Principios de Seguridad Informática en Sistemas Industriales

Contenido

Tendencias en la Economía Digital

Evolución del tráfico de Internet (Gby/s)

Naciones Unidas – Reporte 2019 sobre Economía Digital

Life Is On Schneider Electric

https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2175

https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2175

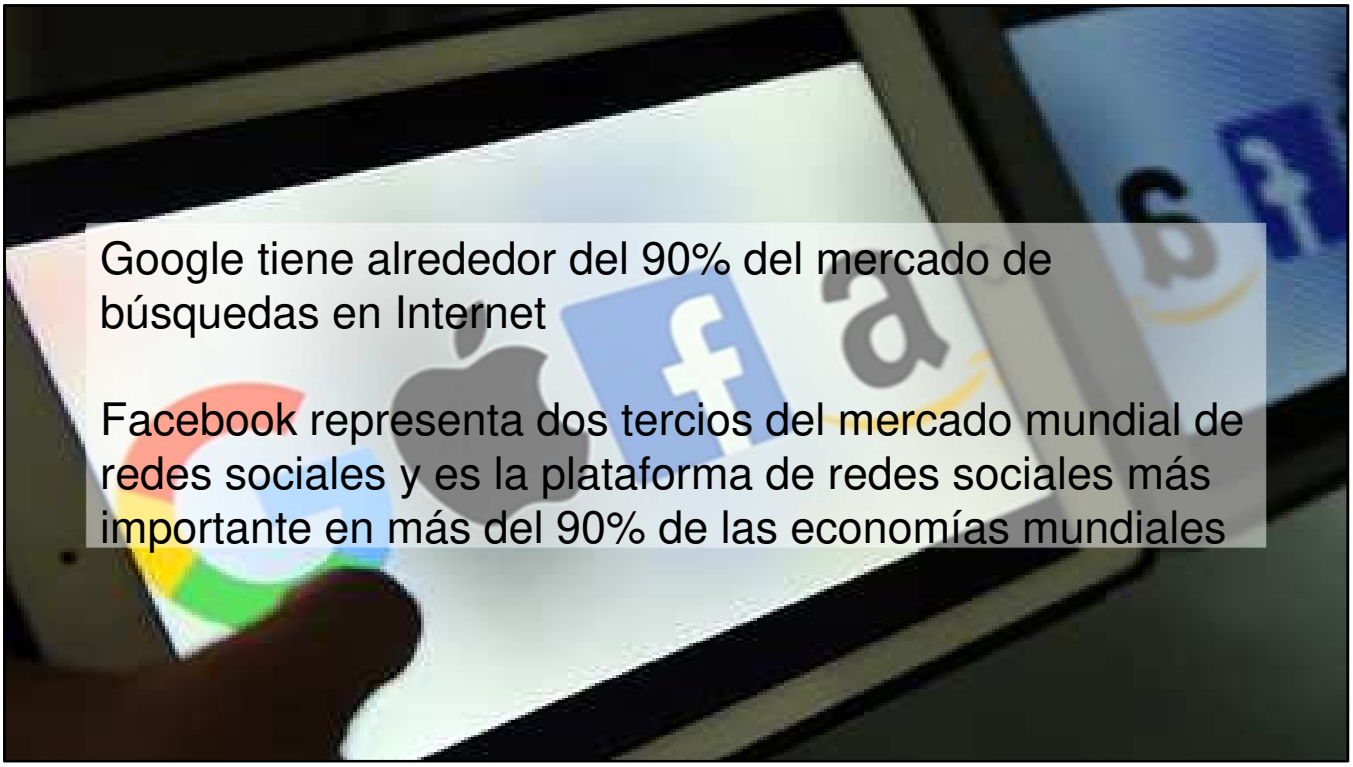
Microsoft, Apple, Amazon, Google, Facebook, Tencent y Alibaba, representan dos tercios del valor total de mercado de las 70 principales plataformas

Naciones Unidas – Reporte 2019 sobre Economía Digital

https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2175

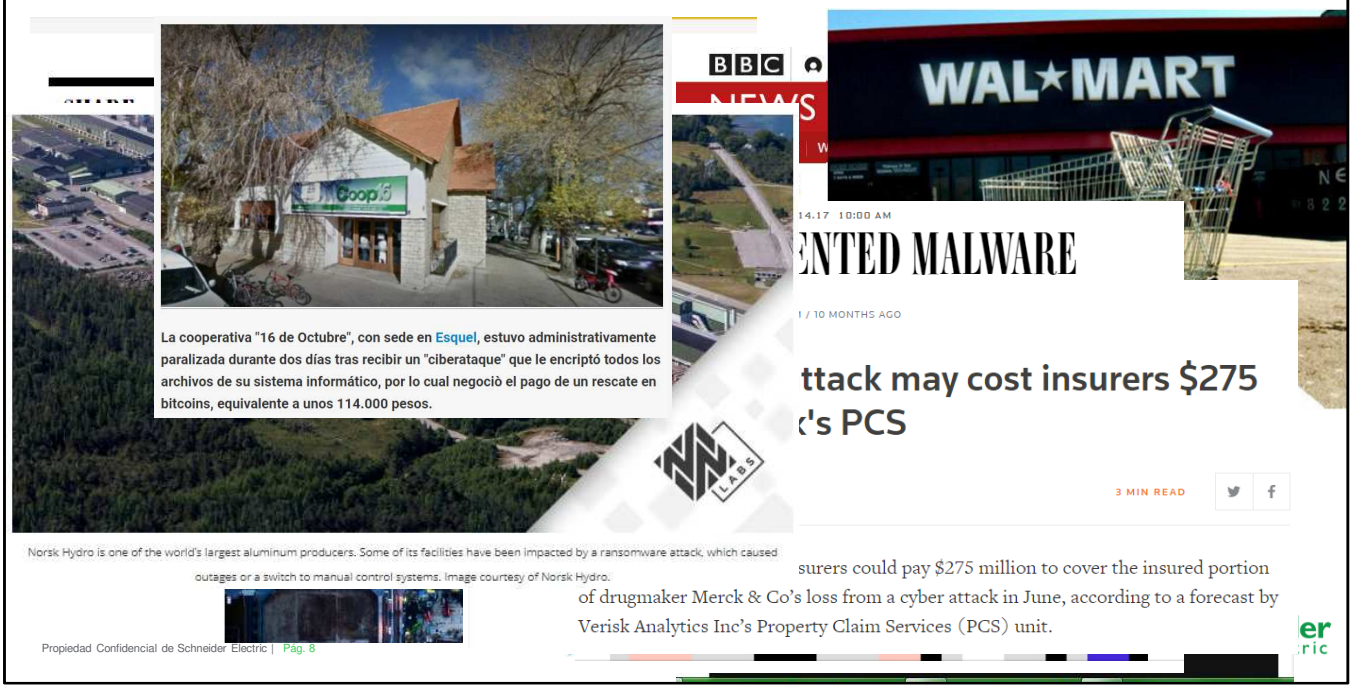
De la página de Tencent:
“About Us - Tencent uses technology to enrich the lives of Internet users. Our communications and social platforms Weixin and QQ connect users with each other, with digital content and daily life services in just a few clicks. Our high performance advertising platform helps brands and marketers reach out to hundreds of millions of consumers in China.”
https://www.tencent.com/

https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2175

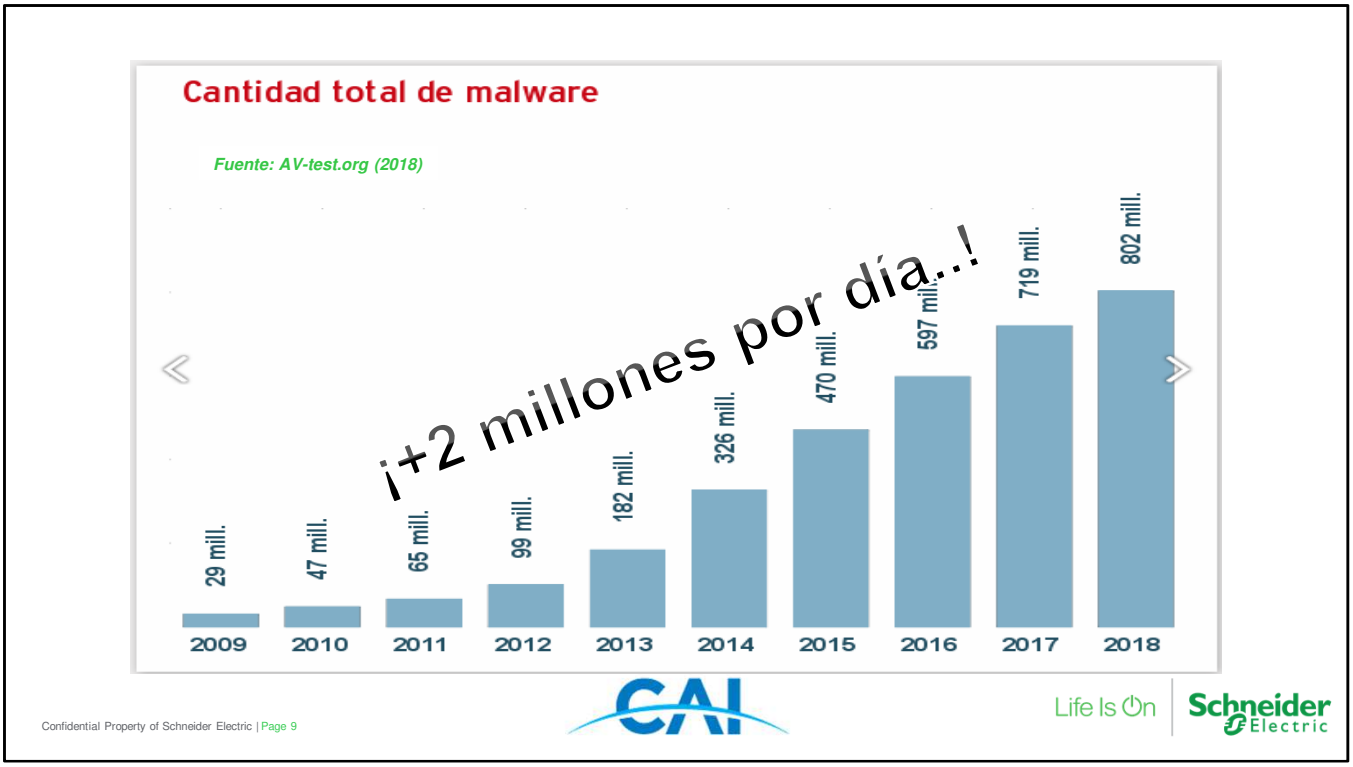

Google tiene alrededor del 90% del mercado de búsquedas en Internet
Facebook representa dos tercios del mercado mundial de redes sociales y es la plataforma de redes sociales más importante en más del 90% de las economías mundiales

Principios de Seguridad Informática en Sistemas Industriales

En las noticias…



https://www.scmagazine.com/ukrainian-officials-blame-russia-for-vpnfilter-attack-on-chlorine-plant/article/780729/
https://www.wired.com/story/sensor-hubs-smart-cities-vulnerabilities-hacks/
https://www.hackread.com/157-gb-of-sensitive-data-from-tesla-gm-toyota-others-exposed-online/
https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/
https://www.wired.com/2009/10/walmart-hack/
https://www.bbc.com/news/technology-38573074
https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP
https://www.nozominetworks.com/blog/breaking-research-lockergoga-ransomware-impacts-norsk-hydro/
→ 40MU$D de pérdidas en la primera semana.
https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-march-26/
https://www.ambito.com/cooperativa-esquel-pago-un-rescate-bitcoins-114000-n5013193

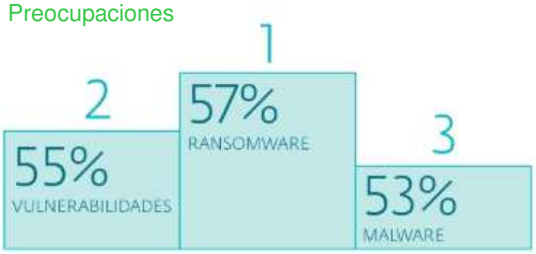


Customers are becoming more interested in cybersecurity due to the increased rate of cybersecurity related issues reported each year. This is the first of two slides illustrating the increase in the rate of cyber attacks. This slide shows the rate of malware infections per year. This is not isolated to industrial applications, but industrial PCs can be infected by malware. As time passes, more people within the population have the technical skills to initiate an attack, and tools are being introduced to simplify malicious code generation. In the future, it is doubtful that the rate of infections will decrease.

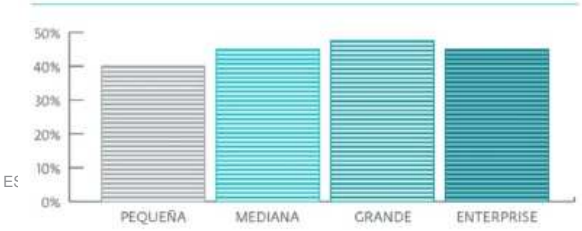
Situación de la Ciberseguridad en Latinoamérica

Reporte de Ciberseguridad - ESET 2018

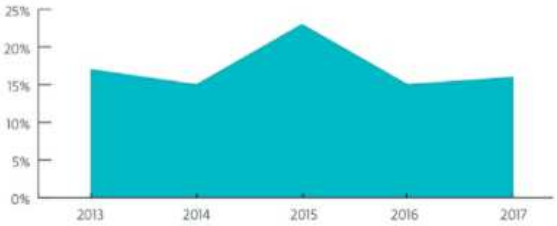
Preocupaciones



% Empresas con incidentes de código malicioso



Incidentes relacionados con ataques de ingeniería social



Life Is On Schneider Electric

https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/

World Economic Forum – The Global Risks Report 2019

Escenario de Riesgos Globales(*)

Top 10 risks in terms of Likelihood	Top 10 risks in terms of Impact
1 Extreme weather events	1 Weapons of mass destruction
2 Failure of climate-change mitigation and adaptation	2 Failure of climate-change mitigation and adaptation
3 Natural disasters	3 Extreme weather events
4 Data fraud or theft	4 Water crises
5. Ciberataques	5 Natural disasters
6 Man-made environmental disasters	6 Biodiversity loss and ecosystem collapse
7 Large-scale involuntary migration	**7. Ciberataques**
8 Biodiversity loss and ecosystem collapse	8 Critical information infrastructure breakdown
9 Water crises	9 Man-made environmental disasters
10 Asset bubbles in a major economy	10 Spread of infectious diseases

(*) World Economic Forum Global Risks Perception Survey 2018–2019.

CAI

Life Is On Schneider Electric

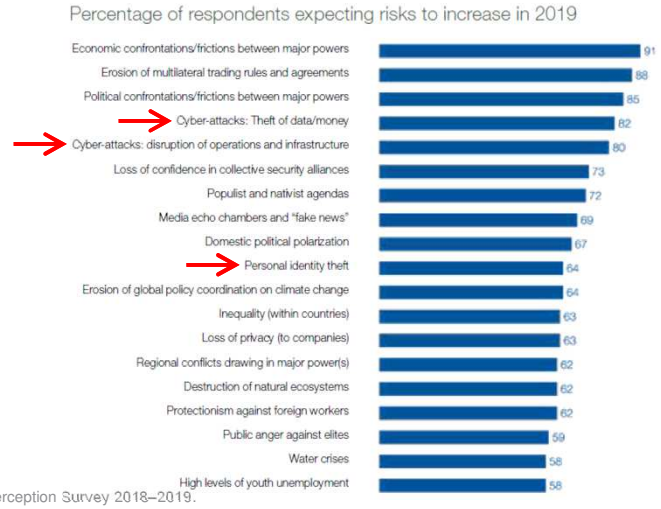
https://es.weforum.org/reports/the-global-risks-report-2019

Note: Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assess the impact on each global risk on a scale of 1 to 5 (1: minimal impact, 2: minor impact, 3: moderate impact, 4: severe impact and 5: catastrophic impact). See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

¿Qué es el World Economic Forum? https://es.weforum.org/about/world-economic-forum

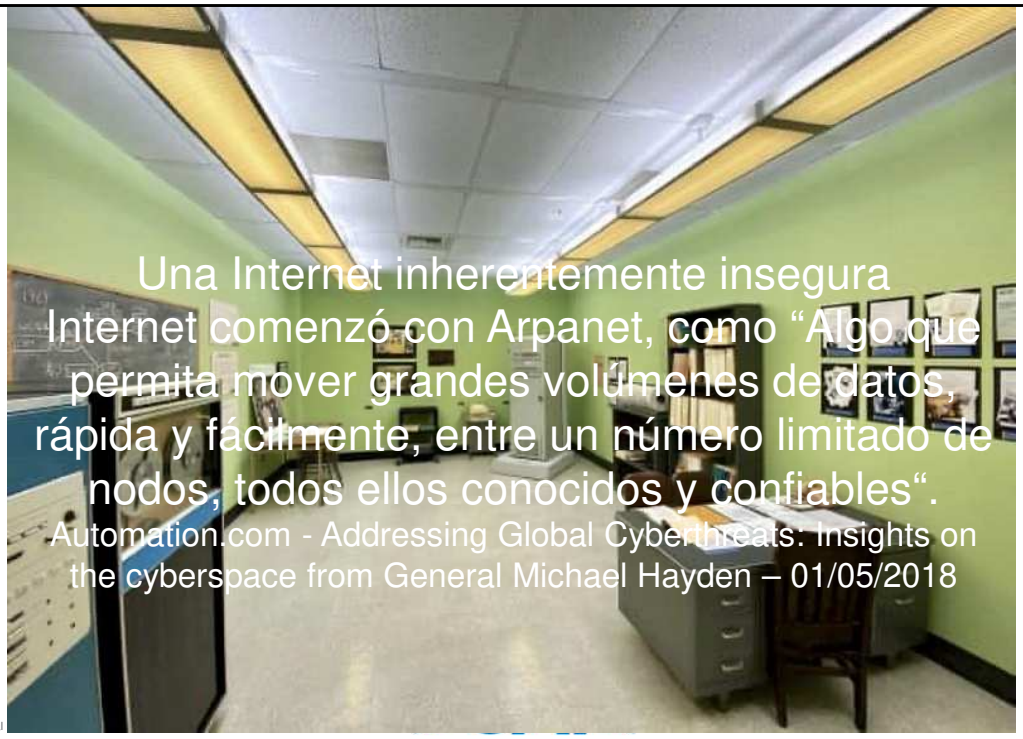
World Economic Forum – The Global Risks Report 2019

Escenario de Riesgos Globales(*)



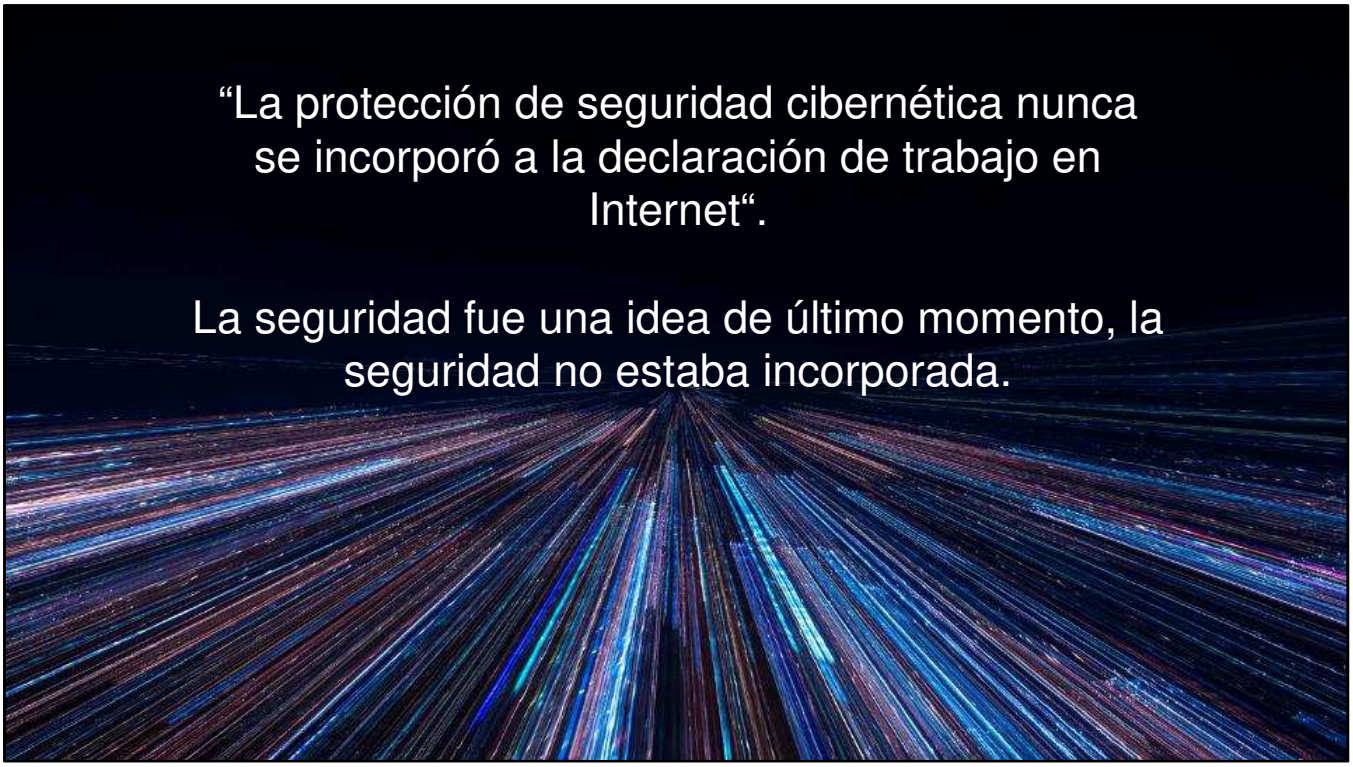
(*) World Economic Forum Global Risks Perception Survey 2018–2019.

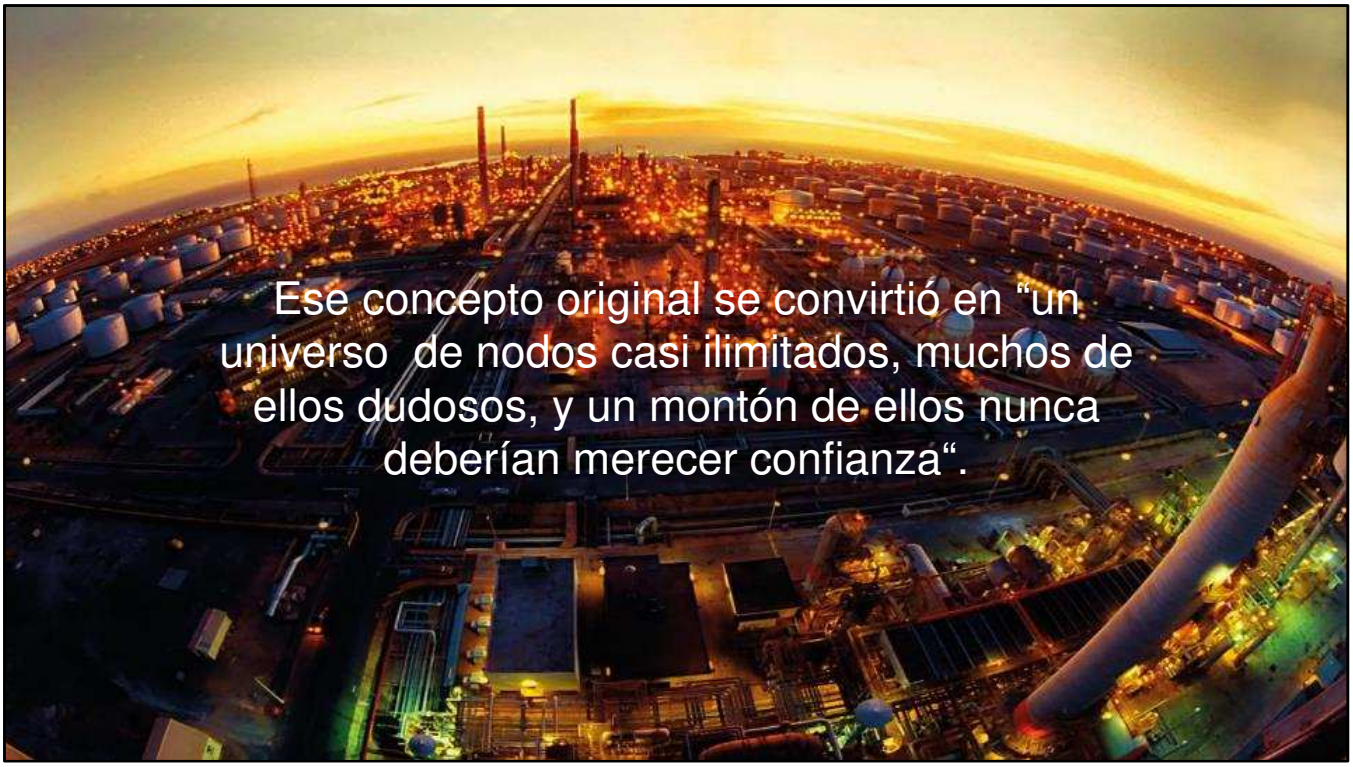
Life Is On Schneider Electric



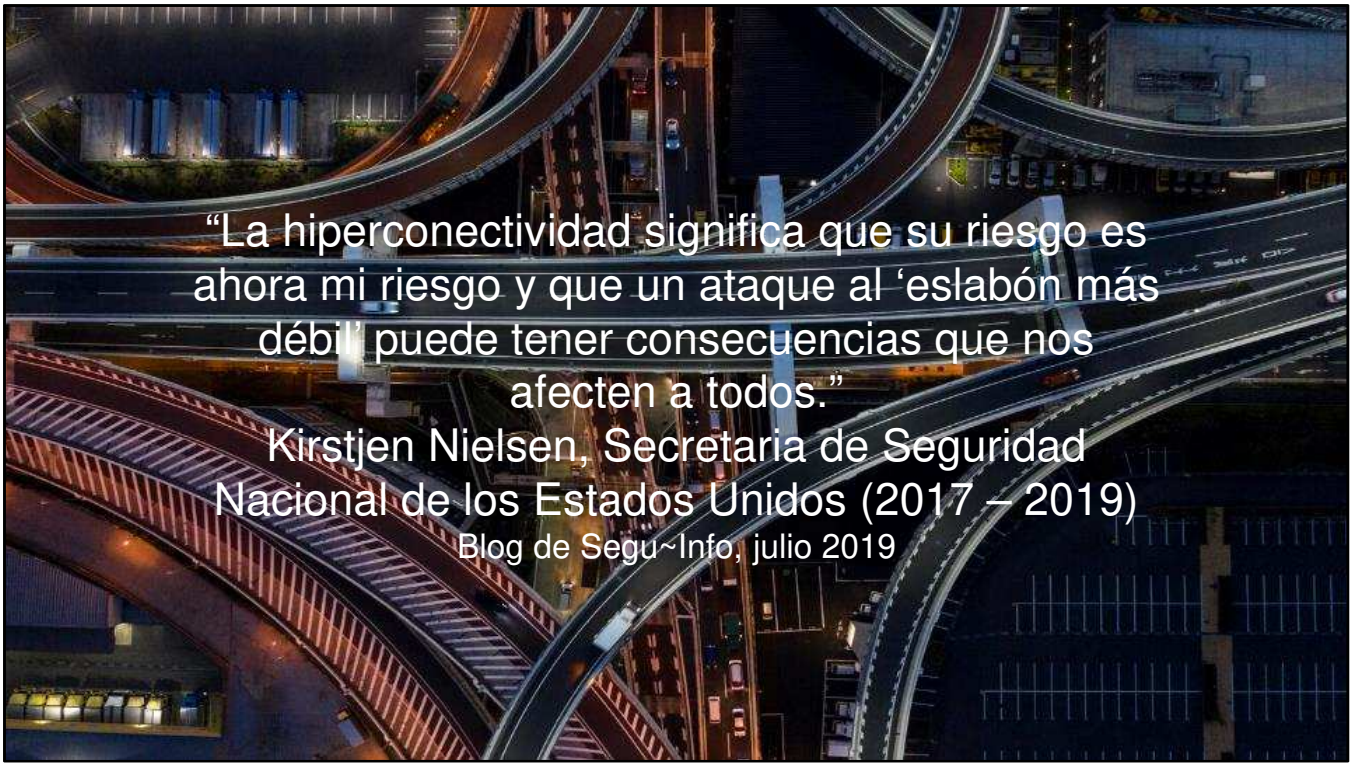
Presentación hecha en la 2018 PAS OptICS Conference - The PAS OptICS Conference (formerly known as PAS Technology Conference) is an event that will bring together operational and cybersecurity professionals from a cross-section of industries. This innovative conference provides a forum for industry experts, vendors and peers to interact and exchange ideas on how to address the operational and cybersecurity challenges facing critical infrastructure today.

As a retired United States Air Force four-star general with over 41 years of service, General Michael Hayden also served as former Director of the National Security Agency, Principal Deputy Director of National Intelligence, and Director of the Central Intelligence Agency. In 2005, the then Lt. Gen Hayden was confirmed by the United States Senate as the first Principal Deputy Director of National Intelligence and awarded his fourth star - making him "the highest-ranking military intelligence officer in the armed forces".
Principal of The Chertoff Group (http://chertoffgroup.com)


“La protección de seguridad cibernética nunca se incorporó a la declaración de trabajo en Internet“.
La seguridad fue una idea de último momento, la seguridad no estaba incorporada.


Ese concepto original se convirtió en “un universo de nodos casi ilimitados, muchos de ellos dudosos, y un montón de ellos nunca deberían merecer confianza“.

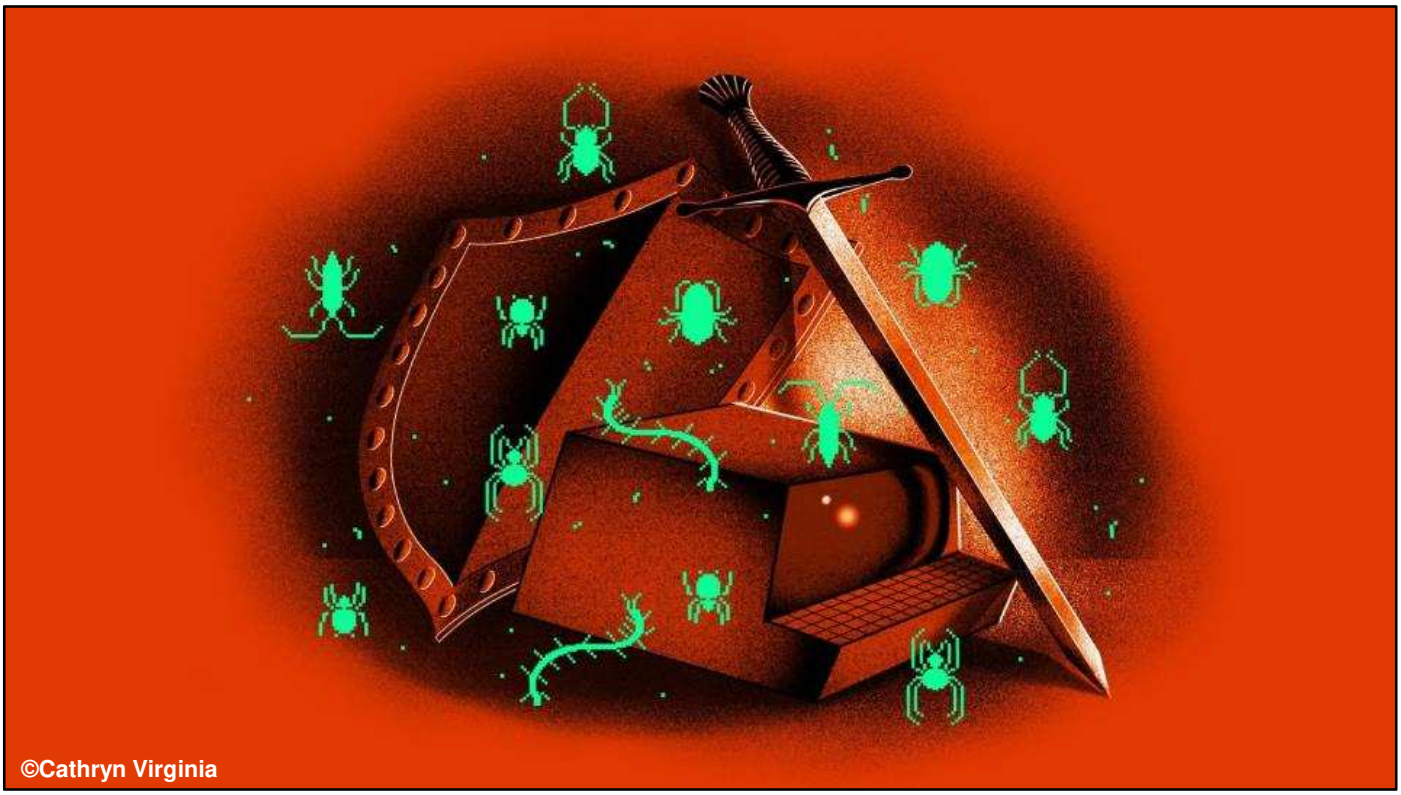
"Las tecnologías digitales, comúnmente denominadas sistemas cibernéticos, son una paradoja de la seguridad: A pesar que otorgan poderes sin precedentes, también hacen que los usuarios sean menos seguros ... Los sistemas cibernéticos nos nutren, pero al mismo tiempo nos debilitan y envenenan."
Richard Danzig, Secretario de Marina del Presidente Bill Clinton (1993 – 1997)


“La hiperconectividad significa que su riesgo es ahora mi riesgo y que un ataque al ‘eslabón más débil’ puede tener consecuencias que nos afecten a todos.”
Kirstjen Nielsen, Secretaria de Seguridad Nacional de los Estados Unidos (2017 – 2019)
Blog de Segu~Info, julio 2019


“El riesgo cibernético es el riesgo empresarial.
En la industria eléctrica, el riesgo cibernético
también es un riesgo para todo el ecosistema.”
Cyber Resilience in the Electricity Ecosystem: Principles and
Guidance for Boards. WEF 01/2019

Ataques en Infraestructura Crítica de Energía

¿Y cuáles son las consecuencias..?



https://www.cathryn-virginia.com/

Según PC Magazine Encyclopedia (https://www.pcmag.com/encyclopedia):

- **MAL**icious soft**WARE**: Software designed to destroy data, steal information or aggravate the user.
- **VIRUS:** Software used to infect a computer. A virus is a self-contained program that attaches itself to an existing application in a manner that causes it to be executed when the application is run. Macro viruses are similar.
- **TROJAN:** A program that appears legitimate but performs some illicit activity when run.
- **WORM:** A destructive program that replicates itself internally or throughout the network.
- (**AD**vertisement**WARE**) Also called "pitchware," adware is software that periodically collects the user's browsing behavior in order to pop up targeted ads on the computer. Adware often accompanies a program the user purposely downloads, and although it may be clearly indicated during the install procedure, novices generally keep clicking Next without reading the dialogs.
- **SPYWARE:** Software that sends information about your Web surfing habits to its website. Often quickly installed in your computer in combination with a free download you selected from the Web, spyware transmits information in the background as you move around the Web.
- **R**emote **A**ccess **T**rojan: Software in a user's machine that is interactively controlled by an attacker. Having full administrator rights, the attacker can perform any operation in the computer remotely and direct the RAT in the infected machine just like a user with a

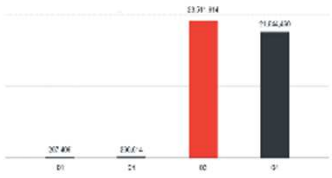
Web browser requests data from a server.

- **Logic Bomb**: A program routine that destroys data when certain conditions are met; for example, it may reformat the hard disk or insert random bits into data files on a certain date or if a particular employee record is missing from the employee database. Many viruses are logic bombs because they deliver their payload after a specific latency or when a trigger event occurs.

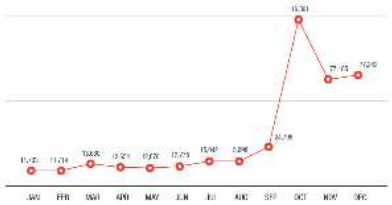
Cryptocurrency Mining Malware

Una amenaza creciente

En 2017, la minería de criptomoneda fue el evento de red más detectado en dispositivos conectados a enrutadores domésticos (según los comentarios de Trend Micro Smart Home Network)



Detecciones de malware de minería de criptomonedas en 2017 (basado en datos de la Trend Micro Smart Protection Network)



https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/

(**CRYPTO**graphic **CURRENCY**)
A digital currency that resides in a decentralized public ledger known as the "blockchain." Cryptocurrencies are not maintained or governed by any bank, financial institution or nation. They are a global entity, and in 2009, Bitcoin was the first. Since then, well more than a thousand others have been introduced with names such as Litecoin, Namecoin, Peercoin, Mastercoin, BlackCoin and Dodgecoin. However, some digital currencies are nothing more than scams that take advantage of the latest craze. As of 2018, after the U.S. and Japan, South Korea does the most Bitcoin trading.

Bitcoin
A peer-to-peer digital currency and electronic payment system introduced by an anonymous person with the alias Satoshi Nakamoto in January 2009. Although thousands of merchants on both the Web and dark Web accept bitcoins as payment, many people buy and hold for investment, and its value has skyrocketed since inception. Naysayers claim Bitcoin is a Ponzi scheme, but proponents predict one coin will be worth $500,000 in the future. Bitcoin has also spawned hundreds of other digital currencies (for a complete list, visit www.coinmarketcap.com).

Blockchain
The blockchain is a distributed ledger that provides verifiable proof of a transaction between two parties. There is no central repository. The blockchain is continuously updated and replicated on many nodes dedicated to that platform.
De PC Magazine Encyclopedia.

Ataques y vulnerabilidades comunes

Ataque Homográfico: en nombres de dominio internacionalizados (IDN). Son aquellos en los que se registran nombres de dominio maliciosos.

Unicode	Punycode
twitter.com	xn--titter-i2e.com
apple.com	xn--pple-43d.com
gmail.com	xn--gmil-6q5a.com

Dominio Real	Dominio Falso
twitter.com	twiter.com
mercadolibre.com	rnercadolibre.com
facebook.com	facebook.com

Ya no alcanza con revisar que la página sea segura, que utilice el protocolo HTTPS y que tenga el certificado de seguridad.

https://blog.segu-info.com.ar/2018/04/evilurl-detectar-dominios-y-ataques.html

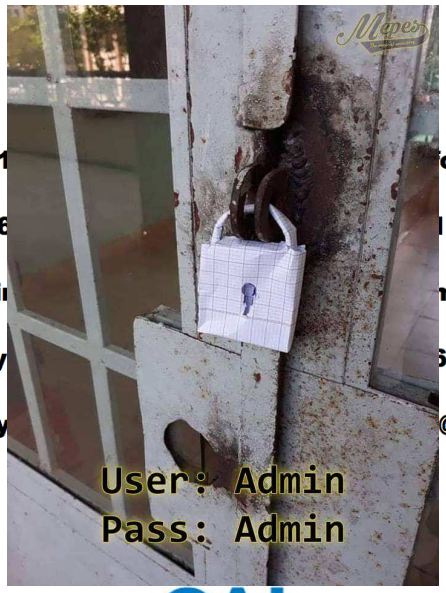
Según PC Magazine Encyclopedia (https://www.pcmag.com/encyclopedia):

- **I**nternationalized **D**omain **N**ame: A .com or .net domain name that is represented in non-English characters and symbols, with .com and .net appended at the end in English letters. IDN names are encoded in Unicode and display in their native language such as Chinese, Japanese or Korean. When entered into a Web browser or other application for name resolution by the DNS system, the Unicode is converted into ASCII Compatible Encoding (ACE), also known as "Punycode." The **Punycode** is an ASCII representation of the Unicode characters and symbols.

Principios de Seguridad Informática en Sistemas Industriales

Las 25 peores contraseñas del 2018

1. 123456	6. 111111	ootball	21. charlie
2. password	7. 123456	123123	22. aa123456
3. 123456789	8. sunshi	monkey	23. donald
4. 12345678	9. qwerty	654321	24. password1
5. 12345	10. ilovey	@#$%^&*	25. qwerty123



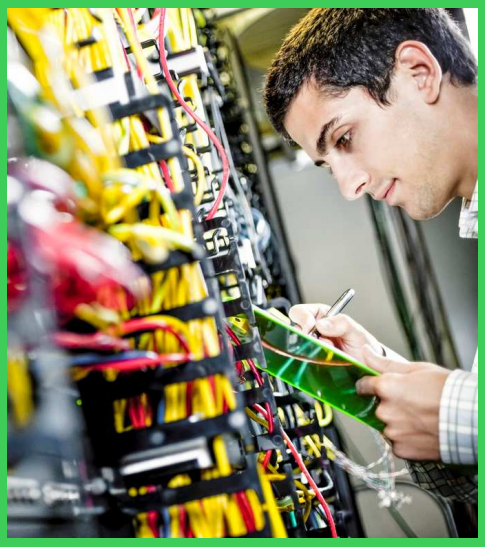
Life Is On Schneider Electric

Cada año *SplashData (https://www.splashdata.com/)* evalúa millones de credenciales a partir de filtraciones de datos y realiza un ranking de las contraseñas más inseguras. Listado de las 100 peores contraseñas: https://www.teamsid.com/100-worst-passwords/; https://www.teamsid.com/100-worst-passwords-top-50/

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by *The Economist*. He is the author of 13 books--including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*--as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and his blog "Schneier on Security" are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; an Advisory Board Member of the Electronic Privacy Information Center and VerifiedVoting.org; and a special advisor to IBM Security and the Chief Technology Officer at IBM Resilient.
schneier@schneier.com.

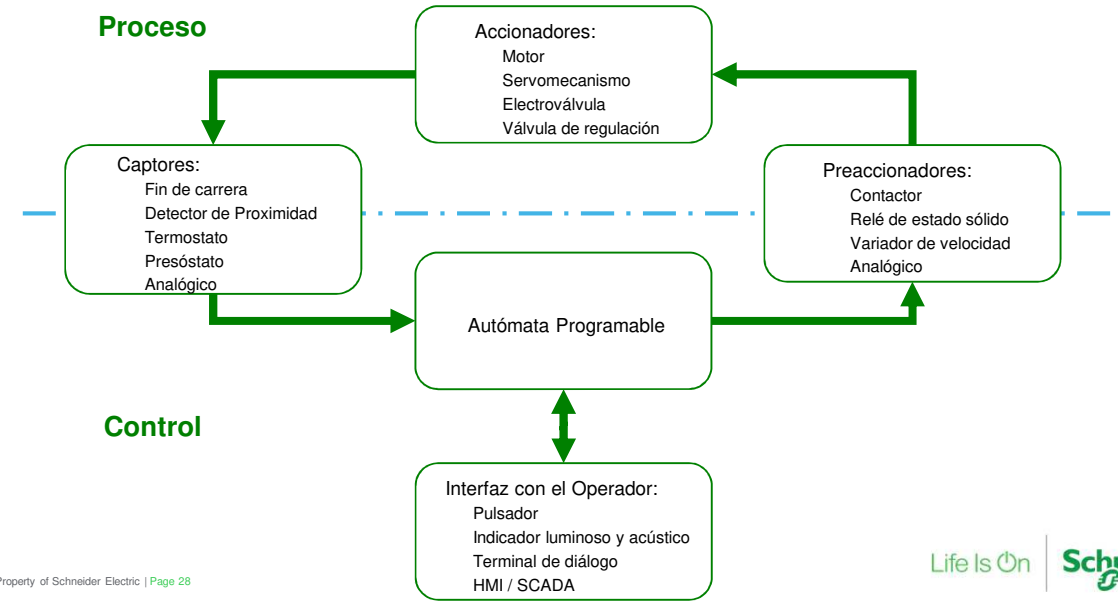

"Hay dos tipos de empresas: aquellas que han sido hackeadas, y aquellas que no saben que han sido hackeadas“
John Chambers, ex CEO de Cisco

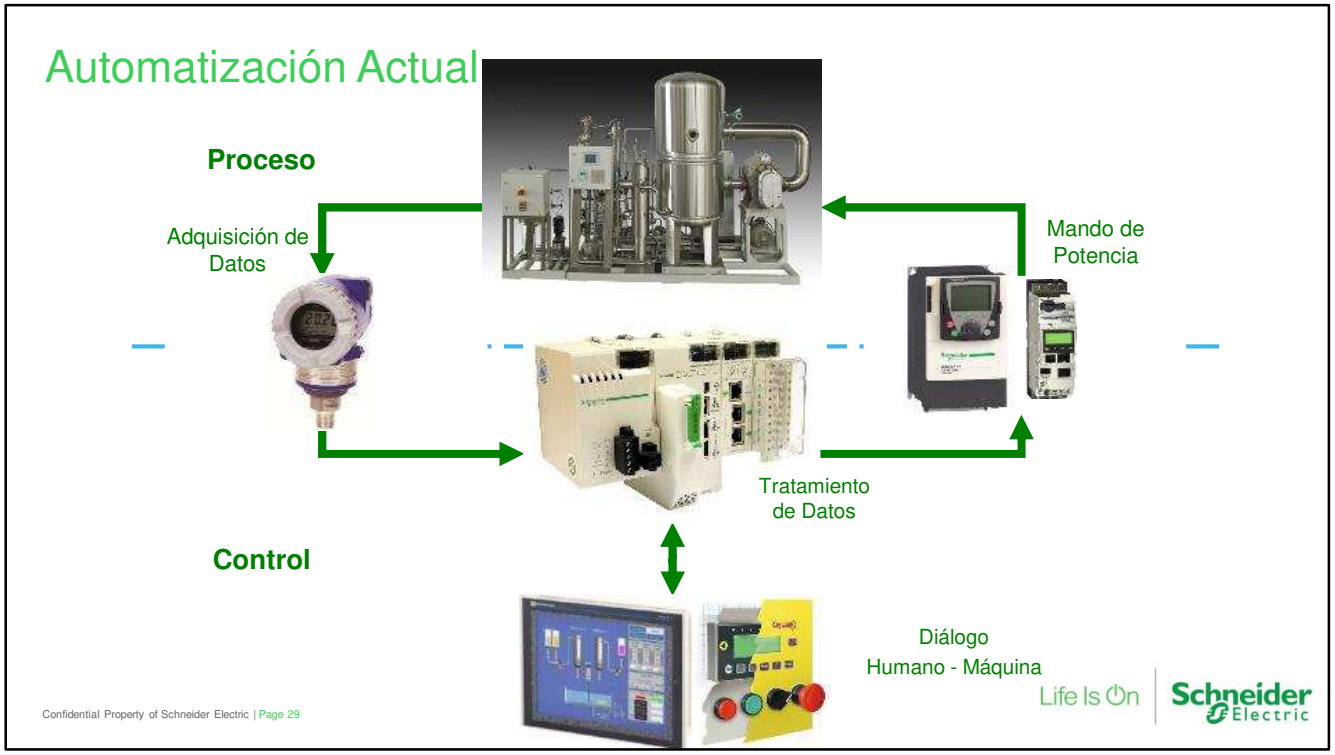
Contenido



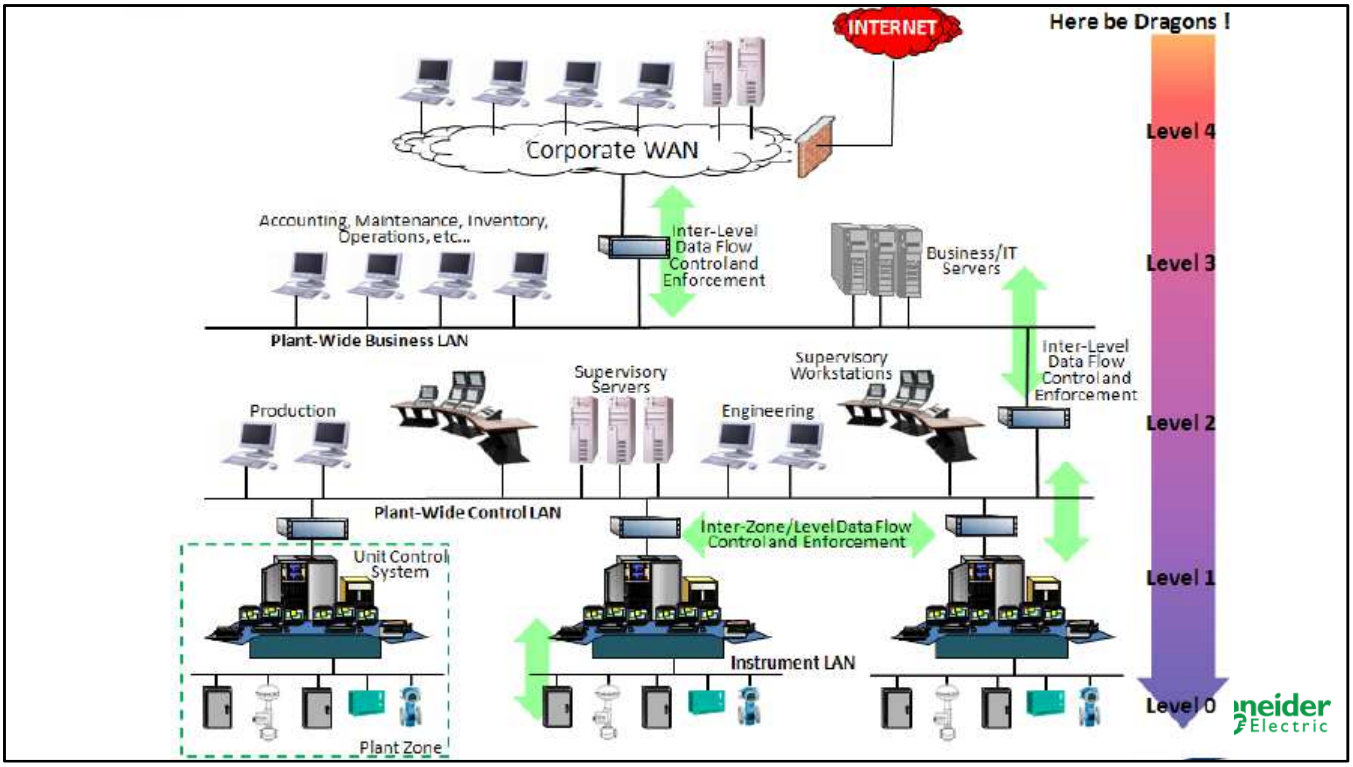
Life Is On Schneider Electric

Automatización Actual





Un ejemplo de un sistema de automatización para ajustar la presión de vapor para esterilización en una línea de producción farmacéutica (imagen de IMCO PROCESS & PACKAGING).


INTERNET
Here be Dragons !
Corporate WAN
Level 4
Accounting, Maintenance, Inventory, Operations, etc...
Inter-Level Data Flow Control and Enforcement
Business/IT Servers
Level 3
Plant-Wide Business LAN
Inter-Level Data Flow Control and Enforcement
Supervisory Servers
Supervisory Workstations
Production
Engineering
Level 2
Plant-Wide Control LAN
Inter-Zone/Level Data Flow Control and Enforcement
Unit Control System
Level 1
Instrument LAN
Level 0
Plant Zone
Schneider Electric

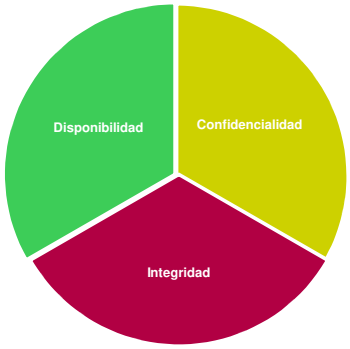
Contenido

Life Is On Schneider Electric

Agenda slide

¿Qué es la seguridad de la información..?

La seguridad de la información es la disciplina responsable de garantizar la disponibilidad, confidencialidad e integridad de la información.



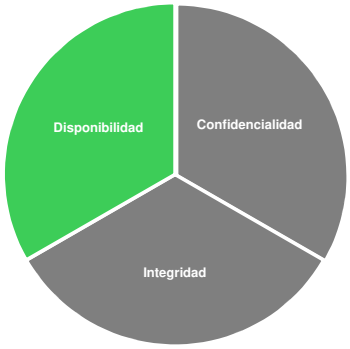
Life Is On Schneider Electric

Pero aplica también a los diferentes dispositivos que la procesan y almacenan, como a las redes de comunicación de datos por donde viaja ésta.

¿Qué es la seguridad de la información..?

Disponibilidad: La información y los sistemas que la almacenan deben estar disponibles cuando los usuarios (y sistemas) lo requieran. Propiedad de asegurar el acceso oportuno y confiable y el uso de la información y la funcionalidad del sistema de control(*).

- Un ataque de negación de servicio es un ejemplo de como se compromete la disponibilidad.



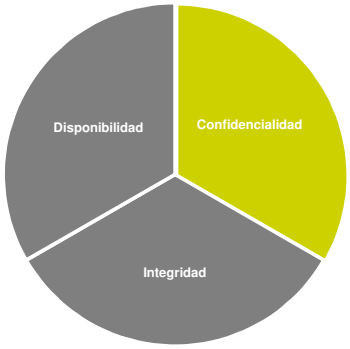
(*) Según ISA/IEC ISA-62443-3-2

¿Qué es la seguridad de la información..?

Confidencialidad: La información y los sistemas que la almacenan sólo debe ser accesibles para los usuarios (y sistemas) que lo requieran.
Preservación de las restricciones autorizadas sobre el acceso a la información y su divulgación, incluidos los medios para proteger la privacidad personal y la información propietaria(*).

- Un ataque de tipo SQL Injection, que le permita a un atacante obtener datos, compromete la confidencialidad.

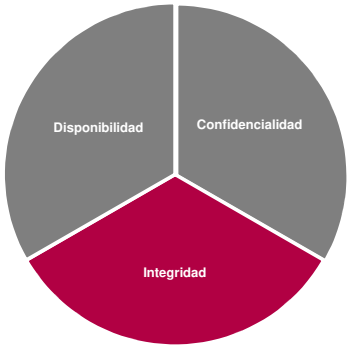
(*) Según ISA/IEC ISA-62443-3-2



¿Qué es la seguridad de la información..?

Integridad: La información sólo podrá ser modificada por los usuarios (y sistemas) autorizados a hacerlo.
Protección contra la modificación o destrucción indebida, incluída la no-repudiación de la información y la autenticidad(*).

- Si un soporte técnico puede acceder a la base de datos de eCommerce y alterar los precios, se compromete la integridad.



(*) Según ISA/IEC ISA-62443-3-2

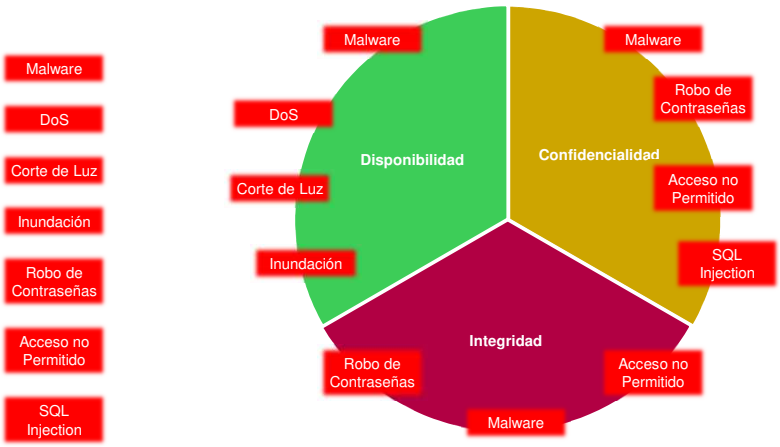
¿Qué puede comprometer la información?

Activo: objeto físico o lógico propiedad de, o en custodia por, una organización, con valor percibido o real para ésta.
Amenaza: violación potencial de la seguridad, que existe cuando hay una circunstancia, capacidad, acción o evento que pueda causar un daño.
Ataque: acción deliberada que intenta evadir las medidas de seguridad del sistema.
Contramedida: acción, dispositivo, procedimiento o técnica que reduce una amenaza, una vulnerabilidad o un ataque, minimizando el daño que pueda causar o bien detectándolo y reportándolo, para permitir una acción correctiva.
Vulnerabilidad: falla o debilidad en el diseño del sistema, su implementación, su operación o su administración que puede ser aprovechada para violar la integridad del mismo o la política de seguridad.
Riesgo: es una medición del daño esperado, expresado como la probabilidad de que una determinada amenaza utilice alguna vulnerabilidad, con una consecuencia específica.

Riesgo = Amenaza x Vulnerabilidad × Consecuencia.

Exploit: código escrito para usar una vulnerabilidad con el fin de violar la seguridad de un sistema.
Zero Day: un exploit para atacar un sistema utilizando una vulnerabilidad desconocida o no publicada por el fabricante.

Algunos Ejemplos de Amenazas



Naturales: terremotos, inundaciones, tornados
Humana: causados por personas

- **Intencional:** realizados con la intención de causar daño (ataque)
- **No Intencional:** realizados por desconocimiento o descuido (incidente)
- **Interna:** por un integrante de la organización (menos frecuentes pero causan mayor daño)
- **Externo:** por personas ajenas a la organización

Ingeniería Social

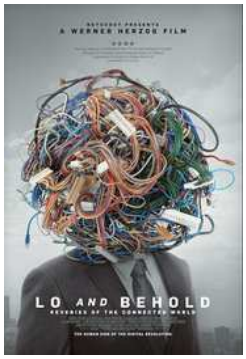
Las personas, el eslabón más débil…

Lo And Behold: Reveries of the Connected World

- 2016, dirigida por Werner Herzog

Fragmento de las entrevistas a:

- Kevin Mitnick, famoso hacker
- Paul Werner, Sandia National Laboratories



Life Is On Schneider Electric

Lo and Behold: Reveries of the Connected World es un documental de 2016 dirigido y producido por Werner Herzog. La película trata sobre el impacto del internet, la robótica, la inteligencia artificial, y otras tecnologías en la vida humana.
Fecha de estreno: 27 de octubre de 2016 (Rusia)
Director: Werner Herzog
Música compuesta por: Mark De Gli Antoni
Guion: Werner Herzog
Cinematografía: Peter Zeitlinger
Distribuidora: Magnolia Pictures

Contenido

¿Qué es ciberseguridad Industrial?

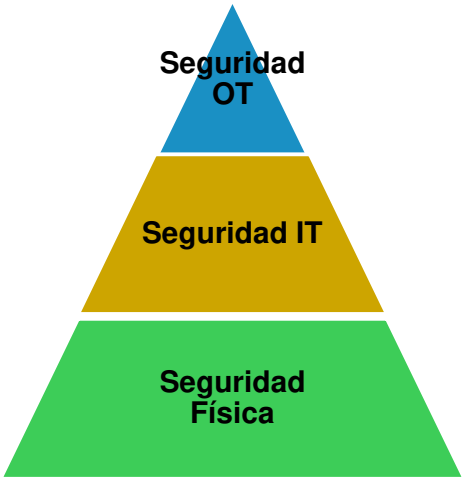
Definiendo términos

Sistema de control: componentes de hardware y software de un Sistema de Automatización y Control Industrial (IACS en inglés).

Ciberseguridad: medidas tomadas para para proteger una computadora, o conjunto de éstas, de accesos no autorizados o ataques.

http://isa99.isa.org/ISA99%20Wiki/Master-Glossary.aspx

Ciberseguridad Industrial vs. Informática

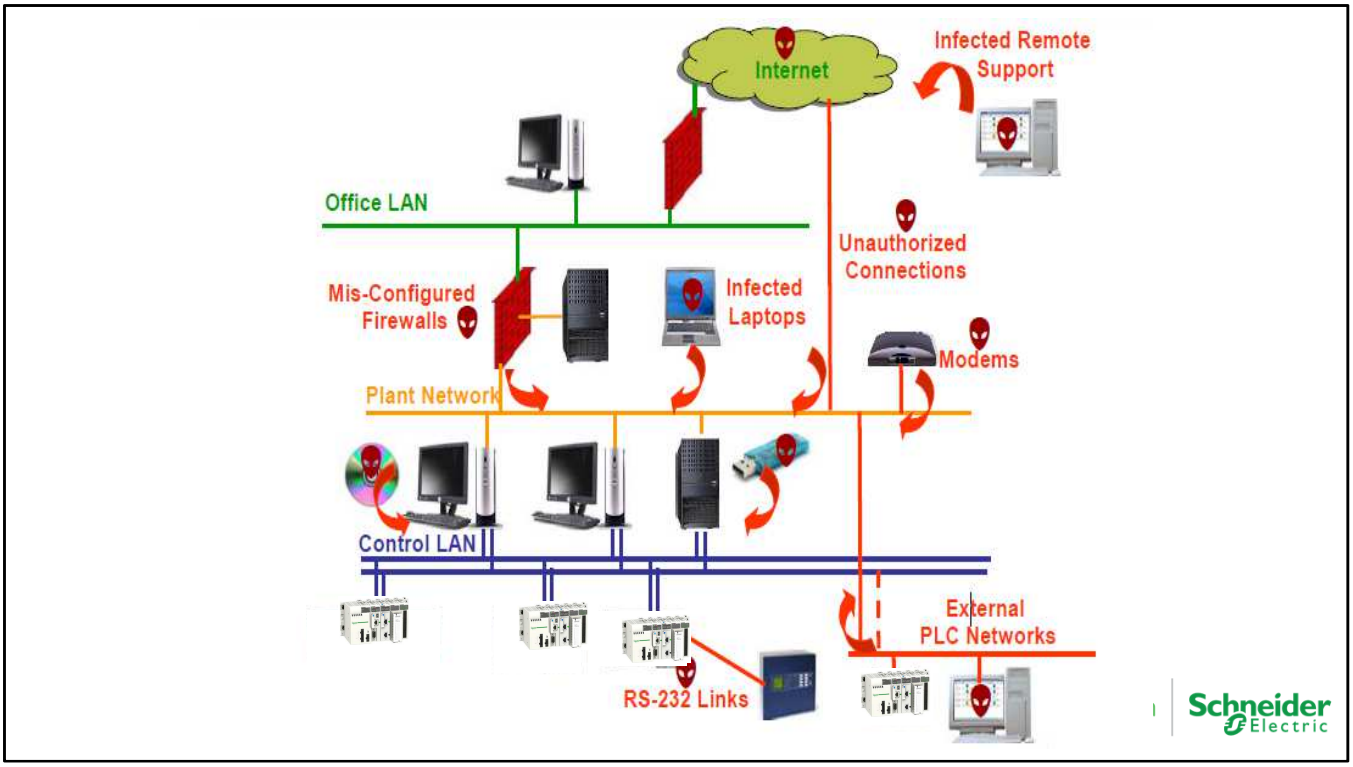


IT: Information Technology

Tecnología y aplicaciones convencionales para el manejo de la información.

OT: Operations Technology

Tecnología y aplicaciones relacionadas con los sistemas de automatización y control industrial (IACS).

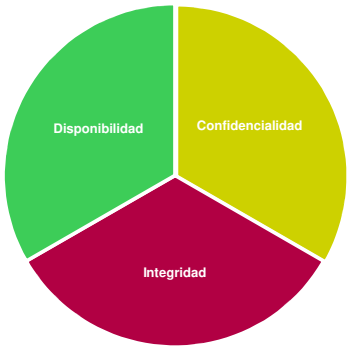


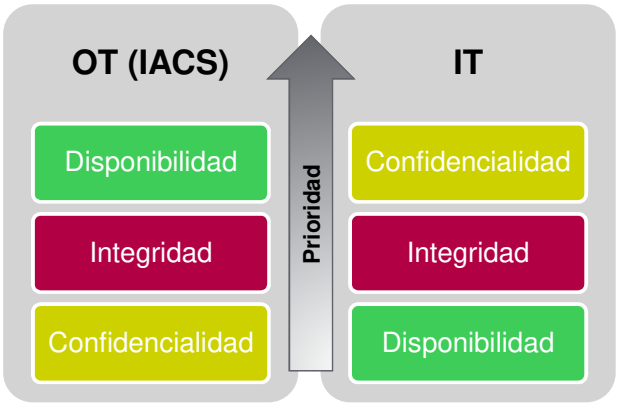
Using the ISA/IEC 62443 Standard to Secure Your Control Systems

Los 5 mitos de la ciberseguridad industrial

1. “No estamos conectados a Internet…”
2. Los sistemas de control están protegidos por un firewall.
3. Los hackers no entienden a los sistemas de control industrial.
4. Nuestra empresa/planta/instalación no es un blanco de interés.
5. Nuestra implementación de SIS nos protege.

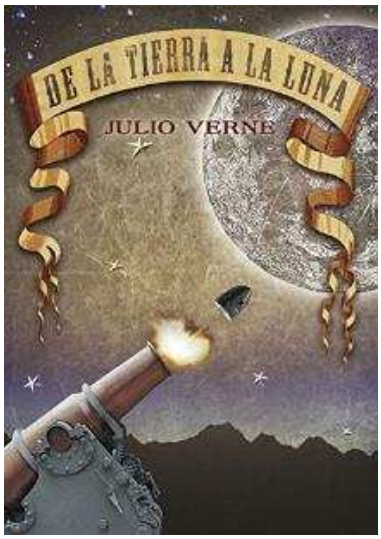
Ciberseguridad Industrial vs. Seguridad Informática





¿Cómo proteger los IACS..?

Atacantes vs. Defensores



Life Is On Schneider Electric

Jules Gabriel Verne (1828 - 1905), conocido en los países hispanohablantes como Julio Verne, fue un escritor, poeta y dramaturgo francés célebre por sus novelas de aventuras y por su profunda influencia en el género literario de la ciencia ficción.

Marie Georges Jean Méliès (1861 - 1938) fue un ilusionista y cineasta francés famoso por liderar muchos desarrollos técnicos y narrativos en los albores de la cinematografía.

En el inicio del libro se enfrentan los miembros del **Gun Club** de Baltimore, presidido por Impey Barbicane con el Capitán Nicholl, quien se dedicaba a la fabricación de blindajes. Ambos, entre otros, serían parte de la tripulación en tan fantástico viaje a la Luna.

¿Cómo proteger los IACS..?

Defensa en Profundidad

Una única defensa perimetral no alcanza:

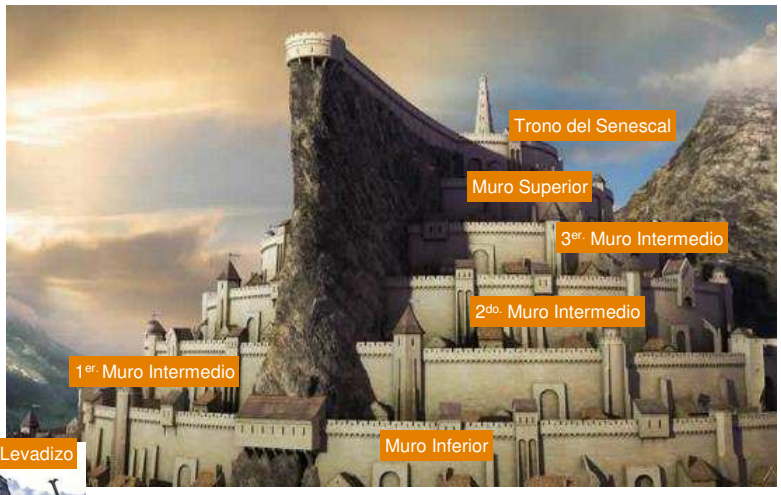
- Los “chicos malos” podrán entrar eventualmente.
- No alcanza con instalar un firewall y “olvidarse” de la seguridad.

El sistema debe de control debe ser robusto, para los cual se necesita:

- Defensa en Profundidad.
- Detección en Profundidad.
- Respuesta oportuna y adecuada a los incidentes.

¿Cómo proteger los IACS..?

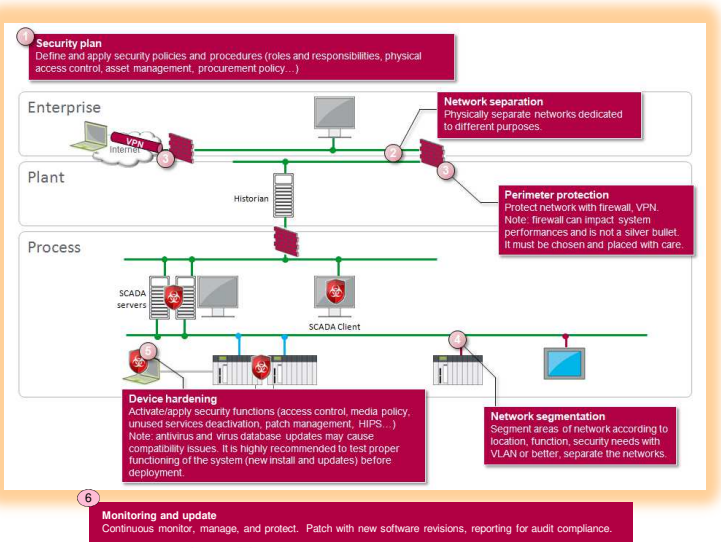
Defensa en Profundidad



¿Cómo proteger los IACS..?

Defensa en Profundidad

1. Plan de Seguridad
2. Separación de Redes
3. Protección Perimetral
4. Segmentación de Redes
5. Dispositivos Robustos
6. Supervisión y Actualización



CAI

Life Is On Schneider Electric

Is the network partitioned into protected zones using defense in depth principles? The defense in depth approach was conceived by the United States National Security Agency. It layers the network with security features and appliances, helping to protect critical processes and to contain damage during an attack. In partitioned networks, control infrastructure is not connected to equipment in the enterprise network. Key elements of a defense in depth approach include the following.

SECURITY PLAN
Create, apply and update security **policies** and **procedures**. They must assess **vulnerabilities**, mitigate and avoid **risks**, and define how to **recover from disaster**.

NETWORK SEPARATION
Fully separate the IACS from other **internal** and **external** networks by creating « **demilitarized** » zones (DMZ).

PERIMETER PROTECTION
Protect the IACS from unauthorized access by using **firewalls**, **authentication**, **authorizations**, **VPN** (IPsec) and **anti-virus software**. Also take into account the **remote access** to the IACS.

NETWORK SEGMENTATION
Make use of **switches** and **VLANs** which divide the network into **sub-networks**. They enable the containment of a potential security breech to only one segment.

DEVICE HARDENING
Configure **PACs**, **PCs**, **switches**, **I/Os** and **instruments** for increased security: **serious** password management, **user profile** definition, **deactivation** of unused services and interfaces.
HIPS: Host Intrusion Prevention System

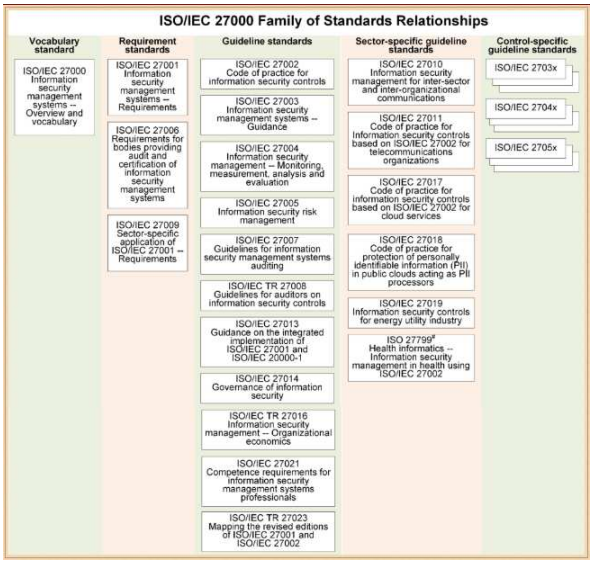
MONITORING AND UPDATE
Permanent surveillance of network communications and of all operator **activities**. **Software** and **firmware** updates to close breaches.

You should definitely initiate a cybersecurity discussion if find unprotected network designs - your customer will thank you in the long run.

Contenido

Estándares ISO 27000

Un conjunto de estándares



La norma ISO/IEC 27001, publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), se conoce como "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos".

La edición más reciente de la norma ISO/IEC 27001:2013 que revisa la edición anterior publicada en 2005. ISO 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI - ISMS). El SGSI presenta un enfoque sistemático para mantener segura la información confidencial. Gestiona personas, procesos y sistemas de TI mediante la aplicación de procesos de gestión de riesgos. El SGSI no solo satisface a las grandes organizaciones, sino también a las pequeñas y medianas empresas.

ISO 27001 está diseñado para ser utilizado junto con controles de soporte, un ejemplo del cual se publica en el documento, ISO/IEC 27002:2013. El cumplimiento de ISO 27001 puede ser formalmente evaluado y certificado por un Organismo de Certificación acreditado. El SGSI de una organización certificado según la norma ISO 27001 demuestra el compromiso de una organización con la seguridad de la información y brinda confianza a sus clientes, socios y partes interesadas.

Por su parte, la ISO 27002 detalla 114 controles de seguridad que están organizados en 14 secciones y 35 objetivos de control.

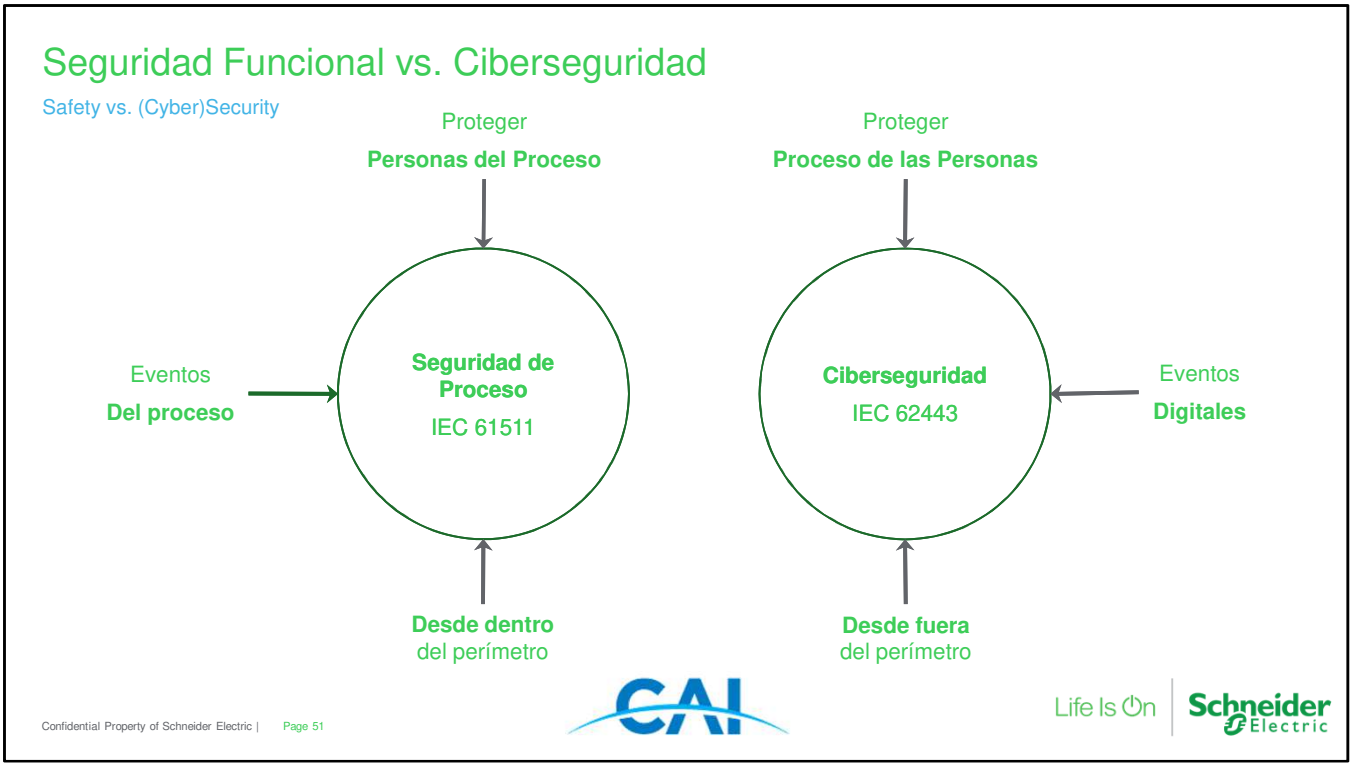
Para cumplir con los requisitos de certificación ISO 27001, el SGSI de una organización debe ser auditado por un organismo de certificación acreditado internacionalmente. Los requisitos en las secciones 4 a 10 en ISO 27001 son requisitos obligatorios sin exclusión permitida. Una vez superada la auditoría formal, el organismo de certificación otorga a una organización un certificado ISO/IEC 27001 para su SGSI. El certificado de ISO 27001 es válido por 3 años, después de lo cual el SGSI necesita ser recertificado.

Durante el período de validez de 3 años, una organización debe realizar el mantenimiento del certificado para

confirmar que el SGSI sigue siendo compatible, funciona según lo especificado y mejora continuamente. Para mantener la certificación, el organismo de certificación visitará el sitio del SGSI al menos una vez al año para llevar a cabo una auditoría de vigilancia. Durante la auditoría de vigilancia, solo se auditará una parte del SGSI.

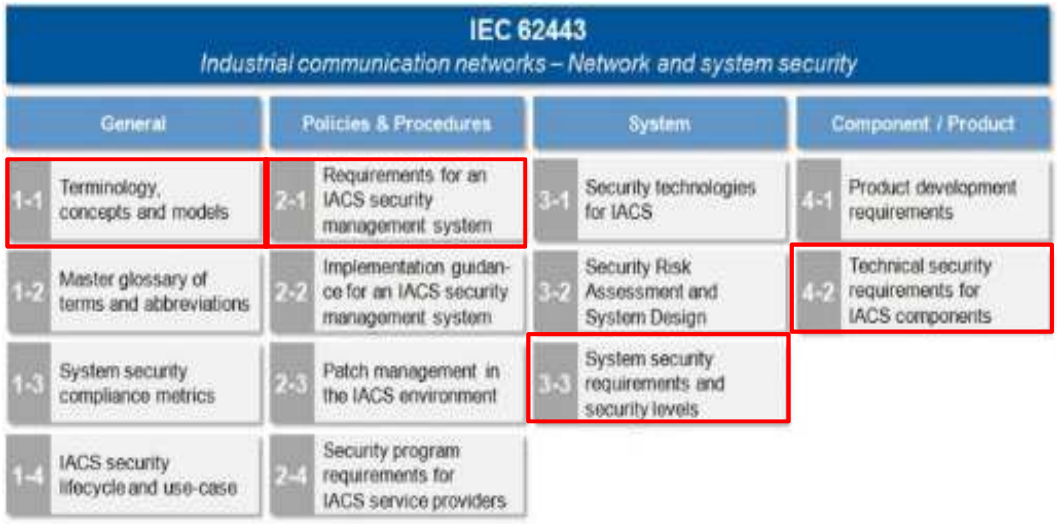
Hacia el final del período de tres años, el organismo de certificación audita todo el SGSI.

Principios de Seguridad Informática en Sistemas Industriales



Estándares ISA/IEC 62443

Un conjunto de estándares



Life Is On Schneider Electric

Overview of IEC 62443 standards. Spend time on 4-2 (product requirements), and 3-3 (system requirements).

ISA/IEC 62443

Definiciones ISA/IEC 62443-1-1

Zona de Seguridad: grupo de activos físicos o lógicos que comparten los mismos requisitos de seguridad.

Conducto: agrupamiento lógico de activos de comunicación, que protege la seguridad de los canales que contiene(*)

Nivel de Seguridad: funcionalidad para prevenir intervenciones que puedan impactar o influenciar el normal funcionamiento de los dispositivos y/o sistemas en la zona o conducto.

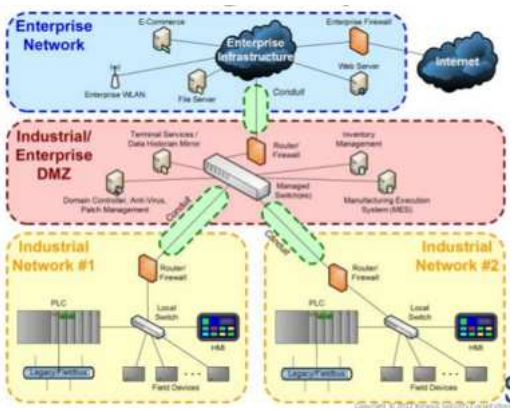
(*) Análogo a los conductos físicos, que protegen de daño a los cables en su interior.

ISA/IEC 62443

Zonas de Seguridad

Se divide la planta en “Zonas de Seguridad”.

- Permiten establecer la protección necesaria entre los límites y vínculos (conductos).
- Se clasifica con un determinado “Nivel de Seguridad”, de acuerdo con el riesgo aceptable.
- El nivel de seguridad define las prestaciones necesarias.



The IEC 62443 standard defines a process through which end users divide networks into security zones. Security levels can be assigned to each zone. Conduits connect the zones, and should be focused on to insure secure connection between zone.

ISA/IEC 62443

Niveles de Seguridad - Alcances

Nivel de Seguridad	Habilidades	Motivación	Intencionalidad	Recursos Humanos
SL1 Empleados	Sin conocimientos	Errores	No intencional	Individual
SL2 Cibercriminal, Hacker	Genéricas	Baja	Simple	Bajos (Individuos)
SL3 Hacktivistas, Terroristas	Específicas de IACS	Moderada	Ataque sofisticado	Moderados (Grupo de hackers)
SL4 Nación, Estados	Específicas de IACS	Alta	Campaña sofisticada	Extensos (Equipos multidisciplinarios)




Overview of IEC 62443 security levels.

ISA/IEC 62443

Niveles de Seguridad - Tipos

SL – T: Nivel de seguridad objetivo para una zona o conducto (TARGET)

SL – A: Nivel de seguridad alcanzado de una zona o conducto (ACHIEVED)

SL – C: Nivel de seguridad posible de las contramedidas asociadas con una zona o conducto. Capacidad inherente del nivel de seguridad posible de dispositivos o sistemas dentro de una zona o conducto (CAPABILITY)

Estándares ISA99/IEC62443

Requisitos Fundamentales de Ciberseguridad (FR) - ISA/IEC 62443-1-1

1. **Control de Acceso (AC):** Control del acceso a los dispositivos, la información o ambos, para protegerlos de accesos no autorizados.
2. **Control de Uso (UC):** Control del uso de los dispositivos, de la información o de ambos, para protegerlos de operaciones no autorizada.
3. **Integridad de Datos (DI):** Asegurar la integridad de los datos en canales de comunicación seleccionados, para protegerlos de cambios no autorizados.
4. **Confidencialidad de Datos (DC):** Asegurar la confidencialidad de los datos sobre los canales de comunicación seleccionados para protegerlos contra las escuchas subrepticias (eavesdropping)

Estándares ISA99/IEC62443

Requisitos Fundamentales de Ciberseguridad (FR) - ISA/IEC 62443-1-1

5. **Restricción de Flujo de Datos (RDF)**: Restringir el flujo de los datos en los canales de comunicación, para protegerlos de su publicación en fuentes no autorizadas.
6. **Disponibilidad de Recursos (RA):** Asegurar la disponibilidad de todos los recursos de red, para protegerla contra ataques de negación de servicio.
7. **Respuesta Oportuna a Eventos (TRE)**: Responder a violaciones de la seguridad notificando a la autoridad pertinente, registrando la evidencia forense necesaria, y tomando la acción correctiva automática y oportuna en situaciones de misión crítica o que comprometan la seguridad física (safety).

Certificación Achilles de WurldTech

Plataforma de ensayo que permite:

- Verificar la robustez de los dispositivos de comunicación industrial.
- Supervisar y verificar aspectos específicos, como respuesta a diferentes condiciones de tráfico de la red.
- Encontrar vulnerabilidades conocidas.
- Uso de lógica difusa para detectar problemas en la implementación de protocolos industriales.

Certifications for differentiation.
Every new product is Achilles certified – device can take traffic on the network, and can take random data (fuzzing). Only communications robustness. You could have bad other security features.
1 standard, 13 parts. Discuss each of the tiers.
Level 1 end devices,
Level 2 PLCs

Certificación Achilles de WurldTech

Tipos de ensayos

Achilles Grammars:

- Prueba de las condiciones del límite de los protocolos.
- Iteraciones sistemáticas sobre cada campo y combinaciones de campos para producir pruebas repetibles y cuantificables de los tipos comunes de errores de implementación.
- Envío de paquetes inválidos, malformados o inesperados al dispositivo bajo prueba (DUT) para probar vulnerabilidades en capas específicas de la pila de protocolos.

Achilles Storms

- Generación de paquetes a un ritmo alto para examinar la capacidad del DUT para manejar altas tasas de tráfico para diferentes protocolos.
- Búsqueda de los umbrales para los cuales el dispositivo ya no puede responder a otras peticiones normales (DoS), frente a diferentes tipos de “tormentas de tráfico”.

Certificación Achilles de WurldTech

Tipos de ensayos

Prueba de vulnerabilidades:

- Pruebas para la detección de vulnerabilidades conocidas (con una alta probabilidad de existir en dispositivos de control), que explotan diferentes condiciones de tráfico.

Certificación Achilles de WurldTech

Protocolos de comunicación ensayados

- EtherNet/IP (CIP)
- Foundation Fieldbus (FF-HSE)
- Modbus TCP/IP
- OPC UA
- PROFINET IO
- DNP3
- MMS (IEC 61850/ICCP)
- Modbus TCP/IP
- SES-92
- ZigBee SE (802.15.4)

Life Is On Schneider Electric

Certificación Achilles de WurldTech

Funcionalidades Verificadas

Comunicaciones de bajo nivel

- ICMP
- ARP
- Estado del vínculo

Comunicaciones de alto nivel

- OPC
- Heartbeat
- Puertos TCP y UDP
- Desempeño Windows/Linux

Control

- Respuesta de E/S discretas (nivel estático u onda cuadrada)
- Respuesta de E/S analógicas

Certificación Achilles de WurldTech

Niveles Certificación Achilles

Nivel 1

- Verifica las implementaciones de los protocolos, (sobre Ethernet) ARP, IP, ICMP, TCP y UDP, verificando su robustez y confiabilidad.

Nivel 2

- Ensayos más rigurosos, con mayores variedad de condiciones extremas de operación (estados no válidos de protocolos, tormentas de paquetes, etc.)

Listado de productos certificados(*)

(*) https://www.ge.com/digital/services/certifications/achilles-communications-certified-products

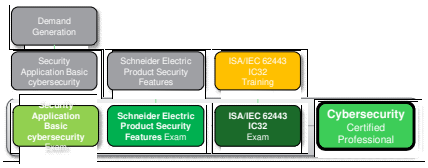
SE Cybersecurity Certifications

Cybersecurity Certified Professional

Learning Path

Investment required: 3.5 days /1500$

- 3 x Webinars, 1 x Classroom Course with examinations for both.



Life Is On Schneider Electric

CAI

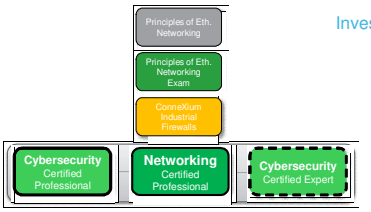
Life Is On Schneider Electric

SE Cybersecurity Certifications

Cybersecurity Certified Expert

Learning Path

- Cybersecurity Certified Professional + Networking Certified Professional & Hirschmann Firewall Trainin



Investment required: 8.5 days /2800$

Life Is On Schneider Electric

CAI

Life Is On Schneider Electric

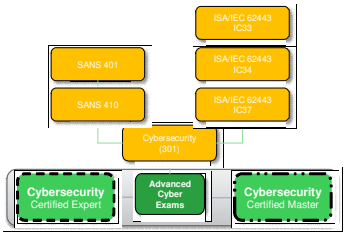
SE Cybersecurity Certifications

Cybersecurity Certified Master

Learning Path

Investment required: 22.5 days /9700$

- Cybersecurity Certified Expert + Advanced Cyber Topic:
  - Option 1: SANS 401 + SANS 410 + Cybersecurity (301)
  - Option 2: IEC Advanced (IC33, IC34 & IC37) + Cybersecurity (301)

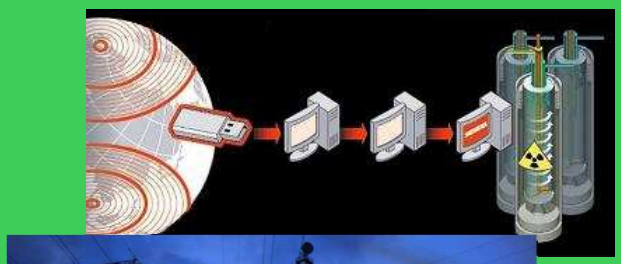


Life Is On Schneider Electric

CAI

Life Is On Schneider Electric

Contenido



Stuxnet

Life Is On Schneider Electric

Section title with image slide

Principios de Seguridad Informática en Sistemas Industriales

Stuxnet

El primero…

Primer reporte de su aparición en junio de 2010, en una planta de enriquecimiento de uranio iraní.

"Gusano" de un tamaño aproximado de 500 Kby.

Primera infección por unidad de memoria USB, aprovechando vulnerabilidades "día cero" de Microsoft y conocidas de WinCC y Step 7.

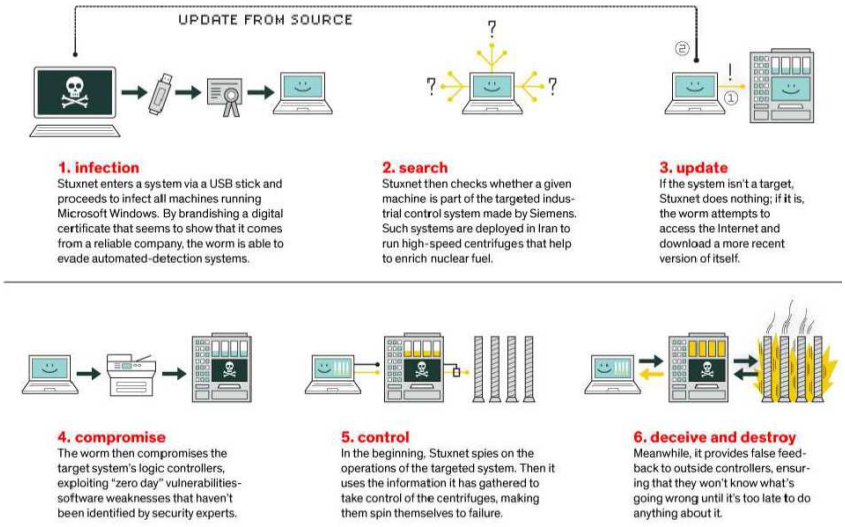
Afectó a más de 45.000 IACS en varios países (60% en Irán y 90% en países asiáticos).

Primer malware que ataca un IACS y con consecuencias en el mundo físico (no digital).

Principios de Seguridad Informática en Sistemas Industriales

Stuxnet

¿Cómo funciona?



The Real Story of Stuxnet - IEEE Spectrum 07/2016

Stuxnet

Conclusiones

Analizado en detalle por Kaspersky Lab y por Symantec.

Por su complejidad se concluyó que mismo fue realizado por especialistas en seguridad informática y en IACS.

Para algunos expertos es el primer caso de un arma en un escenario de ciberguerra.

Red de distribución eléctrica de Ucrania

Life Is On Schneider Electric

Section title with image slide

Ataques a red de distribución eléctrica de Ucrania

¿Qué ocurrió..?

- El sistema de distribución de energía eléctrica de la zona occidental sufrió ciberataques en diciembre de 2015 y 2016.
- El más grave fue el de 2015, con aproximadamente 225.000 personas afectadas por falta de suministro, durante varias horas.
- Por la complejidad del ataque, los especialistas concluyen que fue un acto de ciberguerra.
- Constituye un ejemplo de una “Amenaza Permanente Avanzada (APT)”
- Ver https://www.isa.org/intech/20170406/.

Ataques a red de distribución eléctrica de Ucrania

¿Cómo se realizó el ataque en 2015..?

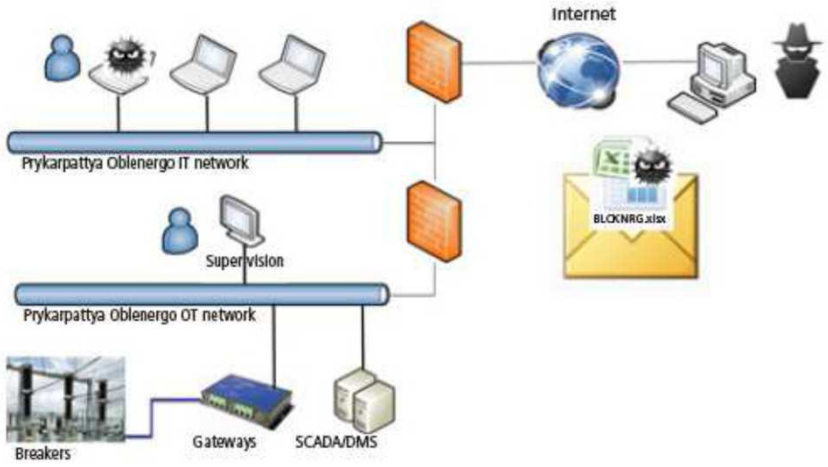
Se cumplieron tres etapas consecutivas:

1. Intrusión inicial del sistema informático (IT) por medio de “spear pishing”.
2. Inteligencia para recolectar información de las redes de IT y OT, utilizando una versión del malware BlackEnergy: escaneos de red, barrido de sistemas, identificación de vulnerabilidades, diseño del ataque e instalación de malware adicional.
3. Ejecución del ataque en dos fases, que duró sólo 10 minutos, el 23 de diciembre.

Fuente: ISA InTech Magazne – Mar/Apr 2017

Ataques a red de distribución eléctrica de Ucrania

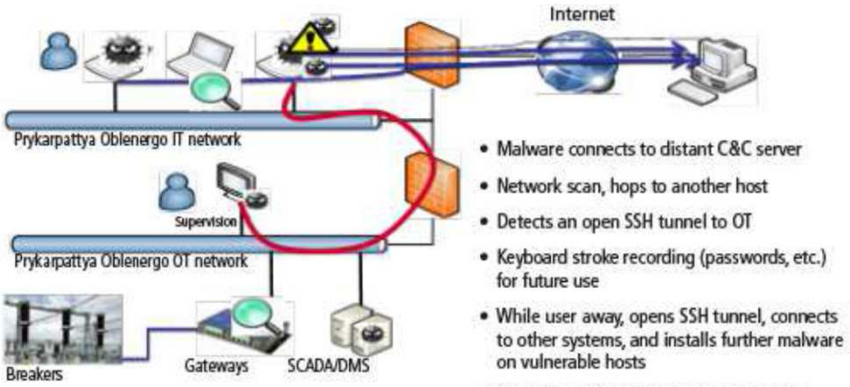
Etapa 1 – Intrusión Inicial



Fuente: ISA InTech Magazne – Mar/Apr 2017

Ataques a red de distribución eléctrica de Ucrania

Etapa 2 – Preparación

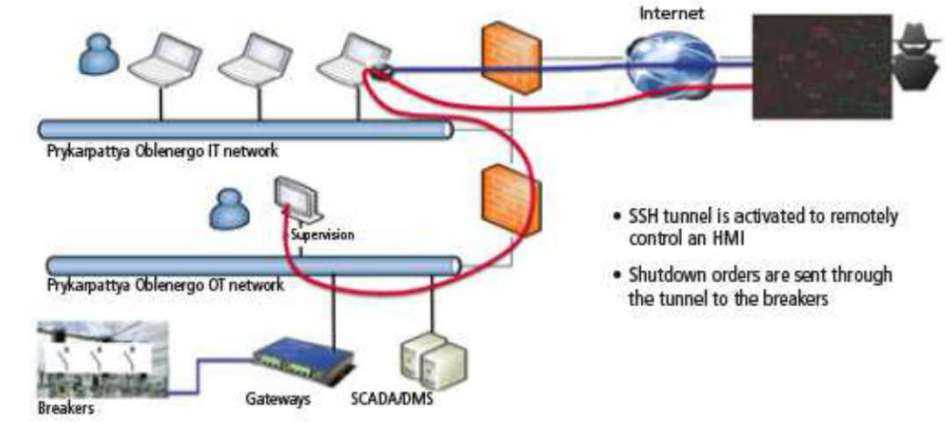


- Malware connects to distant C&C server
- Network scan, hops to another host
- Detects an open SSH tunnel to OT
- Keyboard stroke recording (passwords, etc.) for future use
- While user away, opens SSH tunnel, connects to other systems, and installs further malware on vulnerable hosts
- Cleanup and installation on a low-profile persistent threat, ready for activation

Fuente: ISA InTech Magazne – Mar/Apr 2017

Ataques a red de distribución eléctrica de Ucrania

Etapa 3 – Ejecución Fase 1

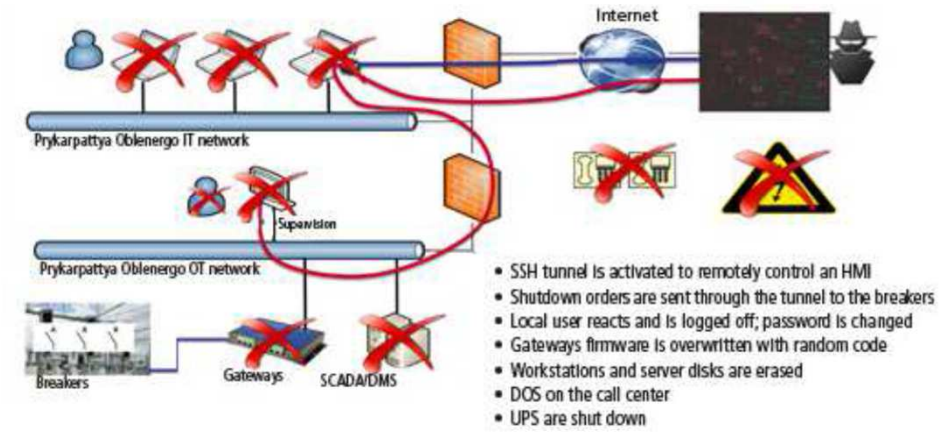


Fuente: ISA InTech Magazne – Mar/Apr 2017

Principios de Seguridad Informática en Sistemas Industriales

Ataques a red de distribución eléctrica de Ucrania

Etapa 3 – Ejecución Fase 2



- SSH tunnel is activated to remotely control an HMI
- Shutdown orders are sent through the tunnel to the breakers
- Local user reacts and is logged off; password is changed
- Gateways firmware is overwritten with random code
- Workstations and server disks are erased
- DOS on the call center
- UPS are shut down

Fuente: ISA InTech Magazne – Mar/Apr 2017

Ataques a red de distribución eléctrica de Ucrania

¿Qué fallo según el estándar ISA/IEC 62443?

1.13	There was no restriction for access from a nontrusted network, which was demonstrated by the fact that, once the hacker had the SSH access password, he or she could connect to the OT network without further credentials, local validation, etc.
2.4	Mobile code: The actual transfer of malware to several systems on the OT network demonstrated that there was no control of files in transit on the network.
2.6	During the attack, the OT operator had no straightforward way to terminate the remote connection, which is an SL-2 RE.
3.2	No malicious code protection: This is unfortunately most often the case in OT. Although it is not possible to install anti-malware software on all OT equipment, the total absence of such software paves the way for cyberattacks and allows the hacker to use publicly available exploits instead of having to develop custom ones.
5	Overall the FR5 SL is 2, which is fine. But this is a very effective demonstration that a firewall is not enough to ensure security. Indeed, as other controls (authentication, detection, local control) were missing, the hacker could use the single exception in the firewall rules without being detected or prevented.
6.2	The overall lack of network monitoring, both on the IT and OT networks, allowed the hacker to scan the network and identify vulnerabilities for days or even weeks.
Note: This SR is set only for SL=2 or higher. It is strange that this requirement, much more effective than SR 5.2 (see discussion above), is only required starting at SL=2 when filtering is already required for SL=1.	
7.4	Disks were erased during the final step of the attack: The standard operating systems could have been restored with an adequate backup policy, except for the gateways where firmware, once overwritten, was unrecoverable.

Fuente: ISA InTech Magazne – Mar/Apr 2017

Ver estándar 62443-3- 3 para una descripción detallada de los “Foundational Requirements (FR)” y de los “System Requirements”.

Ataques a red de distribución eléctrica de Ucrania

Conclusiones

Lo que se tuvo en cuenta:

- Utilización de contraseñas seguras.
- Uso de un firewall, configurado correctamente para restringir el flujo de datos.
- Completo registro de eventos.

Fuente: ISA InTech Magazne – Mar/Apr 2017

Lo que faltó:

- Supervisión de la red con barridos extensivos, detección de vulnerabilidades y del uso del vínculo protegido por SSH.
- Uso de autenticación de dos factores o local en OT para los accesos remotos; permitiendo las conexiones sin ser detectadas desde IT por mucho tiempo.
- Un sistema de detección de intrusiones (IDS); facilitó el barrido de la red de OT, descubrir sus vulnerabilidades, ejecutar código móvil (malware, exploits) y violar restricciones de transferencia.

Análisis de Casos

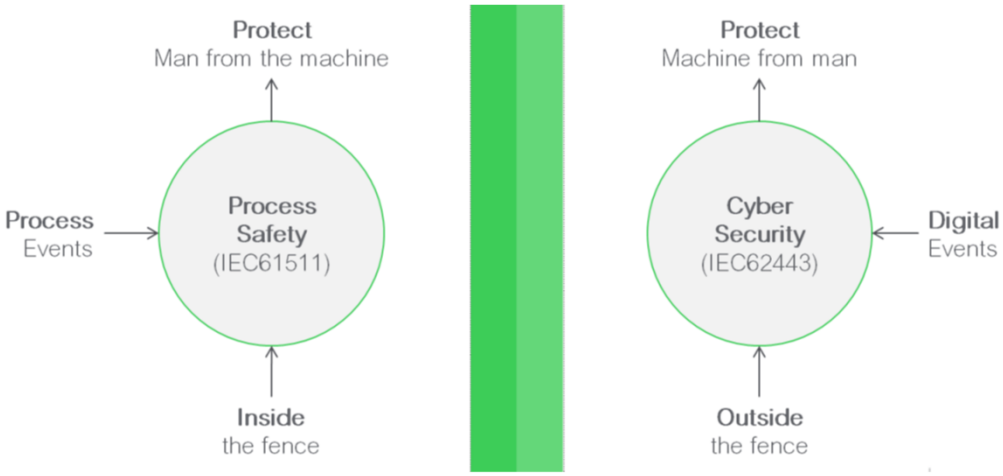
Triton

Randall el Tritón de Monsters Inc.

Principios de Seguridad Informática en Sistemas Industriales

Triton ~ Trisis ~ Hatman

Seguridad Funcional y Ciberseguridad



Life Is On Schneider Electric

Principios de Seguridad Informática en Sistemas Industriales

Triton ~ Trisis ~ Hatman

- Ocurrió en agosto de 2017
- Incidente que involucró a un único controlador Triconex, de 10 años de antigüedad
- El fabricante colaboró con organizaciones independientes y con varias agencias de EE. UU. para el análisis del incidente
- La evidencia forense obtenida determinó que el ataque fue posible por una acumulación de fallas de seguridad en TODO el sistema informático
- Se determinó que el malware estaba destinado a afectar una versión específica de un controlador Triconex, lanzado en 2001, con una versión antigua de firmware.
- El controlador Triconex involucrado en el ataque respondió correctamente, llevando la planta a una condición segura
- No se afectaron las instalaciones, las personas o el medio ambiente
- Se desarrolló una herramienta para detectar y eliminar el malware

Department of Homeland Security
ICS-CERT
DARPA
FBI
National Security Agency

Principios de Seguridad Informática en Sistemas Industriales

Triton ~ Trisis ~ Hatman

- El ataque **no está relacionado con un virus,** que se pueda propagar y propagar fácilmente.
- El malware sólo actuará si:
  - El sitio utiliza un controlador Triconex de un modelo antiguo y sin actualización de su firmware
  - La red de seguridad es accesible local o remotamente
  - Los atacantes pueden acceder a la terminal TriStation u otra máquina conectada a esa red de seguridad
- Toda la instalación informática debe adecuarse a estándares reconocidos de ciberseguridad (p.e. IEC 62443)
- La llave de seguridad del controlador debe estar siempre en la posición recomendada por el fabricante

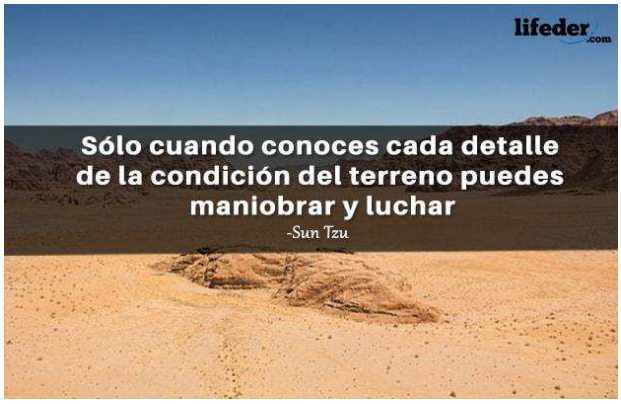
Y atacar es más fácil de lo que parece…

Life Is On Schneider Electric

Section title with image slide

El arte de la (ciber)guerra

La sabiduría de Sun Tzu



Algunos sitios útiles

O una guía útil para “Script Kiddies”

Shodan – IoT Browser: https://www.shodan.io/

Mapas de ciberataques:
https://cybermap.kaspersky.com/
https://threatmap.checkpoint.com/ThreatPortal/livemap.htmlSE

Security notifications:
http://www.schneider-electric.com/b2b/en/support/cybersecurity/security-notifications.jsp

Exploit database: https://www.exploit-db.com/

Browsers insecurities: http://webkay.robinlinus.com/

Análisis de archivos y URL sospechosas:
https://www.virustotal.com

Compruebe si tiene una cuenta que ha sido comprometida en una violación de datos:
https://haveibeenpwned.com/

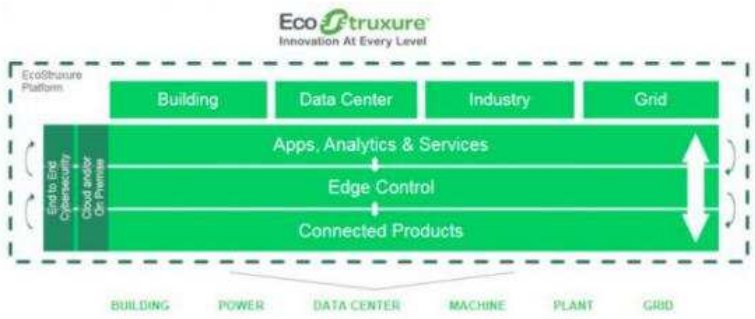
Probar robustez de contraseñas
https://howsecureismypassword.net/

Base de conocimiento y modelos de ataques:
https://attack.mitre.org

Contenido

La propuesta de Schneider Electric

EcoStruxure



Principios de Seguridad Informática en Sistemas Industriales

La propuesta de Schneider Electric

Productos y Soluciones Seguras

Desarrollo y ciclo de vida seguro

2.200 Desarrolladores entrenados

70 Ingenieros con ciber- certificaciones

5 Centros R&D certificados IEC 62443

>75 Productos certificados

Servicios de Ciberseguridad

>80 Expertos de servicios en ciberseguridad

- Auditorias y Evaluaciones
- Consultoría en Ciberseguridad
- Diseño e Implementación
- Capacitación
- Servicios de Mantenimiento

Partners Globales

CISCO, McAfee, intel Security, HIRSCHMANN, Microsoft, WATERFALL, NOZOMI NETWORKS

Regionales/Específicos Segmento

STORMSHIELD, JUNIPER NETWORKS, paloalto, Symantec, observable networks, INDUSTRIAL DEFENDER, FORTINET, OWL CYBERSECURITY, THALES

CAI

Electric

We have partnerships with best in class security vendors to help you secure your networks

- Some partners are global, others have more of a regional focus based on the profile of the partner.
- Examples of partnerships include: Cisco (e.g. Bliss secure pipeline offer), Microsoft, Industrial Defender, Hirschmann, Intel Security, Symantec, Stormshield, Thales, Waterfall, etc.
- We validate that our solutions work with selected partners.

Partner expertise

Authentication, Authorization, Accounting
Policy, Procedure, Documentation,
Endpoint Protection, Integrity Control,
Data Loss Prevention, Anti Virus / Malware
Network Segmentation (Secure Remote, DMZ,
Auxiliary and Process Control)
Patch Management, Hardening,
and Workstation / Server Security
Network Performance Monitoring /
Central Security Management and Alerting
Event Logging, System / Network Maintenance, and Disaster Recovery

ePAC Modicon M580

Section title with image slide

M580 – Características de Ciberseguridad

Integridad del firmware y de los ejecutables

- Firmware con firma digital e encriptado
- Los ejecutables de Unity Pro y los DLL de OFS DLL firmados electrónicamente

Integridad del sistema M580

- Verificación en tiempo real del procesador, memoria y tareas del sistema

Modos de operación segura del PLC

- Cambios de configuración y/o programa protegidos con contraseña, a nivel de PLC (para modificar la aplicación o cambiar el modo de operación)
- Protección, con una entrada discreta, de cambios RUN/STOP remotos
- Protección de la memoria del PLC controlada con una entrada discreta

Integridad del firmware y de los ejecutables
- Firmware con firma digital e encriptado
  - Se verifica la integridad del firmware al inicio, antes de la carga
  - Utiliza algoritmos criptográficos robustos (SHA256; RSA4096 y AES256)
- Los ejecutables de Unity Pro y los DLL de OFS DLL firmados electrónicamente
  - Verificación de integridad al inicio y por demanda

Integridad del sistema M580
- Verificación en tiempo real del procesador, memoria y tareas del sistema

Modos de operación segura del PLC

- Cambios de configuración y/o programa protegidos con contraseña, a nivel de PLC
  - Autenticación necesaria para modificar la aplicación o cambiar el modo de operación
- Protección, con una entrada discreta, de cambios RUN/STOP remotos
- Protección de la memoria del PLC controlada con una entrada discreta
  - Al habilitar la protección la única interacción posible con el PLC es en modo “sólo lectura”

M580 – Características de Ciberseguridad

Atributo de las variables que define el permiso de acceso remoto a las mismas (Lectura/Escritura, Sólo Lectura o Sin Acceso Remoto

Se configura en Unity Pro

Aplicable a todas las variables (localizadas y no localizadas)

Habilitación/Deshabilitación de servicios no necesarios

- Los servicios con esta posibilidad son: FTP, TFTP, HTTP, EIP, DHCP, BOOTP y SNMP

Listas de control de acceso (ACL)

- Las listas de control de acceso se aplican a estos protocolos: FTP, TFTP, HTTP, MBTCP, EIP y SNMP
- Control de direcciones IP únicas o por subred

Atributo de las variables que define el permiso de acceso remoto a las mismas:

- Lectura / Escritura
- Sólo Lectura
- Sin Acceso Remoto

Se configura en Unity Pro

Aplicable a todas las variables (localizadas y no localizadas)

Habilitación/Deshabilitación de servicios no necesarios

- Los servicios con esta posibilidad son:
  - FTP, TFTP, HTTP, EIP, DHCP, BOOTP y SNMP
- El control de esos servicios puede hacerse desde:
  - Unity Pro al configurar
  - Programación para FTP y HTTP

Listas de control de acceso (ACL)

- Las listas de control de acceso se aplican a estos protocolos:
  - FTP, TFTP, HTTP, MBTCP, EIP y SNMP
- Control de direcciones IP únicas o por subred

M580 – Características de Ciberseguridad

El PLC y Unity Pro incluyen un cliente SYSLOG

- Detectan y envían a una base de datos SYSLOG todos los eventos relacionados con seguridad, tanto del PLC como de Unity PRO
- Algunos ejemplos de eventos de seguridad: Conexiones exitosas y fallidas, Cambios significativos del sistema (configuración del PLC, reinicios, cambios RUN/STOP)
- Compatible con cualquier servidor SYSLOG

Protocolo IPSEC para asegurar la comunicación entre la red de control y la red de PLC y dispositivos (en módulos de comunicación BMENOC)

- IPsec provee autenticación de origen y verificación de integridad de datos
- Del lado del cliente se utilizan servicios estándar de Windows (Windows security policy)
- Bajo impacto en la comunicación con el SCADA: +10 ms para leer 10.000 variables

El PLC y Unity Pro incluyen un cliente SYSLOG

Detectan y envían a una base de datos SYSLOG todos los eventos relacionados con seguridad, tanto del PLC como de Unity PRO

Algunos ejemplos de eventos de seguridad:

Conexiones exitosas y fallidas

Cambios significativos del sistema (configuración del PLC, reinicios, cambios RUN/STOP)

Formato del evento de seguridad:

fecha/hora/tipo de evento/@IP

Compatible con cualquier servidor SYSLOG

Protocolo IPSEC para asegurar la comunicación entre la red de control y la red de PLC y dispositivos

- Implementada en módulos de comunicación BMENOC
- IPsec provee autenticación de origen y verificación de integridad de datos

•Del lado del cliente se utilizan servicios estándar de Windows (Windows security policy)

•Bajo impacto en la comunicación con el SCADA :

+10 ms para leer 10.000 variables

M580 – Características de Ciberseguridad

Certificaciones

Certificación Achilles nivel 2

- Todos los procesadores y módulos con puerto Ethernet cuentan con esta certificación
- Somete a ensayos extensivos la implementación de los protocolos ARP, IP, ICMP, TCP y UDP
- Prueba la robustez del dispositivo para soportar sin bloqueos una serie de ensayos, incluyendo tráfico elevado y paquetes mal formados

EDSA nivel 1

- Certificación ISA Secure
- Conforme con estándar IEC 62443-4-1 (dispositivos embebidos)

Certificaciones locales

- CSPN - Francia
- CITSEC - China

Altivar Process
Altivar Machines

Life Is On Schneider Electric

Section title with image slide

Altivar Process Altivar 340

Certificados IEC62443 y Achilles

Control de acceso (WEB server y contraseña general)

Protección de acceso a parámetros

Certificación Achilles nivel 2

Filtrado maestro de IP

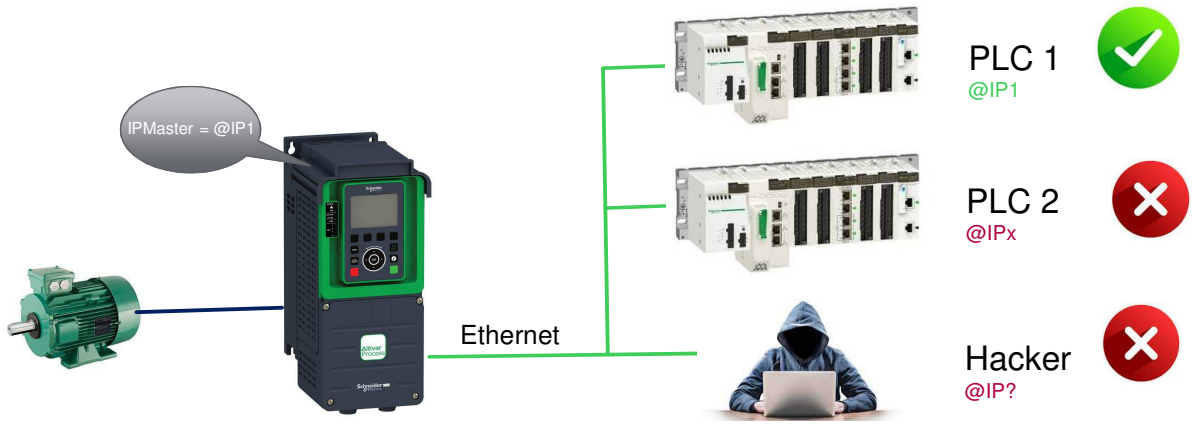
Control de servicios

Control de integridad de configuración

Life Is On Schneider Electric

Control de Acceso para Comandos

IP Master ~ Autorización Comando



IP master – allow access only based on IP address. Table where you assign IP addresses. Start, stop and change speed.

Protección de Configuración

Visibilidad de Parámetros Configurable

Selección de Canal

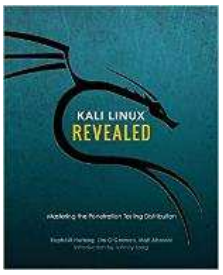
Modbus Serie — No visible en Modbus

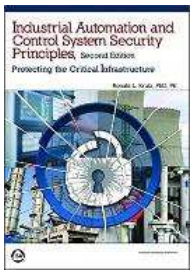
Comunicacion Profibus, Ethernet, etc. — No visible en redes

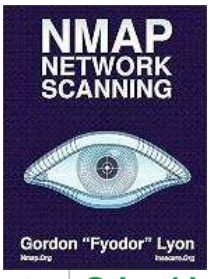
Display Gráfico — Visible en display gráfico

Mayor información en

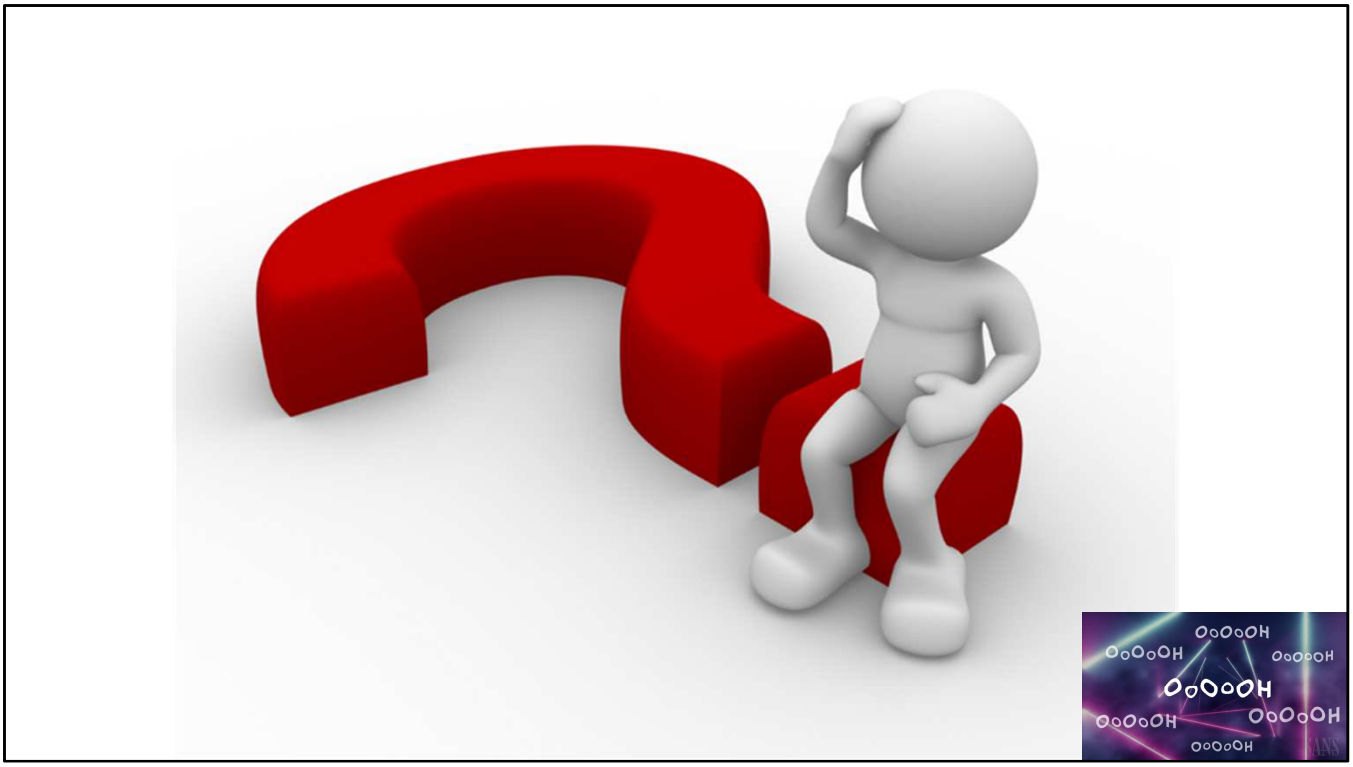
- Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure, 2nd. Edition
  Ronald L. Krutz
- Kali Linux Revealed – Mastering the Penetration Testing Distribution
  Raphaël Hertzog, Jim O'Gormand and Mati Aharomi
- Nmap Network Scanning – The Official Nmap Project Guide to Network Discovery and Security Scanning
  Gordon "Fyodor" Lyon



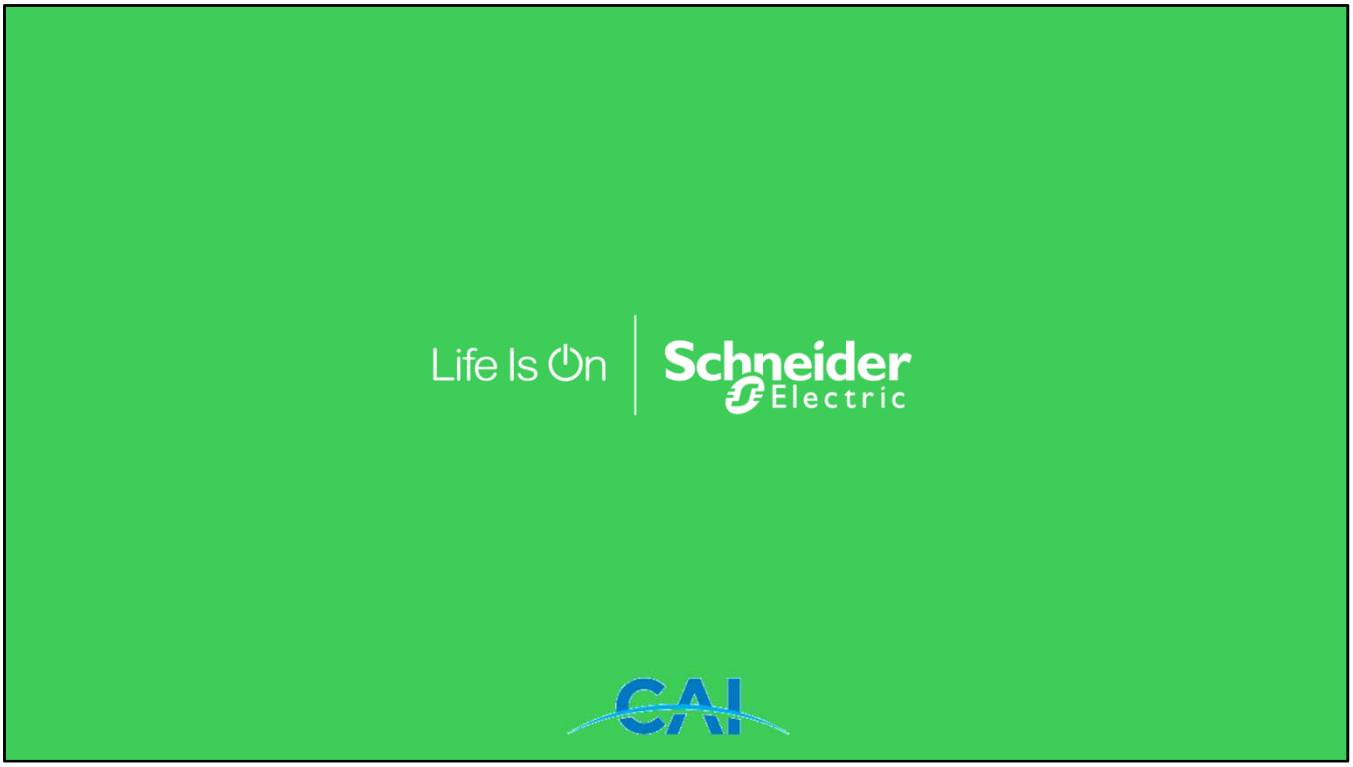




Principios de Seguridad Informática en Sistemas Industriales



Principios de Seguridad Informática en Sistemas Industriales



Closing slide