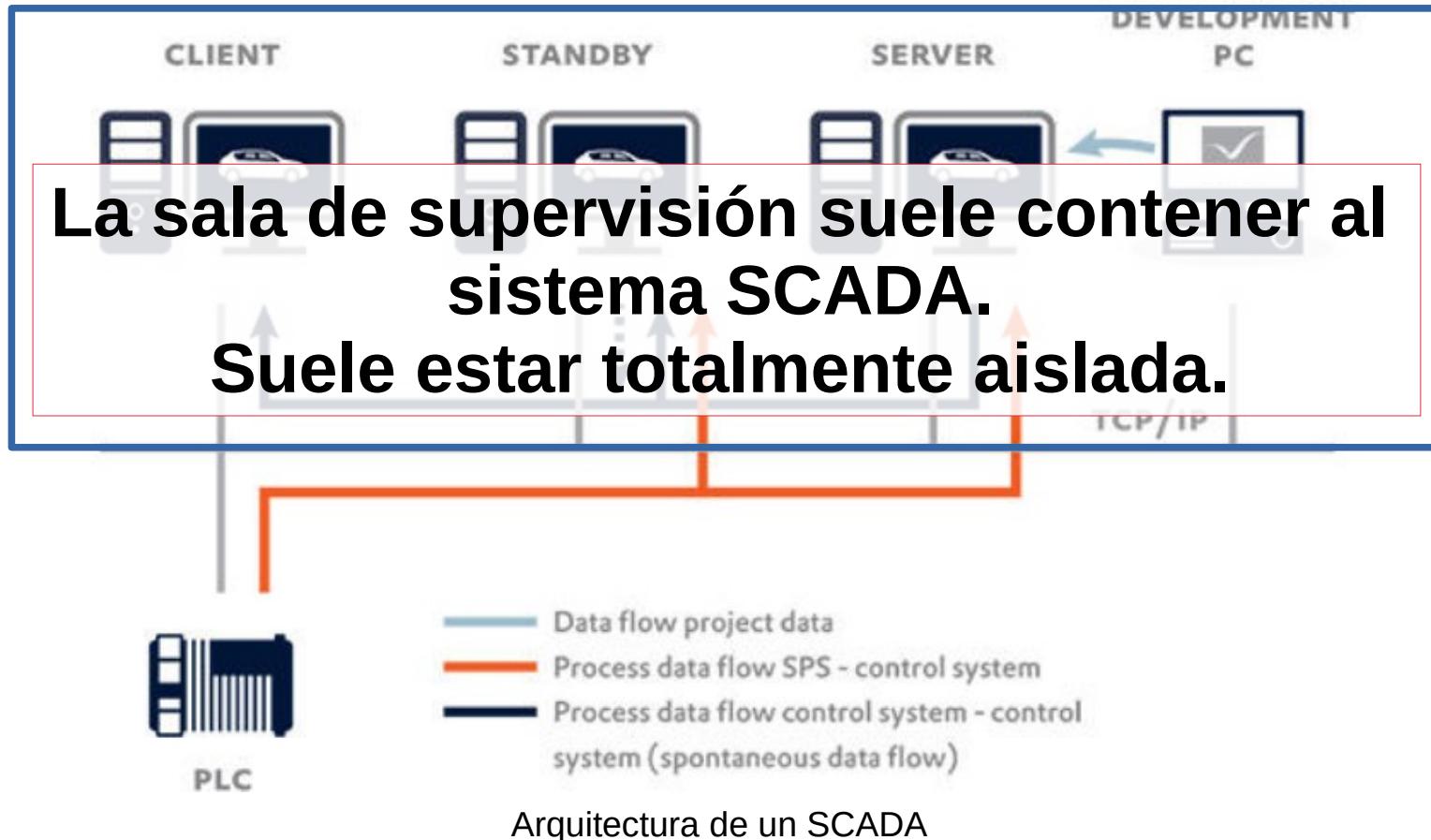


Imagen: <https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – La Supervisión de los Sistemas de Control Industrial



Imagen de una sala de supervisión con un SCADA

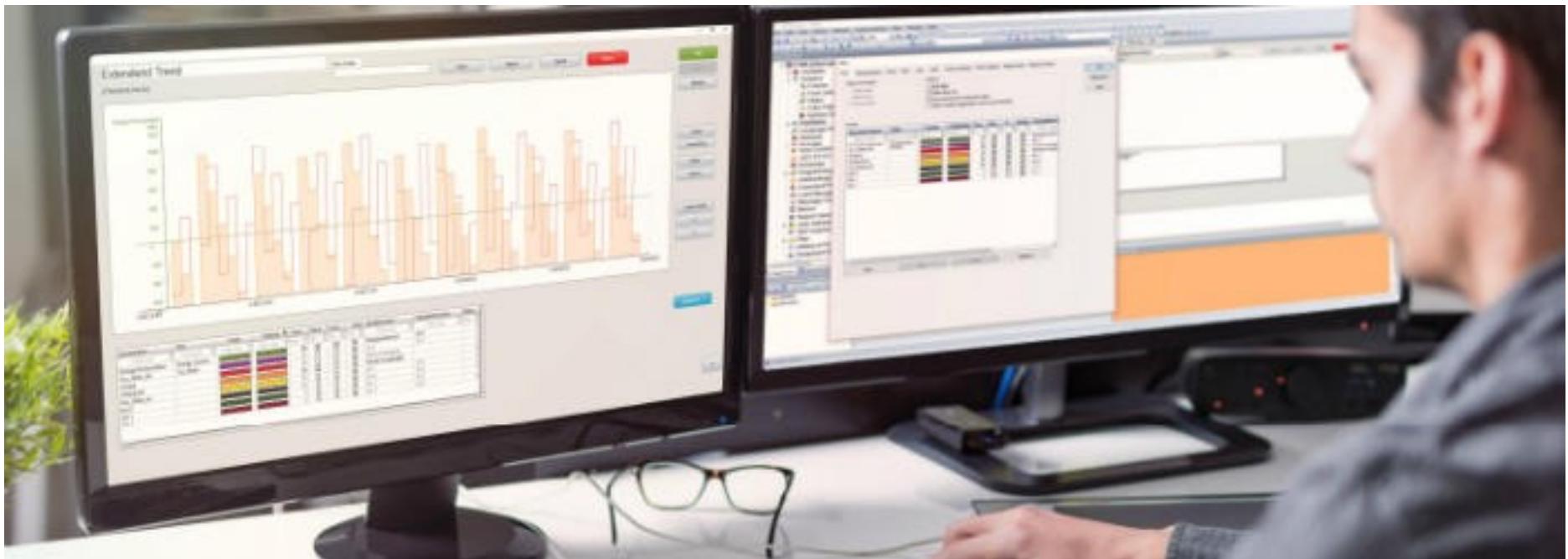
Imagen: <https://www.virtualpro.co/noticias/control-de-sistemas--ejemplos-y-aplicaciones>

Universidad FASTA: Ciberseguridad y Análisis Forense de entornos Industriales - 1/7/2022

Jorge.kamlofsky@uai.edu.ar

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – La Supervisión de los Sistemas de Control Industrial



Pantallas de un Cliente SCADA

Imagen: <https://www.copadata.com/es/productos/zenon-software-platform/visualizacion-control/que-es-scada/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – La Supervisión de los Sistemas de Control Industrial



Pantalla de una terminal de Ingeniería de un SCADA (Wonderware)

Imagen obtenida de: <https://www.gea.com/it/products/gea-otas-brewery.jsp>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – Infraestructuras Críticas Industriales

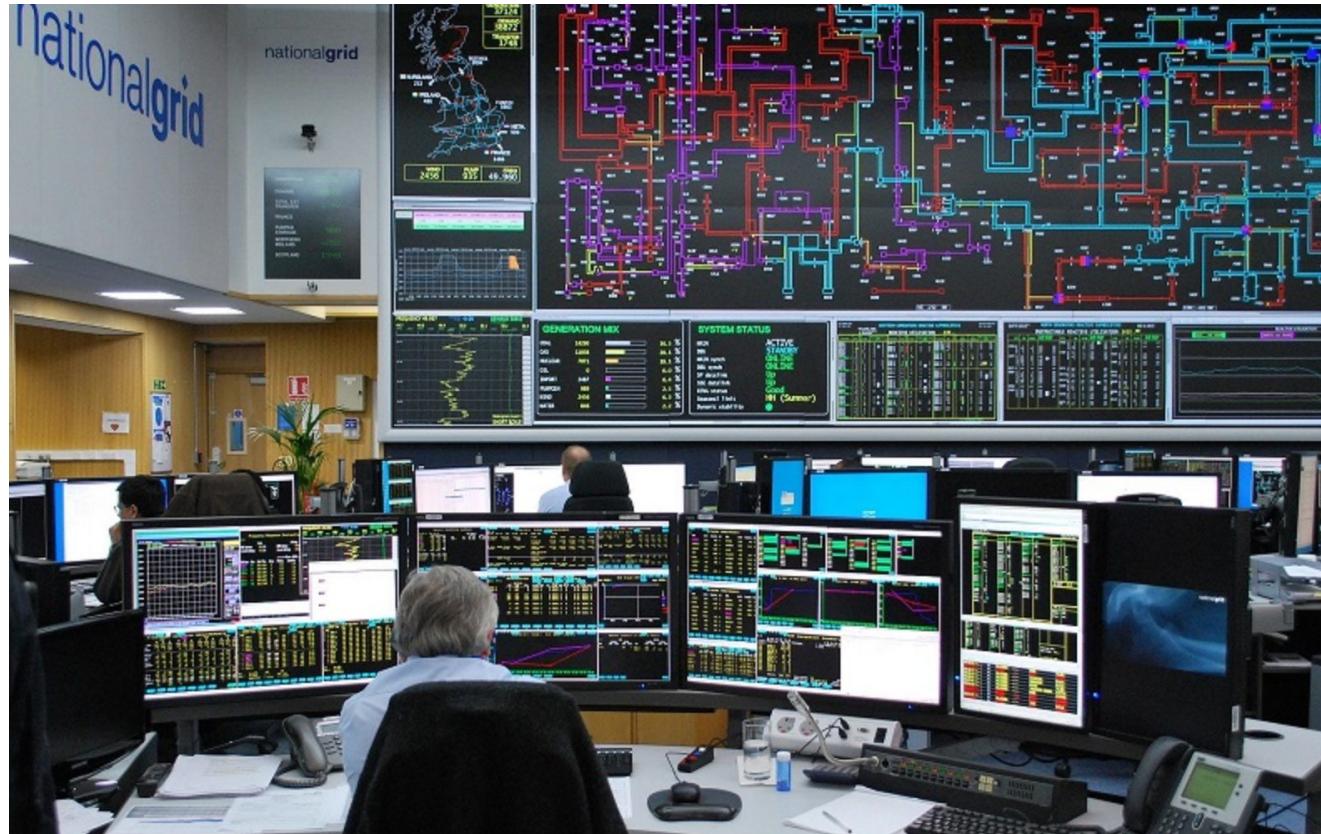


Imagen del SCADA del sistema de distribución de Gas Neoyorquino National Grid

Imagen obtenida de: <https://www.current-news.co.uk/news/cyber-attacks-rise-of-distributed-generation-among-top-risks-to utilities>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – Infraestructuras Críticas Industriales



Imagen de un SCADA del sistema de infraestructuras críticas canadiense

Imagen obtenida de: <https://48cubes.com/canada-not-doing-enough-to-protect-critical-infrastructure/>

Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Nivel 3: SCADA – Infraestructuras Críticas Industriales

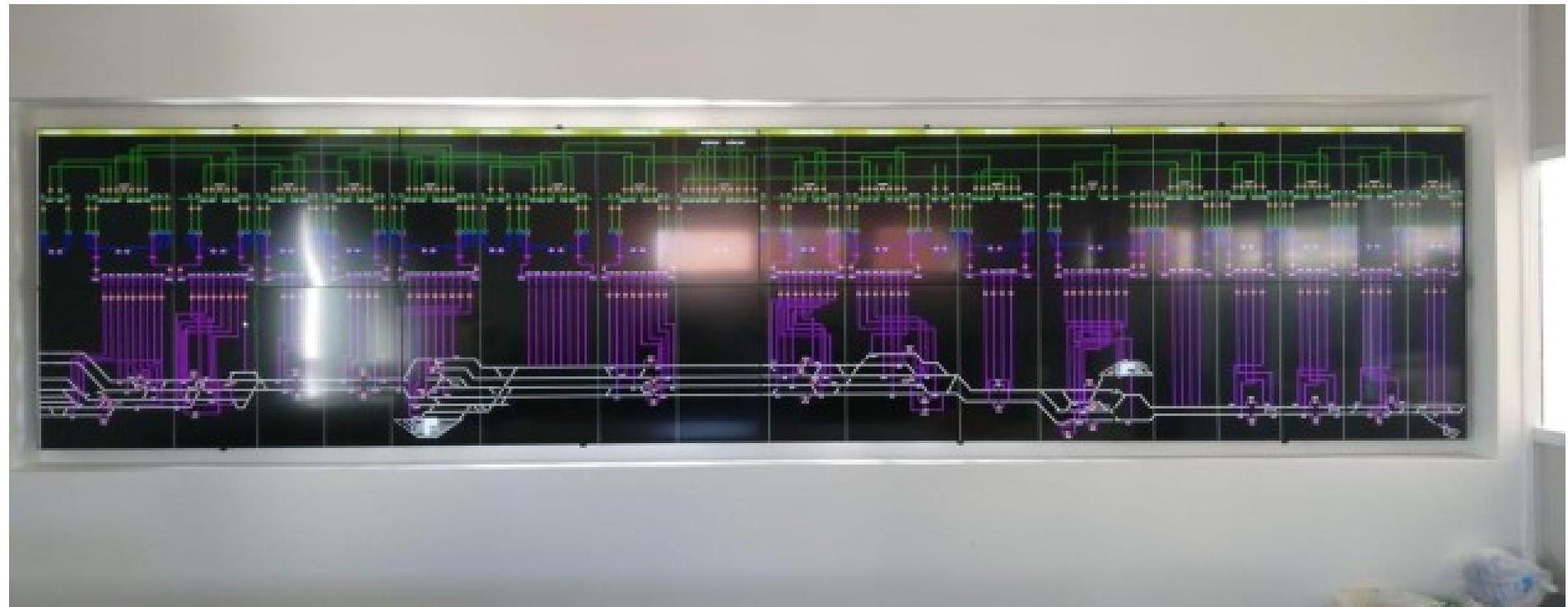
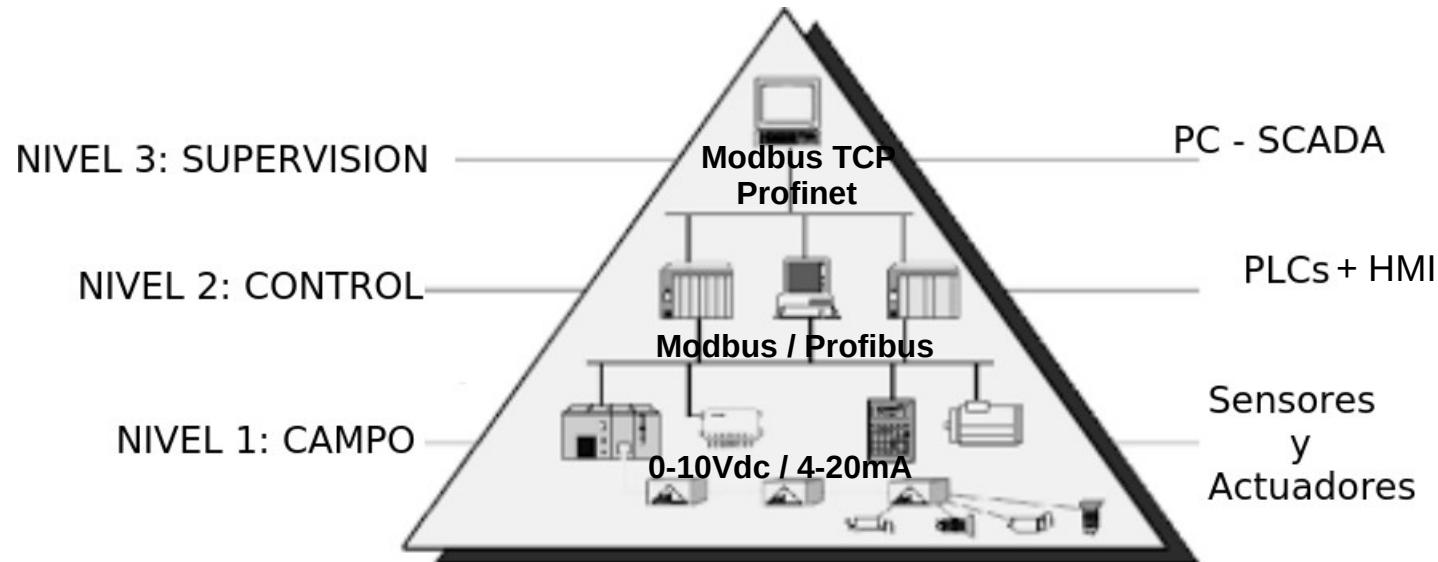


Imagen del SCADA del sistema de administración y control de energía del FFCC Sarmiento

Imagen obtenida de la presentación realizada por la empresa Trend Ingeniería en la Jornada de Automatización Industrial realizada el 21-06-2019 en la Universidad Abierta Interamericana

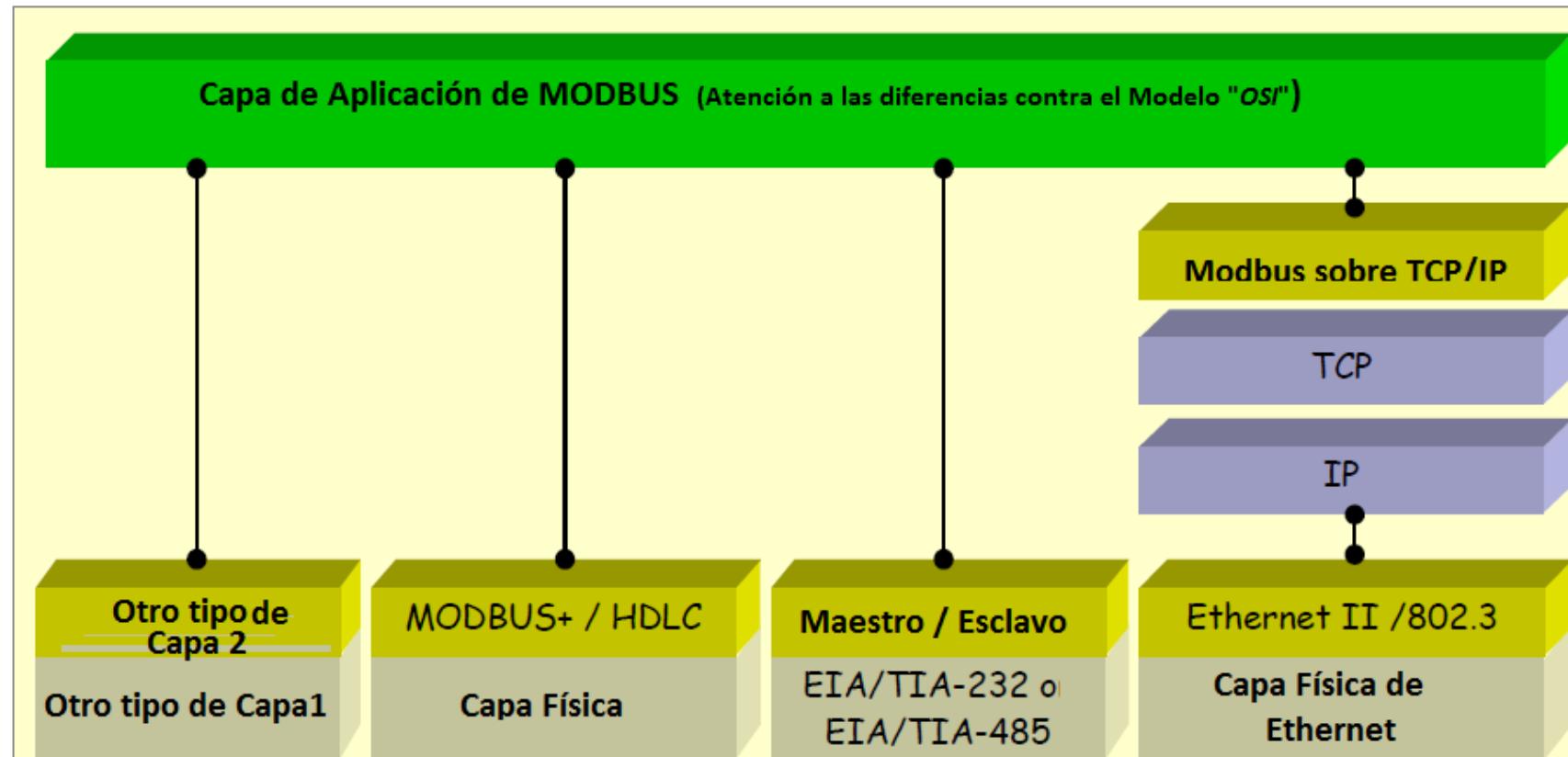
Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Las Comunicaciones



Los Sistemas de Control Industrial (ICS): Las Tecnologías Operacionales

Las Comunicaciones



Esquema del protocolo Modbus

Imagen obtenida de:

Colombo, H. Presentación: Proyecto: CIDEI/CRIPTO “Ciber” Defensa en Entornos industriales. Protocolo Modbus ¿Dónde incluir las Digraffías?. Universidad Abierta Interamericana, (2015).

Contenido de esta Presentación

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

Seguridad en Tecnologías Operacionales

Resumen de Nuestro Proyecto

Seguridad en Tecnologías de la Información

En el mundo TI se dispone de amplia experiencia en el tratamiento de los problemas de Seguridad de la Información.

Seguridad en Tecnologías de la Información

Recomendaciones de Buenas Prácticas



Ilustración de ISO27000 (1)



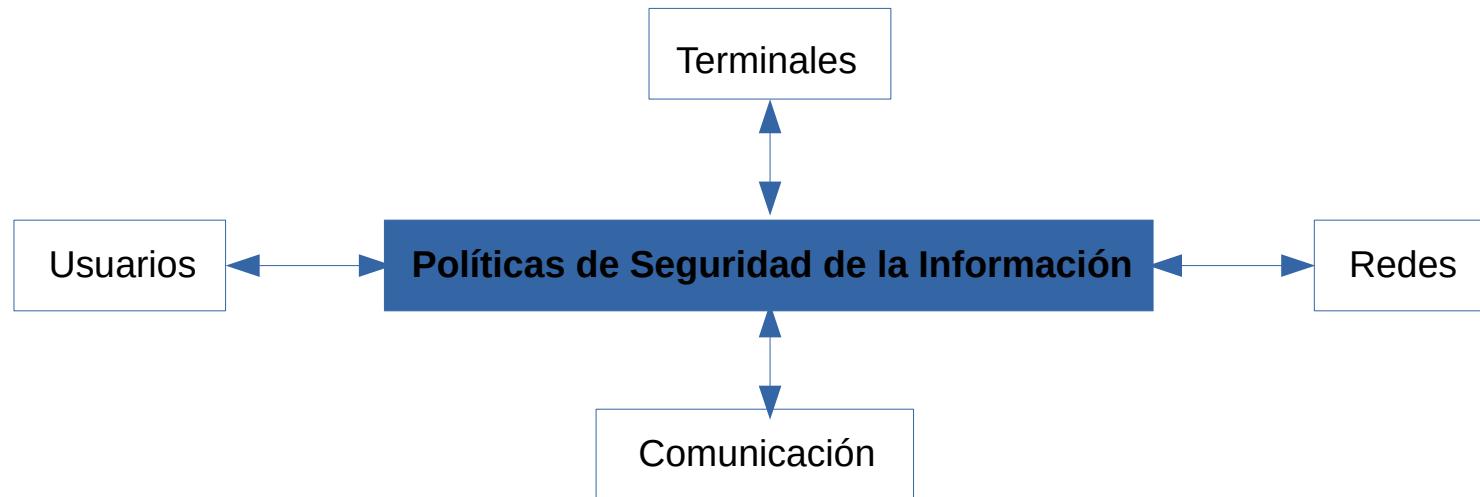
Ilustración de NIST / NSA (2)

Imágenes obtenidas de:

- (1)http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacion.html
- (2) <https://www.muyseguridad.net/2013/11/05/estandares-criptograficos-nist-nsa/>

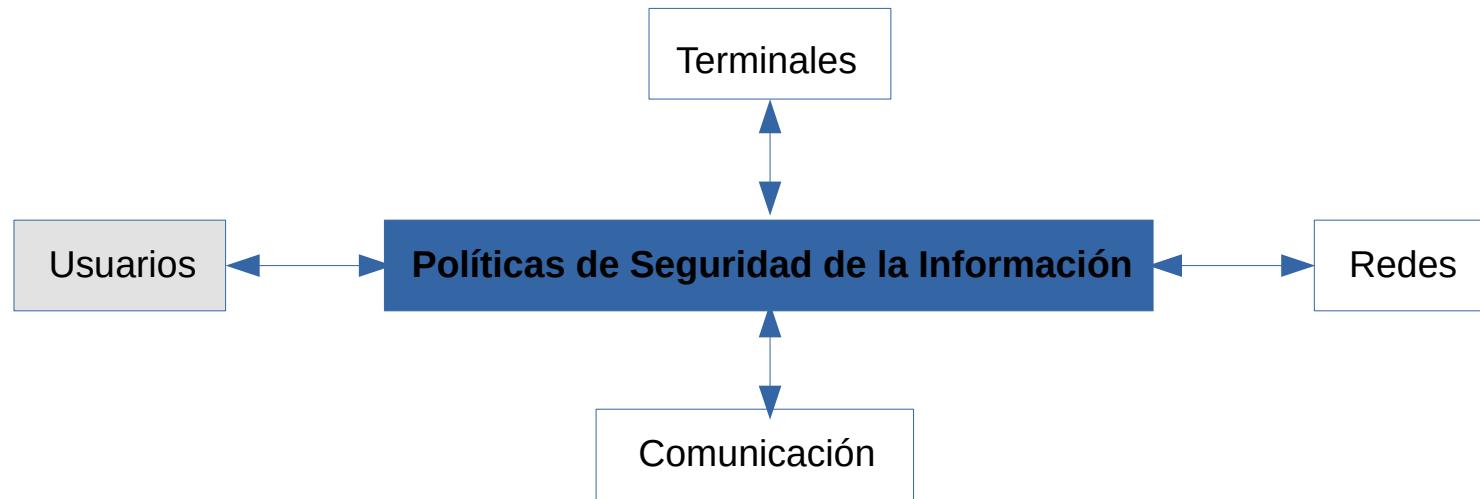
Seguridad en Tecnologías de la Información

Política integral de Seguridad de la Información



Seguridad en Tecnologías de la Información

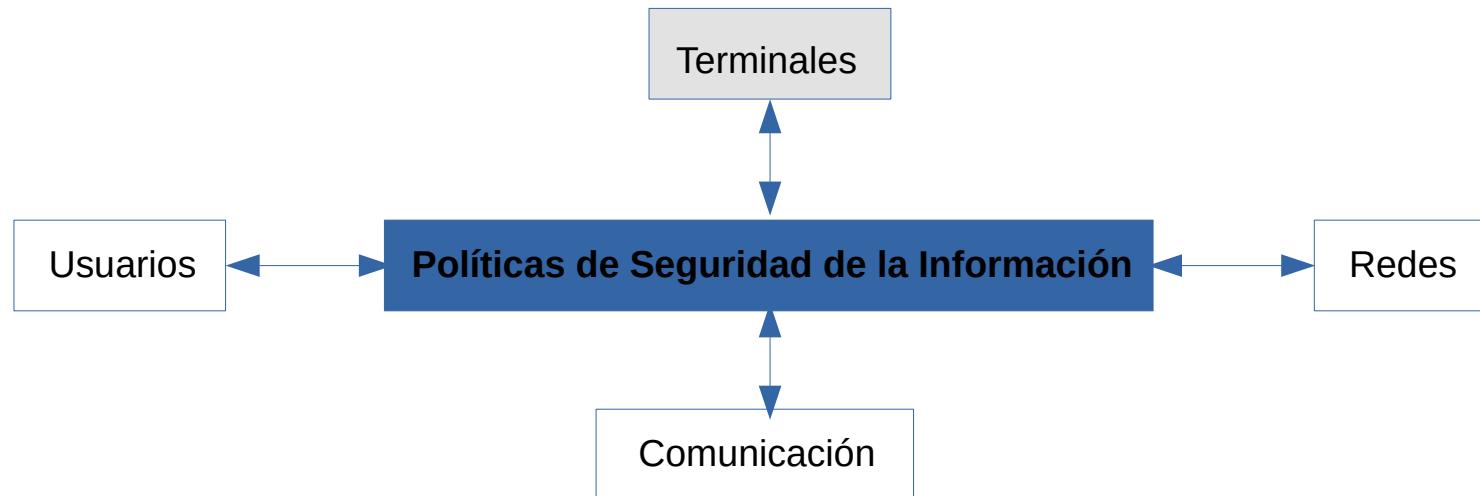
Política integral de Seguridad de la Información



Gran parte de los problemas de Seguridad de la Información se deben a acciones negligentes o a causa de la falta de capacitación de los usuarios.

Seguridad en Tecnologías de la Información

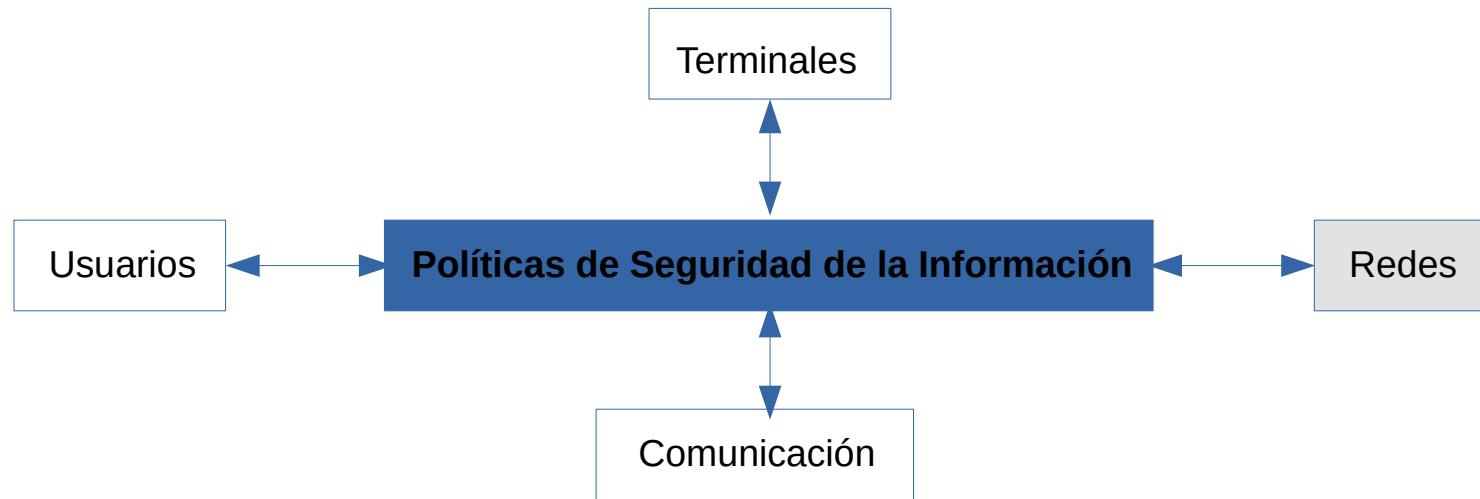
Política integral de Seguridad de la Información



Los terminales no deben presentar vulnerabilidades ante ataques. Tanto el sistema operativo, como el antivirus de todas las terminales deben estar actualizados.

Seguridad en Tecnologías de la Información

Política integral de Seguridad de la Información

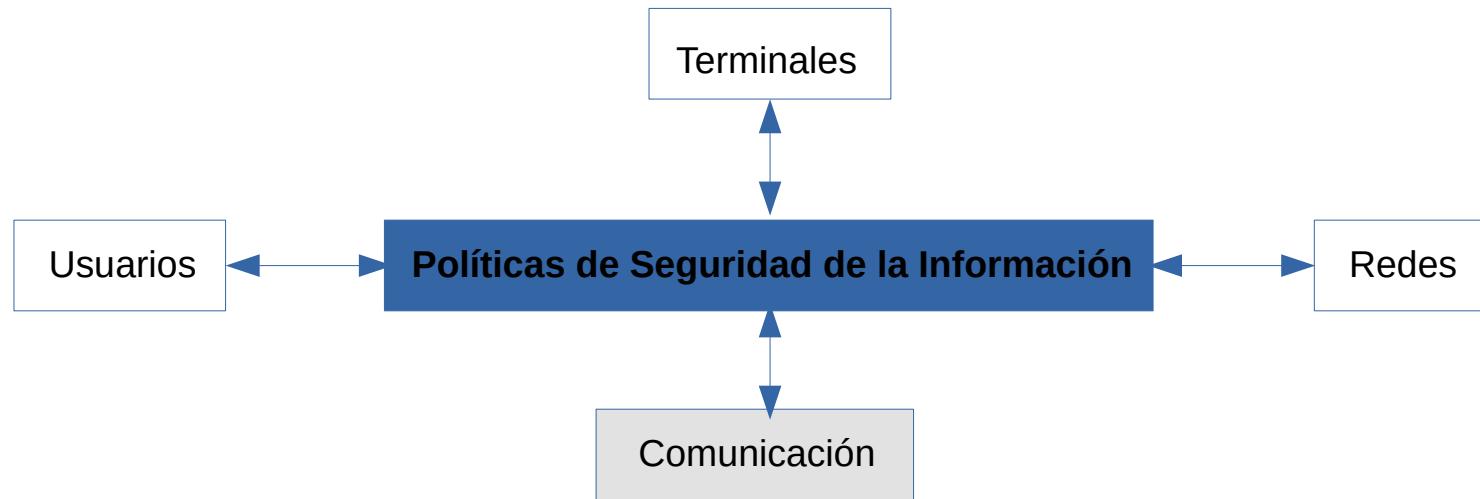


Se debe evitar el acceso de intrusos manteniendo la confidencialidad, integridad, disponibilidad y control de la red.

Es útil disponer de un sistema de seguridad en capas: cortafuegos, Sistemas de Detección de Intrusos, Sistemas de Prevención de Intrusos, Listas de Control de Accesos y sistemas de autenticación.

Seguridad en Tecnologías de la Información

Política integral de Seguridad de la Información

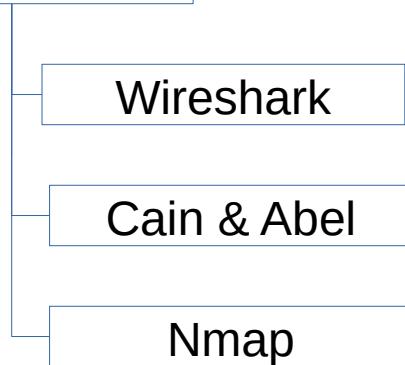


Es recomendable el cifrado de las comunicaciones siempre que sea posible.

Seguridad en Tecnologías de la Información

Herramientas potencialmente muy peligrosas

Herramientas:



- **Wireshark** permite escuchar los puertos, por lo que es posible obtener claves de acceso.
- **Cain & Abel** copia de la red información mediante un ataque del tipo “man in the middle” partiendo de un ataque tipo “ARP-Poisoning”.
- Por otro lado, la herramienta **Nmap** permite escanear puertos de red, lo que permite buscar “víctimas”.

Seguridad en Tecnologías de la Información

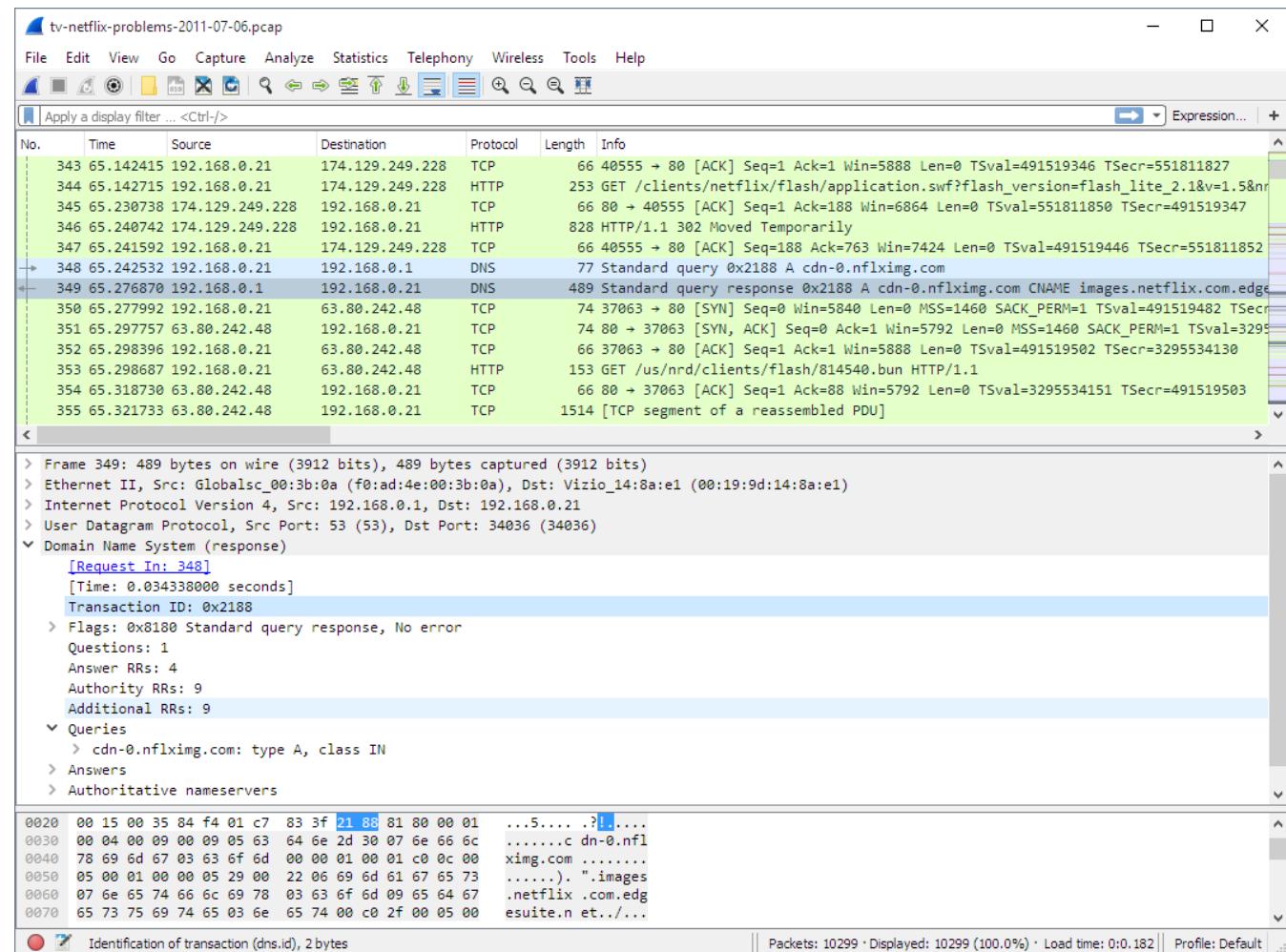
Herramientas potencialmente muy peligrosas

Herramientas:

Wireshark

Cain & Abel

Nmap



Seguridad en Tecnologías de la Información

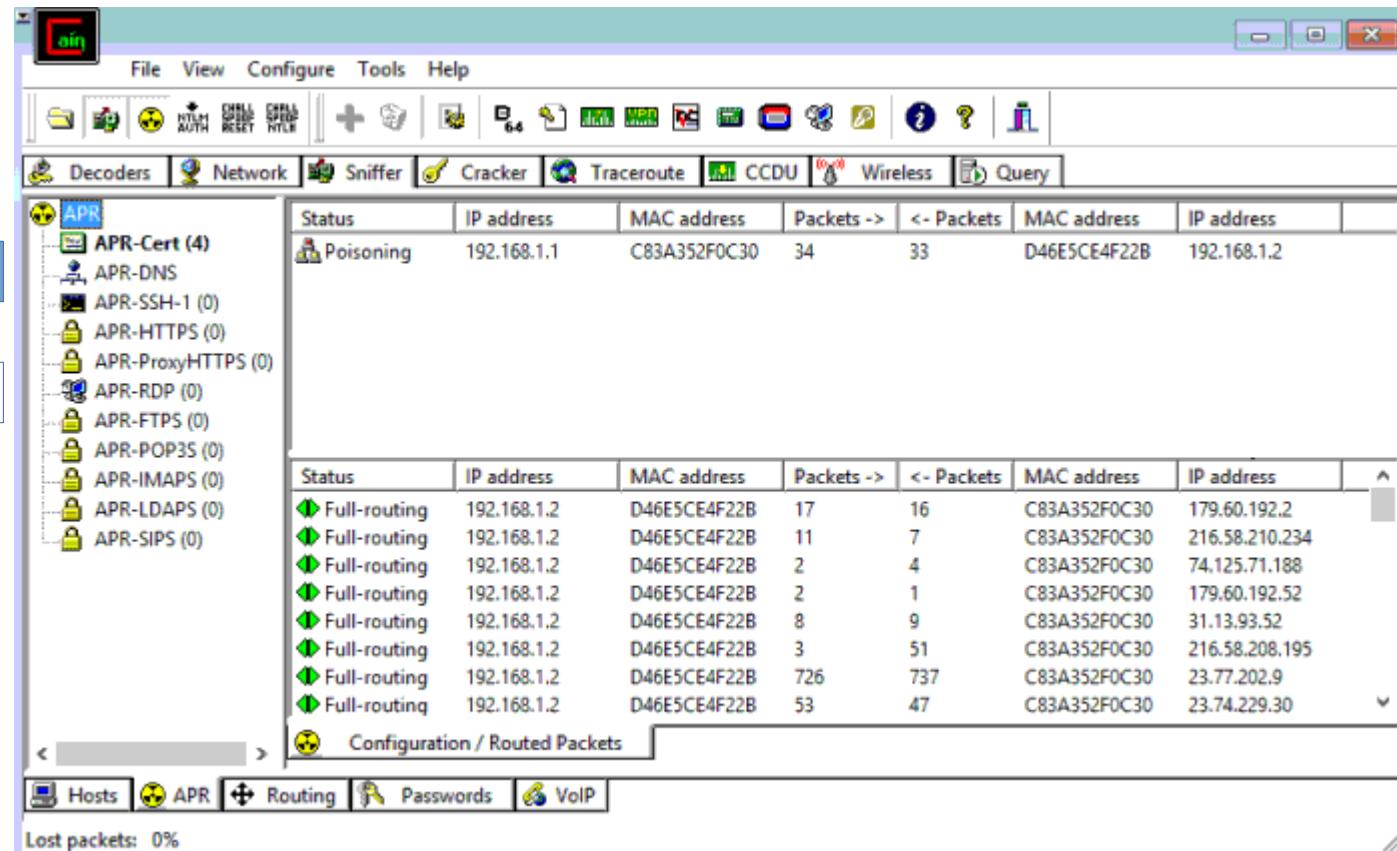
Herramientas potencialmente muy peligrosas

Herramientas:

Wireshark

Cain & Abel

Nmap



Pantalla Principal de Wireshark

Imagen obtenida de: <https://gbhackers.com/man-in-the-middle-attack-with-cain-and-abel-tool/>

Seguridad en Tecnologías de la Información

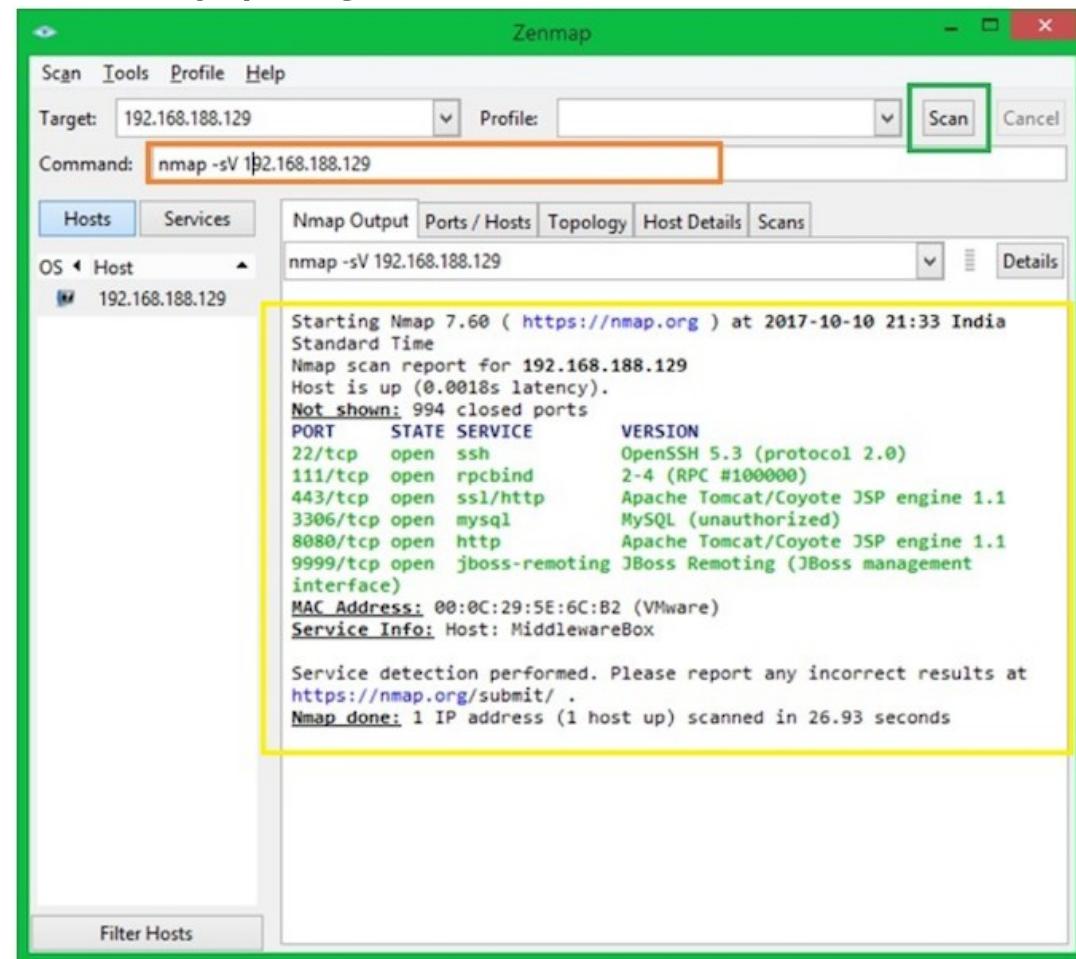
Herramientas potencialmente muy peligrosas

Herramientas:

Wireshark

Cain & Abel

Nmap



Contenido de esta Presentación

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

Seguridad en Tecnologías Operacionales

Resumen de Nuestro Proyecto.

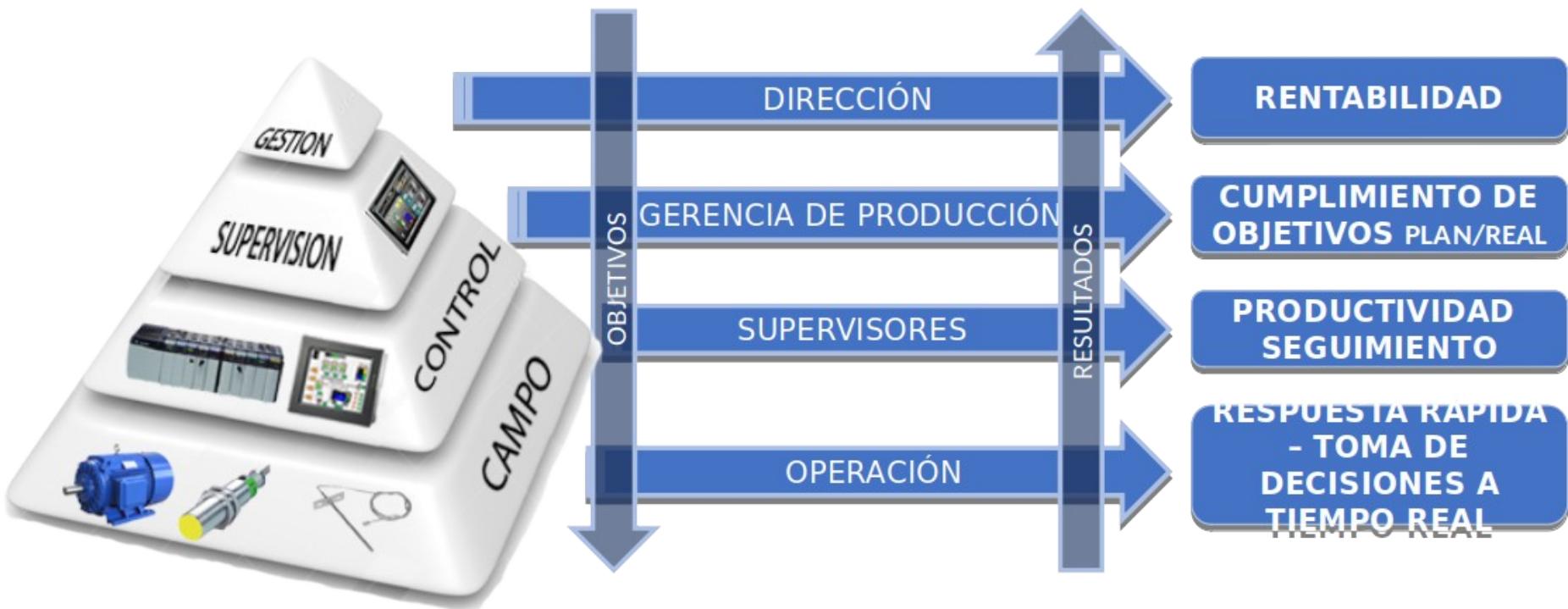
Seguridad en Tecnologías Operacionales

Seguridad por Ocultamiento

Frente a los problemas de Seguridad Informática, el mundo OT optó por aislar sus sistemas de las redes.

Seguridad en Tecnologías Operacionales

La interconexión de los sistemas OT

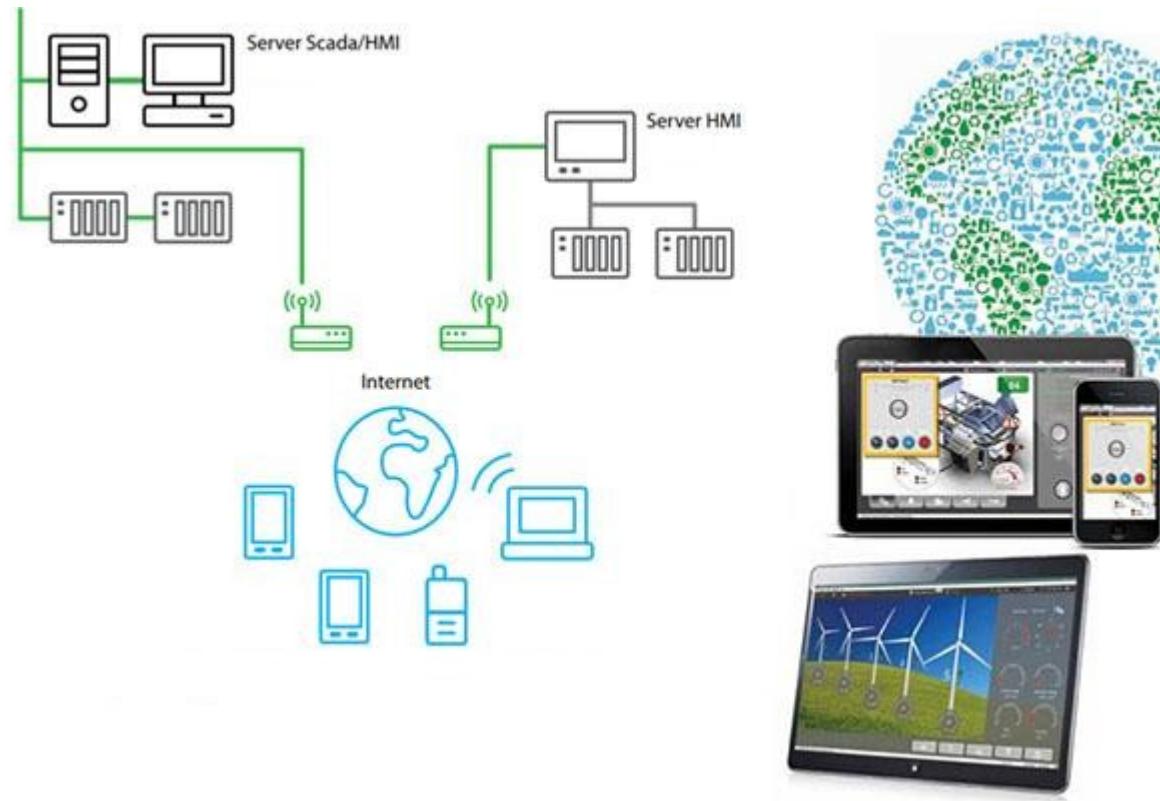


La industrial 4.0: Interconexión entre las tecnologías IT y OT

Imagen obtenida de la presentación realizada por la empresa Trend Ingeniería en la Jornada de Automatización Industrial realizada el 21-06-2019 en la Universidad Abierta Interamericana

Seguridad en Tecnologías Operacionales

La interconexión de los sistemas OT



La industrial 4.0: Interconexión de las tecnologías OT con Internet

Imagen obtenida de: <https://www.contaval.es/scada-movicon-11-6-con-cliente-web-html5/>

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales



Plantas Nucleares de Irán (2011): La planta de enriquecimiento de Urano de Natanz (Irán) fue atacada por el *virus* informático ***Stuxnet***. Este gusano carcome un tipo muy específico de sistema de control industrial fabricado por Siemens.

Fuente: <https://www.wired.com/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/>

Seguridad en Tecnologías Operacionales

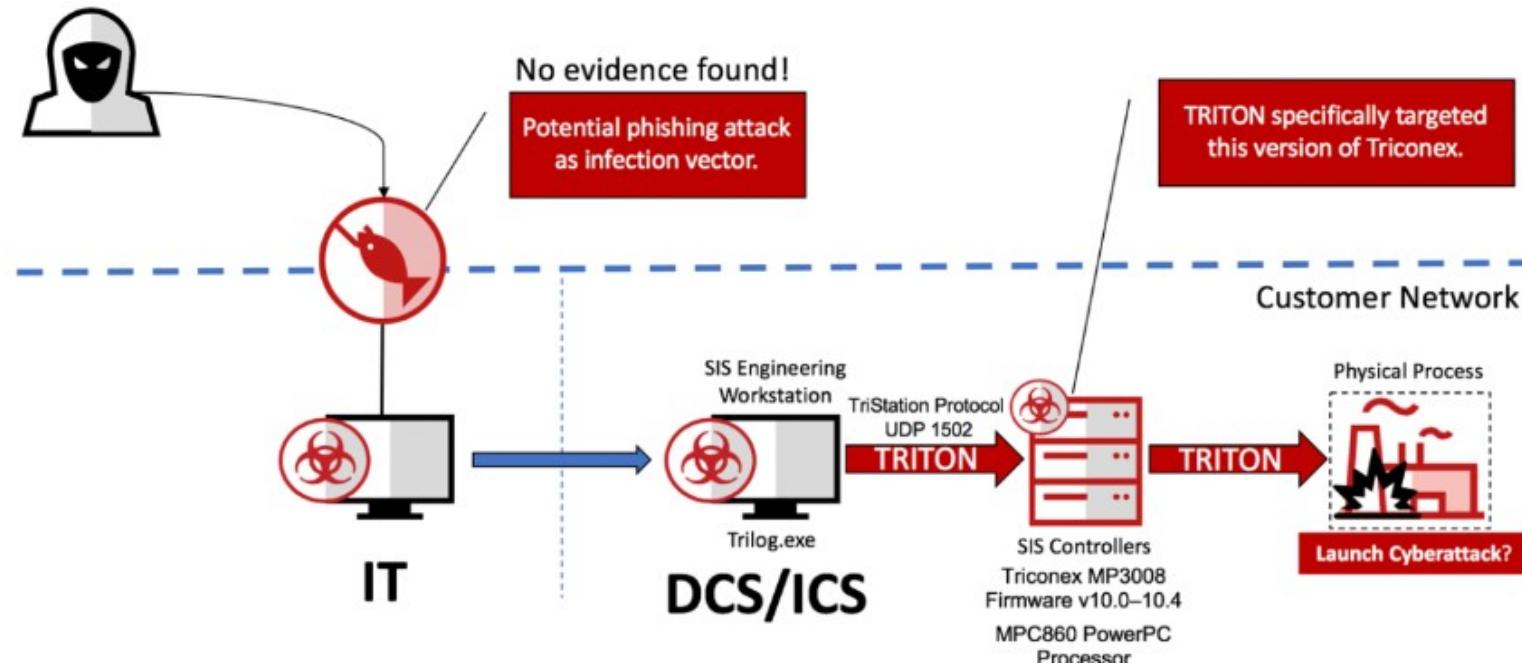
Algunos Ataques a Infraestructuras Críticas Industriales



Distribuidoras eléctricas de Ucrania (2015): El sistema eléctrico de Ucrania ha sido recientemente atacada por malware cuyo objetivo ha sido sabotear los sistemas de control de las infraestructuras públicas. Varias distribuidoras eléctricas fueron comprometidas por el ***troyano BlackEnergy*** el 23 de diciembre (2015), dejando a los hogares de la región ucraniana Ivano-Frankivsk (de una población alrededor de 1,5 millones de habitantes) sin electricidad.

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales

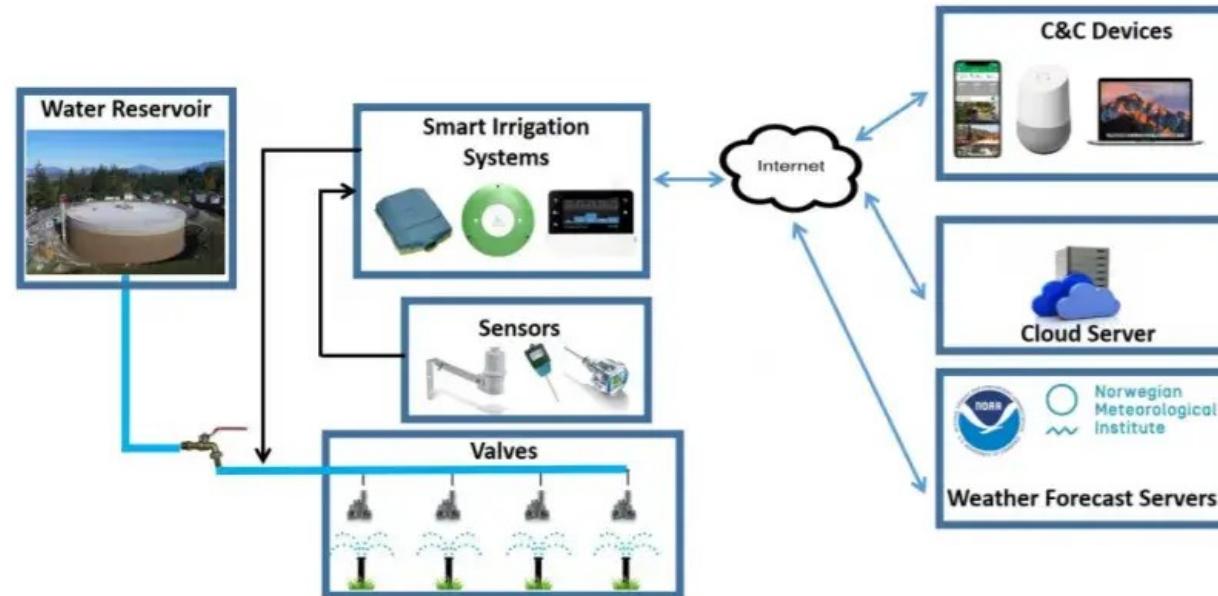


Petroquímica Saudí (2017): Ataque realizado mediante un malware específico para ICS llamado **Triton**. El ataque permitió a los piratas informáticos hacerse cargo de los sistemas de instrumentos de seguridad (SIS) de la planta. *Este código malicioso podría haber provocado una explosión o liberación de gas tóxico. Fue la primera vez que un ataque de este tipo se diseñó para causar la pérdida de vidas.*

Fuente: <https://cnls.lanl.gov/External/GSSlides2021/Sandberg.pdf>

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales



Ataques a Plantas de agua en Israel (2020): Los ataques fueron diseñados para comprometer los sistemas de mando y control del ICS para las estaciones de bombeo, los sistemas de alcantarillado, las plantas de aguas residuales y las bombas agrícolas de Israel. Aunque finalmente fracasaron, los ataques tenían como objetivo intentar aumentar el cloro y otros químicos en el agua a niveles dañinos e interrumpir el suministro.

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales



Potabilizadora de agua de USA (Olsmar (FL), 2021): El intruso accedió a varias funciones que controlan el tratamiento del agua, incluyendo la parte del software que controla los niveles de hidróxido de sodio. En ese momento el atacante procedió a cambiar los niveles de 100 partes por millón a 11.100 partes por millón, saliendo después del sistema. Tras identificarse la intrusión, y tras la identificación del cambio, se restauró los valores modificados por el atacante.

Fuentes:

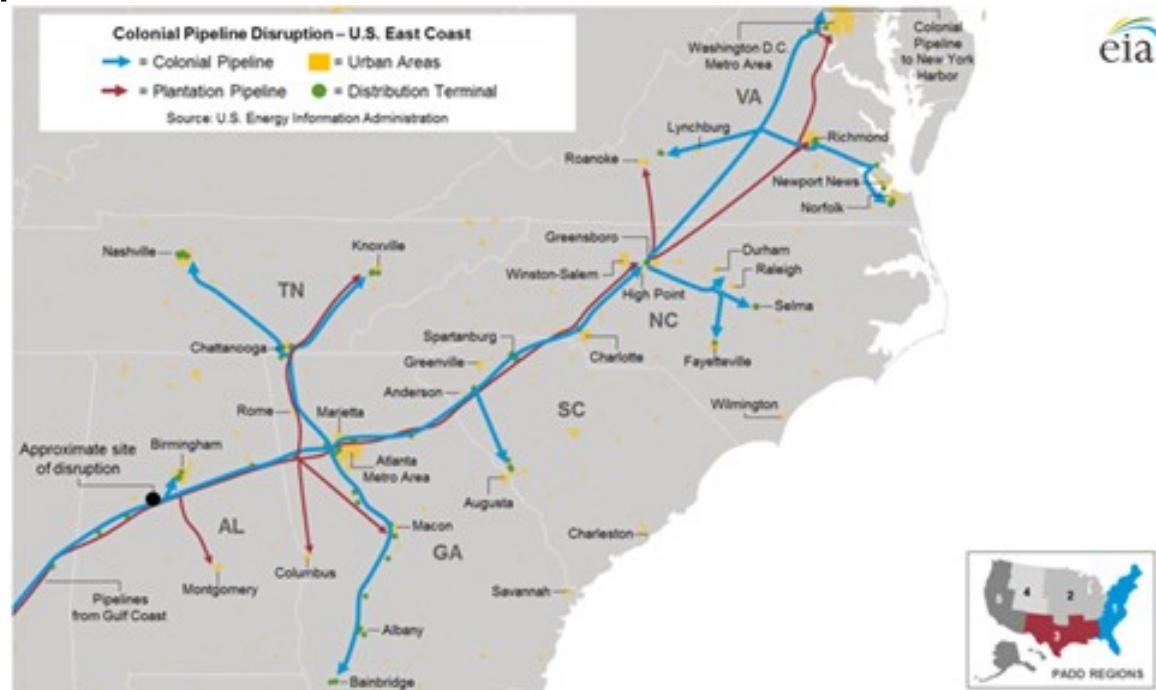
<https://www.welivesecurity.com/la-es/2021/02/10/atacante-intenta-envenenar-suministro-agua-ciudad-florida/>

<https://www.infobae.com/america/eeuu/2021/02/10/hackers-intentaron-contaminar-el-agua-de-un-pueblo-en-la-florida/>

Universidad FASTA: Ciberseguridad y Análisis Forense de entornos Industriales - 1/7/2022 Jorge.kamlofsky@uai.edu.ar

Seguridad en Tecnologías Operacionales

Algunos Ataques a Infraestructuras Críticas Industriales



Oleoductos de USA (Colonial Pipeline, 2021): El ataque tuvo lugar entre el jueves 6 de mayo y el viernes 7 de mayo de 2021. Un ataque de malware obligó a cerrar su sistema. Detuvo todas las operaciones del oleoducto. El ataque afectó a algunos de sus sistemas de información. Joe Biden declaró el estado de emergencia. El ataque fue llevado a cabo por una empresa criminal de **ransomware** llamada **DarkSide**.

Fuente: https://es.wikipedia.org/wiki/Ciberataque_a_Colonial_Pipeline

Contenido de esta Presentación

Presentación de los Sistemas de Control Industrial: Tecnologías Operacionales

Seguridad en Tecnologías de la Información

Seguridad en Tecnologías Operacionales

Resumen de Nuestro Proyecto.