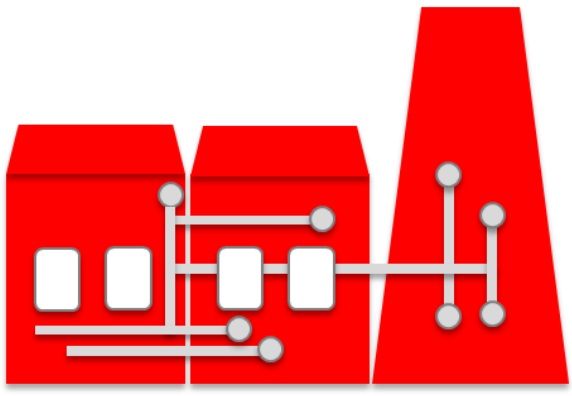
TEMA 1. INTRODUCCIÓN A LOS SISTEMAS DE CONTROL Y AUTOMATIZACIÓN Y A LA PROBLEMÁTICA DE SEGURIDAD ASOCIADA

1.3. Particularidades de la configuración de la seguridad industrial



Curso avanzado de ciberseguridad en sistemas de control y automatización industrial

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1.3 Particularidades de la configuración de la seguridad industrial 3
1.3.1 Consideraciones generales 3
1.3.2 Redes Extensas 3
1.3.3 Configuración limitada 5
1.3.4 Productos de larga vida 6
1.3.5 Protocolos de comunicación fijos 7
1.3.6 Pocas posibilidades de software 8
Referencias Técnicas 9

ÍNDICE DE FIGURAS

Figura 20. Consideraciones generales y virus (Imagen). Fuente: www.wikipedia.org 3
Figura 21. Redes extensas y Planta química (imagen). Fuente: www.wikipedia.org 3
Figura 22. Arquitecturas de red típicas de una red Profinet. Fuente: www.profibus.com ... 4
Figura 23. PLC Compacto con funciones de seguridad prácticamente nulas. 5
Figura 24. Entrada de contraseña en un PLC. Única medida de seguridad del mismo. 5
Figura 25. PLC de los años 90 completamente operativo. 6
Figura 26. Cable específico Profinet. 8
Figura 27. Posibilidades software limitadas. 8

ÍNDICE DE TABLAS

Tabla 1. Medios de comunicación inalámbricos más frecuentes en automatización industrial e infraestructuras 5
Tabla 2. Razones para el cambio en diferentes sectores. 6
Tabla 3. Vida media de los elementos planta. 7
Tabla 4. Ejemplos de protocolos, según la marca. 7

1.3 PARTICULARIDADES DE LA CONFIGURACIÓN DE LA SEGURIDAD INDUSTRIAL

1.3.1 Consideraciones generales

Existen diferencias importantes entre las posibilidades de configuración que permite una aplicación de automatización industrial con respecto al resto de instalaciones de la empresa. Las diferencias más importantes que se podrían indicar serían las siguientes:

- Redes muy extensas dentro de planta.
- Posibilidad de configuración normalmente limitada.
- Imposibilidad de modificar los protocolos de comunicaciones.
- Productos de larga duración.
- Imposibilidad de añadir módulos de *software* específicos.

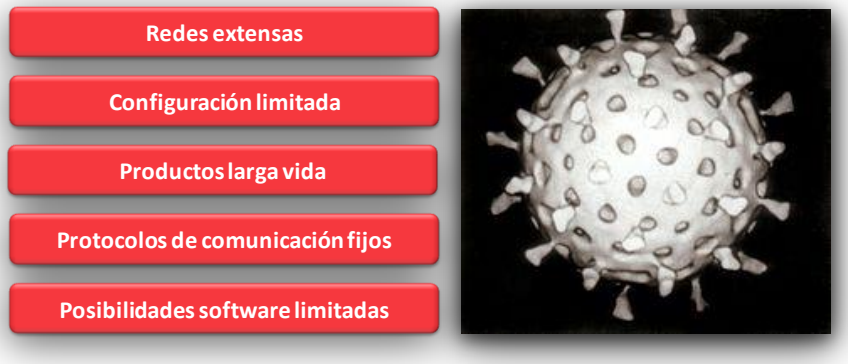


Figura 20. Consideraciones generales y virus (Imagen). Fuente: www.wikipedia.org

1.3.2 Redes Extensas

Figura 21. Redes extensas y Planta química (imagen). Fuente: www.wikipedia.org

La extensión y distribución de las redes dentro de las instalaciones de automatización difiere de la típica instalación de oficina.

En plantas es posible encontrarse diferentes arquitecturas: en árbol, estrella o bus para un mismo tipo de comunicación.

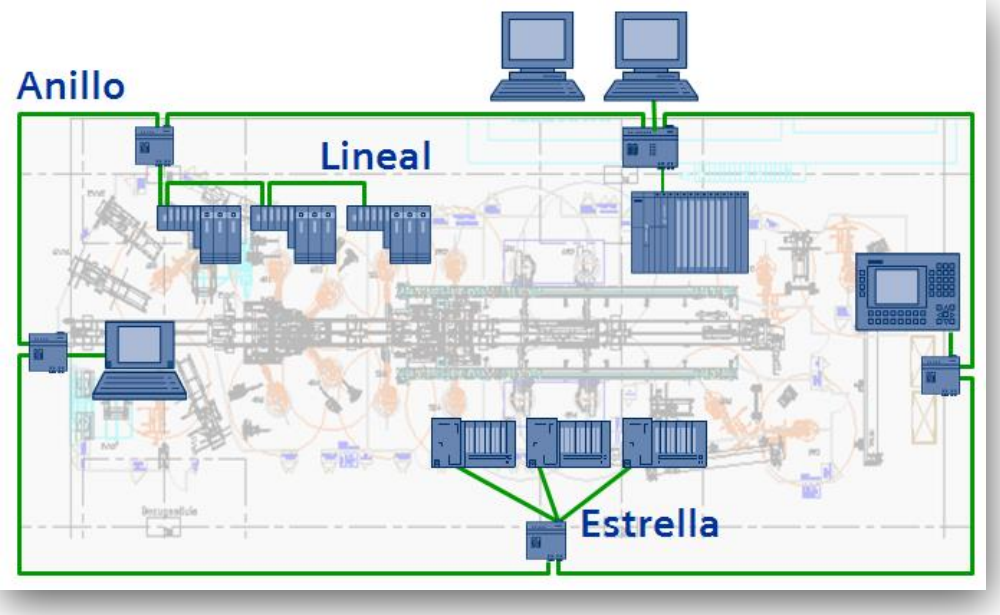


Figura 22. Arquitecturas de red típicas de una red Profinet. Fuente: www.profibus.com

También es frecuente el cambio de medio físico para un mismo protocolo en una misma instalación. Es decir, en determinados entornos es necesario pasar de una conexión inalámbrica, a otra por cable de cobre para finalizar utilizando fibra óptica.

La utilización de la fibra óptica en el sector industrial ofrece las siguientes ventajas:

- Aumento de la distancia máxima de las líneas de comunicaciones.
- Posibilidad de conexión entre instalaciones en la que existen problemas para la instalación de una puesta a tierra común.
- Aislamiento de secciones de redes ante posibles tormentas eléctricas.
- Inmunidad a ruidos electromagnéticos.

En plantas químicas o depuradoras de aguas frecuentemente es conveniente realizar conexiones inalámbricas para instalar dispositivos a centenares de metros. Dentro de este tipo de comunicaciones se pueden encontrar diferentes tecnologías, dependiendo de las necesidades técnicas.

TIPO COMUNICACIÓN INALÁMBRICA	UTILIZACIÓN
Infrarrojos	Almacenes de pallets (tecnología en vías de desaparición).

TIPO COMUNICACIÓN INALÁMBRICA	UTILIZACIÓN
Bluetooth	Máquinas rotativas (algunos metros).
Wifi 802.11	Carretillas autónomas (decenas de metros).
Radio frecuencias propias	Instalaciones aguas potables (algunos kilómetros).
GPRS	Instalaciones desatendidas (distribución geográfica amplia).
Tetra	Aprovechamiento para datos de redes de voz privadas.

Tabla 1. Medios de comunicación inalámbricos más frecuentes en automatización industrial e infraestructuras

Esta multiplicidad de medios y la extensión de la red hacen que el control perimetral de la red sea complicado. Además, ocurre que, en algunos casos, pueden existir puntos de acceso a la red que no están bien fortificados.

1.3.3 Configuración limitada

Las medidas de seguridad que incorporan los dispositivos de control industrial se limitan muchas veces a una simple contraseña en muchos casos fácilmente evitable.

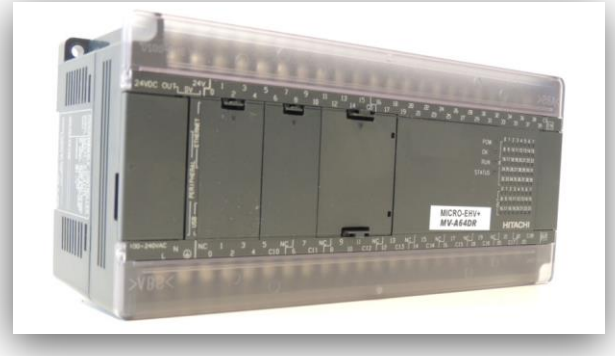


Figura 23. PLC Compacto con funciones de seguridad prácticamente nulas.

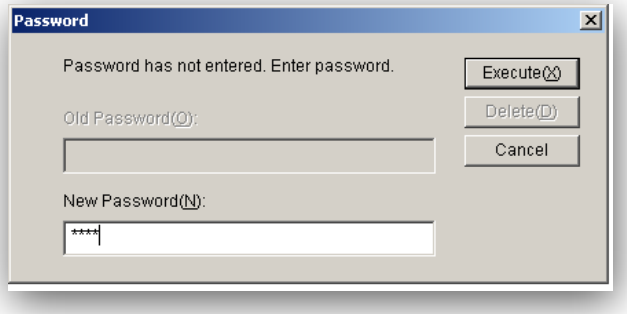


Figura 24. Entrada de contraseña en un PLC. Única medida de seguridad del mismo.

1.3.4 Productos de larga vida

La robustez de los equipos industriales y su alto coste de montaje y renovación de *software* hacen del reemplazo de los equipos de automatización algo que muchos usuarios evitan afrontar. Es común encontrar instalaciones con equipos con una antigüedad de algunos lustros, época en que la ciberseguridad industrial no era un tema prioritario en las instalaciones. Por ejemplo, es frecuente encontrar equipos de mediados de los años 90 conectados a una red industrial, pero difícilmente encontraremos un PC con Windows 3.11 en el entorno corporativo.

TIPO INDUSTRIA	RAZONES PARA LA PERMANENCIA/RENOVACIÓN CONTROL
PLANTAS NUCLEARES	Baja tasa de renovación ante la dificultad de certificar un nuevo equipo o solución tecnológica que afecta directamente al control de la planta.
PLANTAS QUÍMICAS Y ALIMENTARIAS	Instalación de nuevas soluciones al realizarse nuevas líneas de producción manteniéndose en muchos casos las anteriores. En muchos procesos la vida media puede ser inferior a causa de ambientes corrosivos.
PLANTAS FARMACÉUTICAS	Sin renovación mientras dura la producción de un medicamento donde se ha homologado un proceso productivo.
MAQUINA PEQUEÑA INDUSTRIA	Poca rotación mientras no exista avería que exija una renovación.
MAQUINA GRAN INDUSTRIA	Renovación inmediata si se obtiene una mejora del rendimiento o del coste.
INDUSTRIA AUTOMÓVIL	Renovación conjunta con la línea de producción por cambio de modelo a producir.

Tabla 2. Razones para el cambio en diferentes sectores.

En este sentido es imposible realizar una clasificación de la duración de un equipo según el tipo de industria pero si expresar los motivos por los que se realizan los cambios de equipamiento:

Figura 25. PLC de los años 90 completamente operativo.

Esta longevidad de los equipos de control industrial también produce situaciones donde es necesario reutilizar equipos diferentes, intentando adaptar protocolos y medios físicos prácticamente obsoletos, a nuevas tecnologías. Un ejemplo en este sentido sería la

conexión de RTUs con conexión RS-485 a un servidor virtual sin conexión *hardware* de este tipo. Mediante pasarelas *Serie-Ethernet* es posible realizar dicha conexión, pero a costa de aumentar la conectividad de la red y en consecuencia sus amenazas.

CONCEPTO	VIDA MEDIA
OBRA CIVIL	30-50 AÑOS
TENDIDO ELÉCTRICO	30 AÑOS
DISPOSITIVO CONTROL INDUSTRIAL	10-15 AÑOS
ORDENADOR	3-5 AÑOS

Tabla 3. Vida media de los elementos planta.

1.3.5 Protocolos de comunicación fijos

La elección de una determinada arquitectura de comunicación, una marca o modelo de equipos para una aplicación determinada seguramente obligará también al uso de unos determinados protocolos propietarios de comunicación.

A continuación se indica una tabla con las marcas de controles más comunes y los protocolos utilizados.

MARCA	SERIE	PROTOCOLO
SIEMENS	S7 1200/300/400	S7 MESSAGING
OMRON	CJ/CS	FINS
HITACHI	H SERIES	HI-PROTOCOL
ROCKWELL	LOGIX	RS-LOGIX
B&R	X20	INA
SCHNEIDER	TSX	UNITELWAY
HONEYWELL	UDC 3000	UDC
MITSUBISHI	FX	FX PROTOCOL

Tabla 4. Ejemplos de protocolos, según la marca.

Hoy en día, aunque existen protocolos de comunicación industrial con características de seguridad como cifrado o certificación de seguridad, no siempre están disponibles en los dispositivos elegidos.

Algunos buses de campo exigen modelos de red con unas estructuras rígidas y de poca o nula configuración. En caso de redes Ethernet, algunos dispositivos de seguridad sólo estarán disponibles para unos pocos protocolos (los más comunes) o dejando poco margen de maniobra para la elección de una solución de seguridad.

Figura 26. Cable específico Profinet.

En el capítulo 3 de este curso se repasan los protocolos de comunicación habituales entre los diferentes elementos de los niveles de automatización y estudiaremos los seguros.

1.3.6 Pocas posibilidades de software

La mayoría de dispositivos *hardware* para una aplicación específica (como por ejemplo: las pantallas de operador, los robots o los IEDs) disponen de un *software* específicamente diseñado para cumplir sólo con las funcionalidades para las que ha sido diseñado, por lo que resulta prácticamente imposible para el usuario introducir funcionalidades extra no diseñadas específicamente por él. Se puede observar cómo este tipo de sistemas son opuestos a los que se utilizan en entornos transaccionales, en los que, por ejemplo, con un ordenador en entorno *Windows* se podrían añadir soluciones como antivirus, *firewalls* o similares. Tampoco es usual el mantenimiento de los *firmwares* de los dispositivos una vez se ha realizado la puesta en marcha de la instalación y se han cumplido los requisitos funcionales exigidos.

Figura 27. Posibilidades software limitadas.

REFERENCIAS TÉCNICAS

Safety

http://en.wikipedia.org/wiki/Safety

Security

http://en.wikipedia.org/wiki/Security

Safety and Security in SCADA Systems Must be Improved through Resilience Based Risk Management. Stig O. Johnsen. 2013

Security vs. safety. Eirik Albrechtsen. 2003

GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480): SEGURIDAD EN SISTEMAS SCADA. Centro Criptológico Nacional. 2010.

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/480-SCADA/480-Seguridad_sistemas_SCADA-mar10.pdf

Ataque 0-day

http://en.wikipedia.org/wiki/Zero-day_attack

Logs

http://blog.s21sec.com/2009/11/logs.html

Guía para empresas: seguridad de los sistemas de monitorización y control de los procesos e infraestructuras (SCADA)

https://www.incibe.es/file/DqUev-29M3FtRjmJl-mD6A

ICS-CERT

https://ics-cert.us-cert.gov/

Safety and security

http://forum.wordreference.com/showthread.php?t=5489&langid=24

Seguridad: Safety o Security?

http://www.aena.es/csee/Satellite/SeguridadOperacionalNA/es/Page/1228215516978/1228215409300/

Buses de campo profibus y profinet

http://www.profibus.com

Especificaciones protocolo comunicación Modbus
http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

Documento vida media de un DCS
http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Whitepapers/WP_Col_Lifecycle_Mgmt.pdf
Información entrada contraseña Siemens (Capítulo 3)
https://www.swe.siemens.com/spain/web/es/industry/automatizacion/simatic/controladores/Documents/S7300ManualProducto.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD