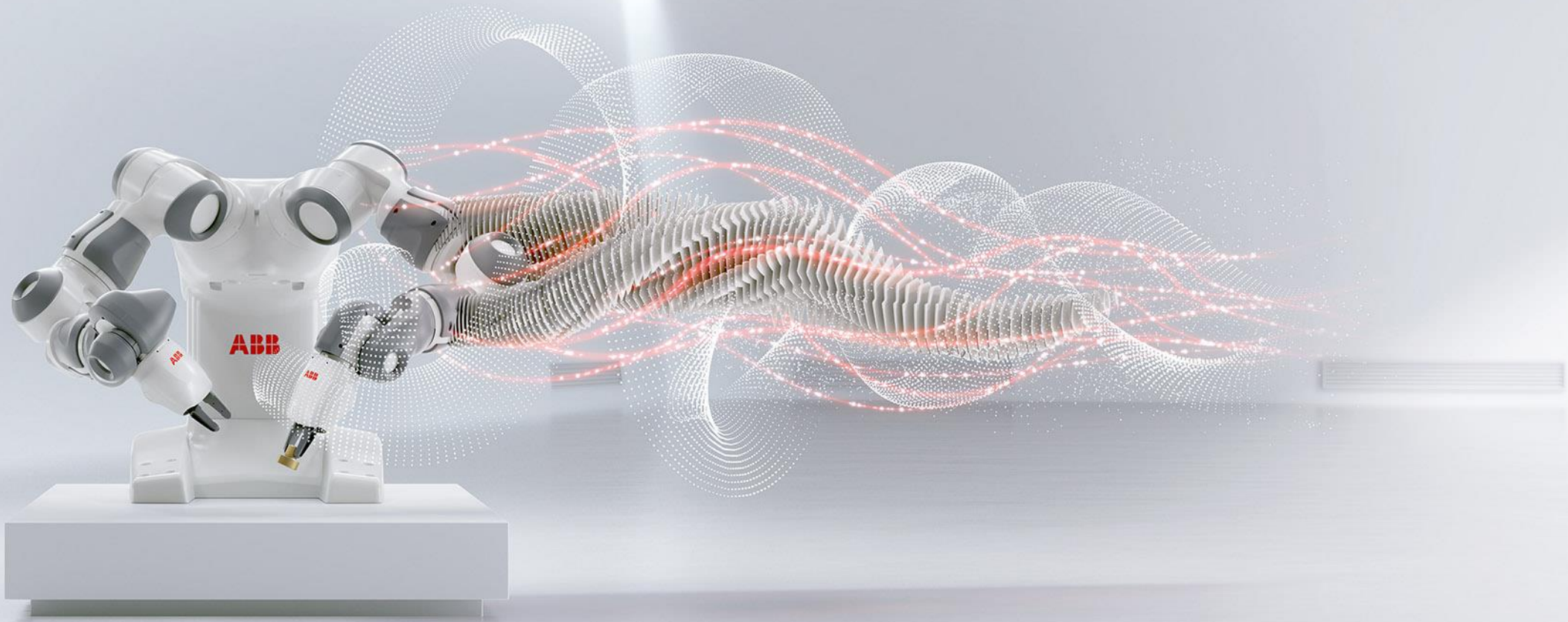


SANTIAGO – CHILE - JULIO 30-31, 2019

XI Jornadas Técnicas ABB en Chile

Ciberseguridad en sistemas de control industrial

Ivan Granados - Chile

XI Jornadas Técnicas ABB en Chile

Índice

Ciberseguridad en sistemas de control industrial

Indice

- Estado de la ciberseguridad industrial
- El impacto de un ciberataque
- Los desafíos de la ciberseguridad
- Medidas base de seguridad para un ICS
- Servicios digitales de ABB

3 stages to protect digital systems

People process and technology: each must be leveraged to protect digital systems

People

- People are critical in preventing and protecting against cyber threats
- Organizations need competent people to implement and sustain cyber security technology and processes

Process

- Policies and procedures are key for an effective security strategy
- Processes should adapt to changes as cyber threats evolve

Technology

- Technology is important in preventing and mitigating cyber risks
- Technology needs people, processes and procedures to mitigate risks

XI Jornadas Técnicas ABB en Chile

Objetivo

Ciberseguridad en sistemas de control industrial

Objetivo

- Evolucion de los ciberataques en la ultima decada
- Impacto de un incidente de ciberseguridad
- Modelos de seguridad aplicados a ICS
- Ciberseguridad como un proceso

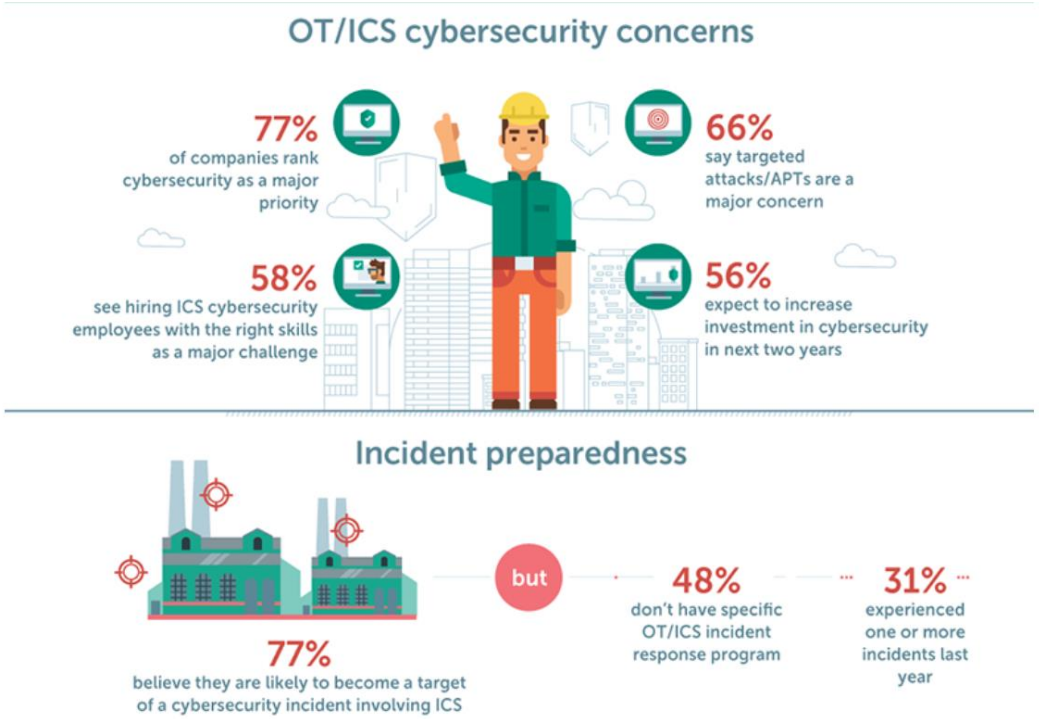
XI Jornadas Técnicas ABB en Chile

Estado de la ciberseguridad industrial

Ciberseguridad en sistemas de control industrial

Estado de la ciberseguridad industrial

- La ciberseguridad industrial es una prioridad, pero…
- Desconexión entre la percepción y la realidad.
- Incremento en incidentes de ciberseguridad
- Fuentes principales de amenaza
- Ataques no sofisticados



Karspersky Industrial Cybersecurity 2018

Ciberseguridad en sistemas de control industrial

Estado de la ciberseguridad industrial

2010 Stuxnet

- First publicly-known example of a cyber weapon
- Designed to disrupt the Iranian nuclear development program
- A self-propagating application (a "worm") spread via USB drives and network connections
- It took over the PLC controlling the uranium enrichment centrifuges and ultimately caused these to break down at an accelerated rate
- It was able to operate undetected for an extended period of time

2014 German Steel Mill

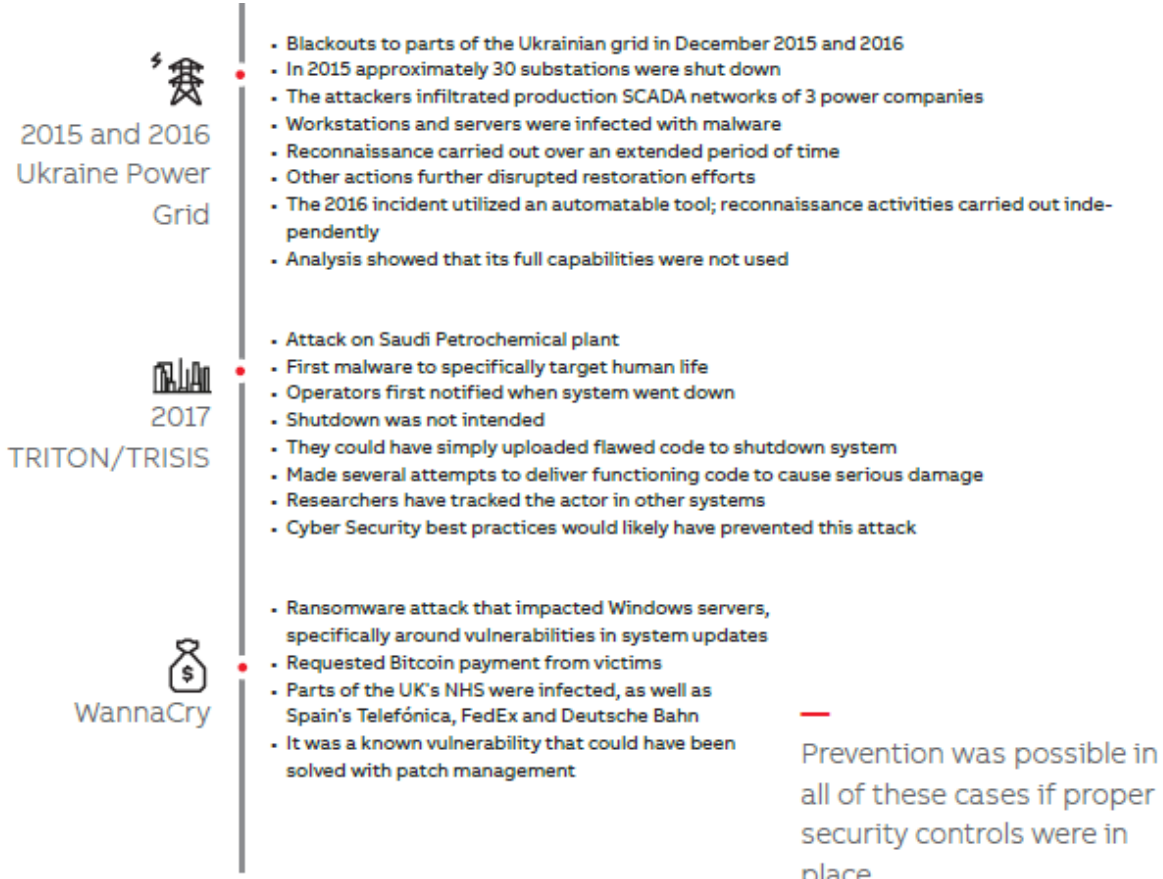
- Second confirmed case of a cyber attack causing physical damage
- Attackers used a spearphishing campaign to capture user credentials
- They connected through the business systems to the OT network
- Caused massive damage when a blast furnace had to be shut down abnormally

2014 Havex/Dragonfly

- Victims from multiple industries, including energy, manufacturing and pharmaceuticals
- Malware campaign using multiple attack vectors
- These were spearphishing, waterhole poisoning, and replacing suppliers' support websites
- Installed a Remote Access Trojan (RAT) on systems inside targets' networks
- RATs coordinated and updated via the internet

Ciberseguridad en sistemas de control industrial

Estado de la ciberseguridad industrial

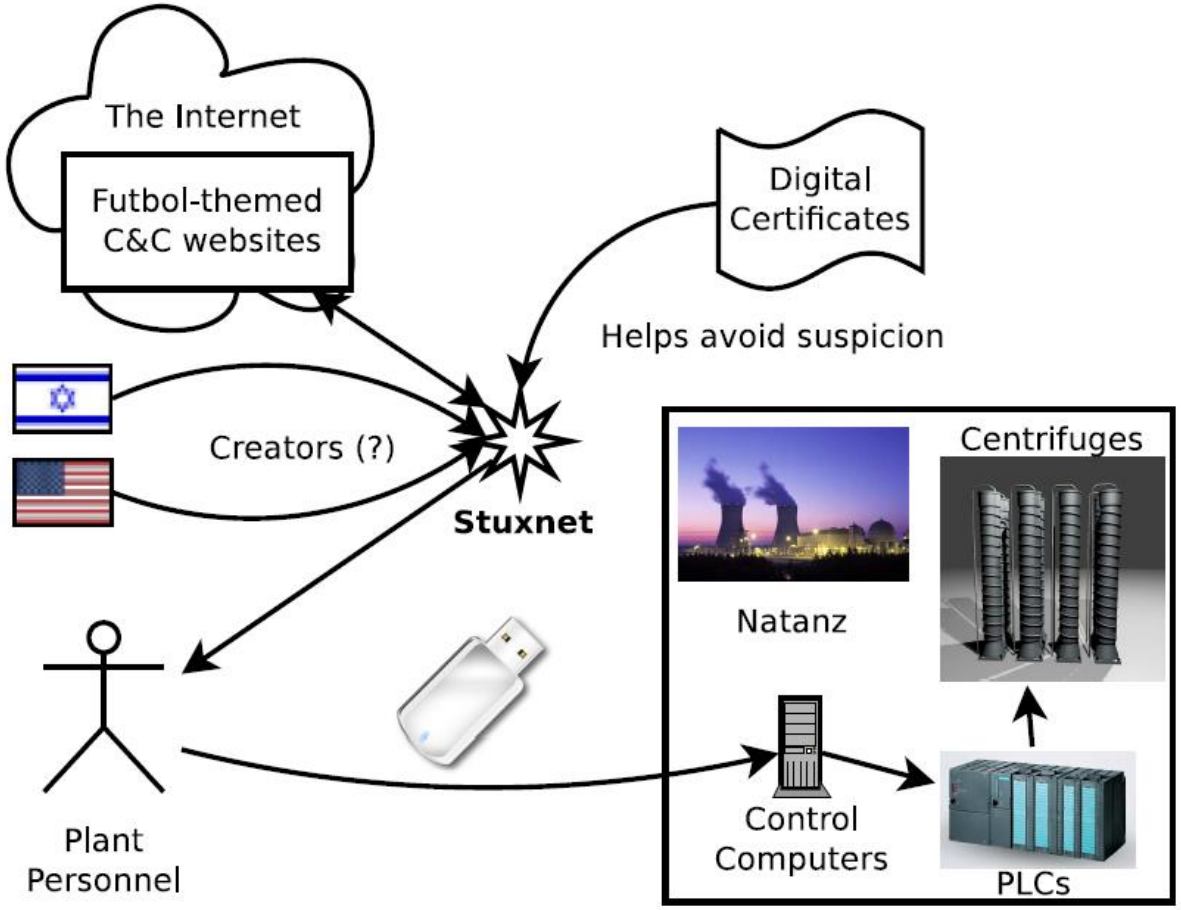


XI Jornadas Técnicas ABB en Chile

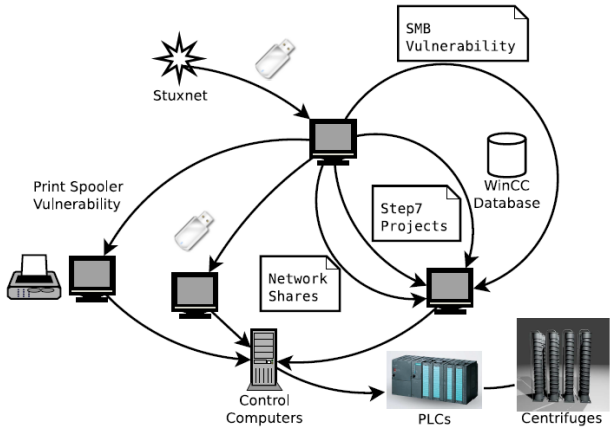
El impacto de un ciberataque

Ciberseguridad en sistemas de control industrial

El impacto de un ciberataque



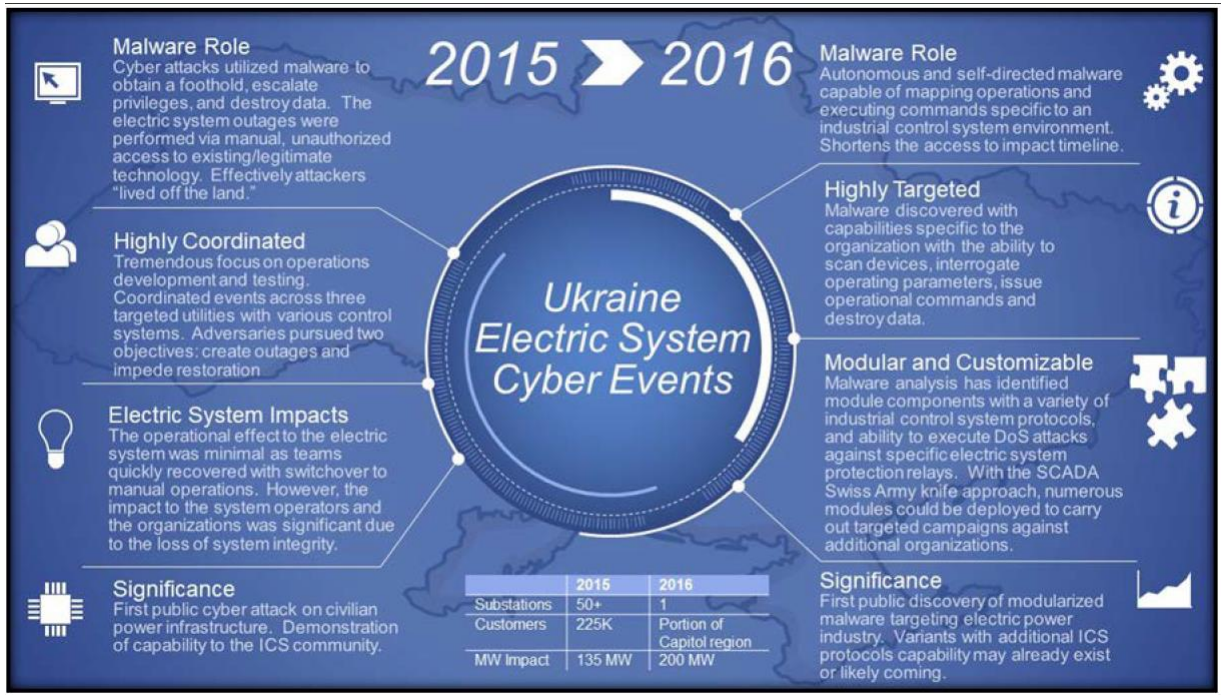
- Stuxnet – June 2010
- How does it spread?
  - USB Drives
  - WinCC via hardcoded password
  - Network Shares
  - MS10-061 Print Spooler vulnerability (0day at the time)
  - MS08-067 SMB vulnerability
  - Step7 Projects



Ciberseguridad en sistemas de control industrial

El impacto de un ciberataque

- Industroyer / CrashOverride - Ukrainian Power System Attack – 2015 & 2016
  - Issues breaker commands
    - IEC101
    - IEC104
    - IEC 61850
    - OLE for Process Control (OPC)
- Command and Control (C2C) Capabilities
- Launcher executed with direct access to SCADA Network
- Internal proxy listener – attack vector not publicly disclosed
- Device scanning tools
- Data destruction tools
- Extendable framework



Ciberseguridad en sistemas de control industrial

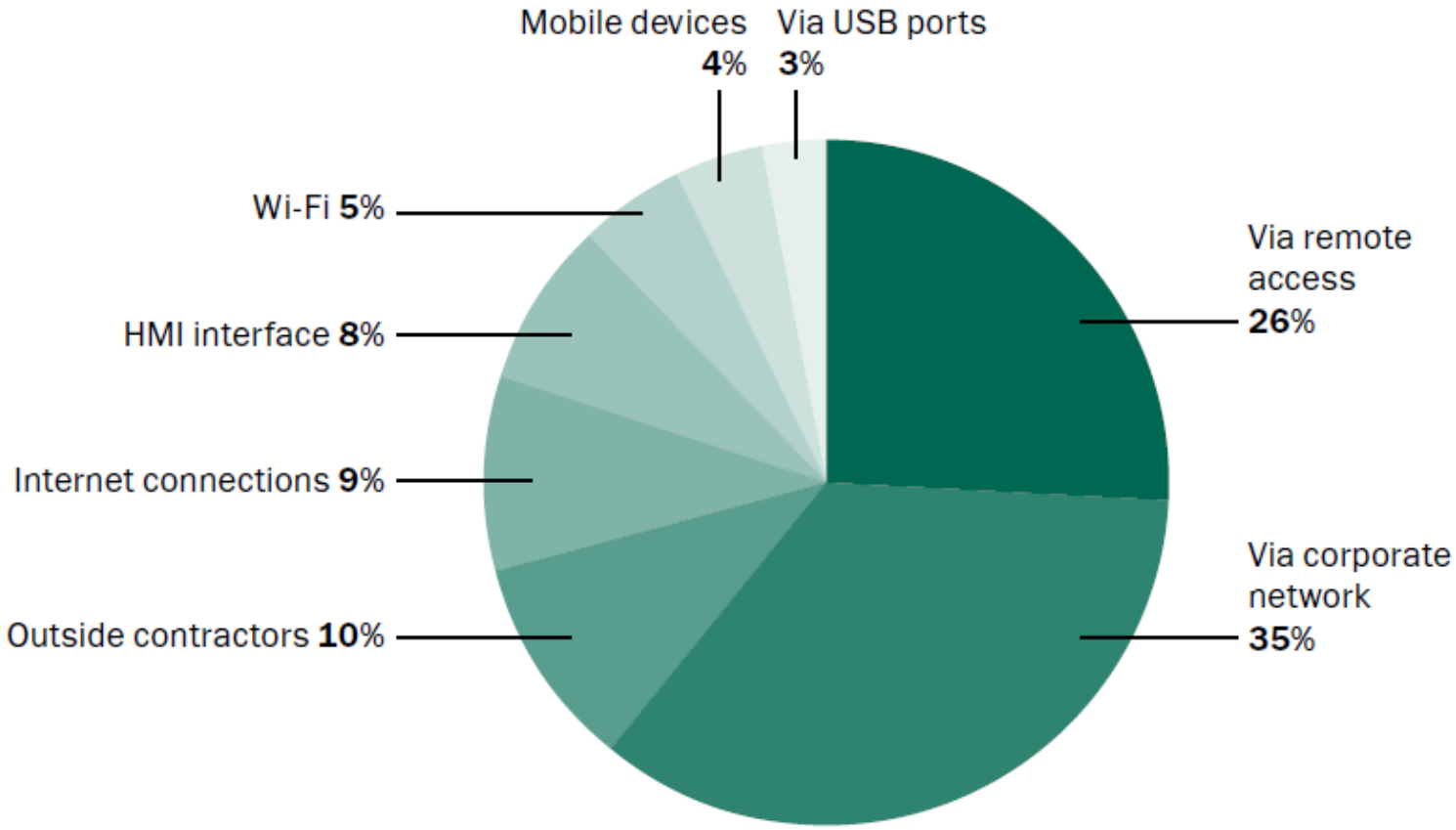
El impacto de un ciberataque

- Triconex Emergency Shutdown System - 2017
  - Controller Code Vulnerability.
  - Key Switch bit in unprotected memory.
  - First known malware that could kill people.
  - 6 controllers involved.
  - RDP sessions into Engineering workstations from IT network.
  - Poorly configured DMZ.
  - VPN compromised and infiltrated.
  - Unprecedented public sharing of attack findings by vendor.

Ciberseguridad en sistemas de control industrial

El impacto de un ciberataque

Sources from which malicious code penetrates industrial networks
(image courtesy of Securityincidents.net)



XI Jornadas Técnicas ABB en Chile

Los desafíos de la ciberseguridad

Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Reality	There is no such thing as 100% or absolute security
Process	Cyber security is not destination but an evolving target – it is not a product but a process
Balance	Cyber security is about finding the right balance – it impacts usability and increases cost

Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

Version		End of mainstream	End of extended*
Windows XP	SP 3	4/14/2009	4/8/2014
Windows Vista	SP 2	4/10/2012	4/11/2017
Windows 7	**SP 1**	1/13/2015	1/14/2020
Windows Server 2008	**R2**	1/13/2015	1/14/2020
Windows 8	**Windows 8.1**	1/9/2018	1/10/2023
Windows 10		10/13/2020	10/14/2025

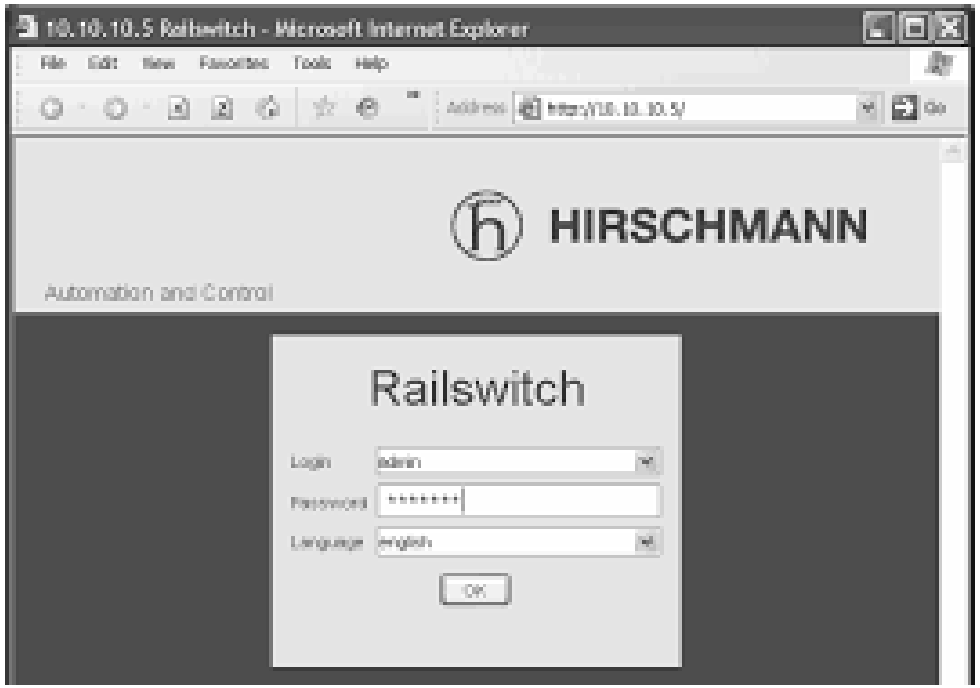
***End of extended: Security and non-security updates are no longer provided**

Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

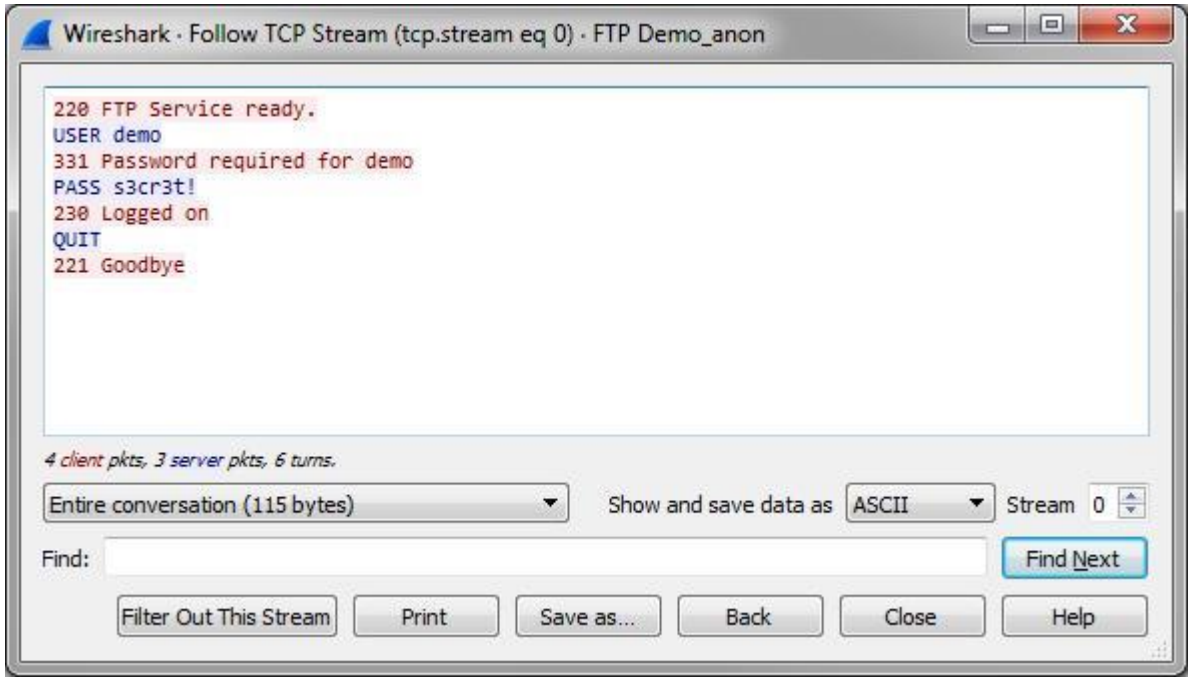


Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

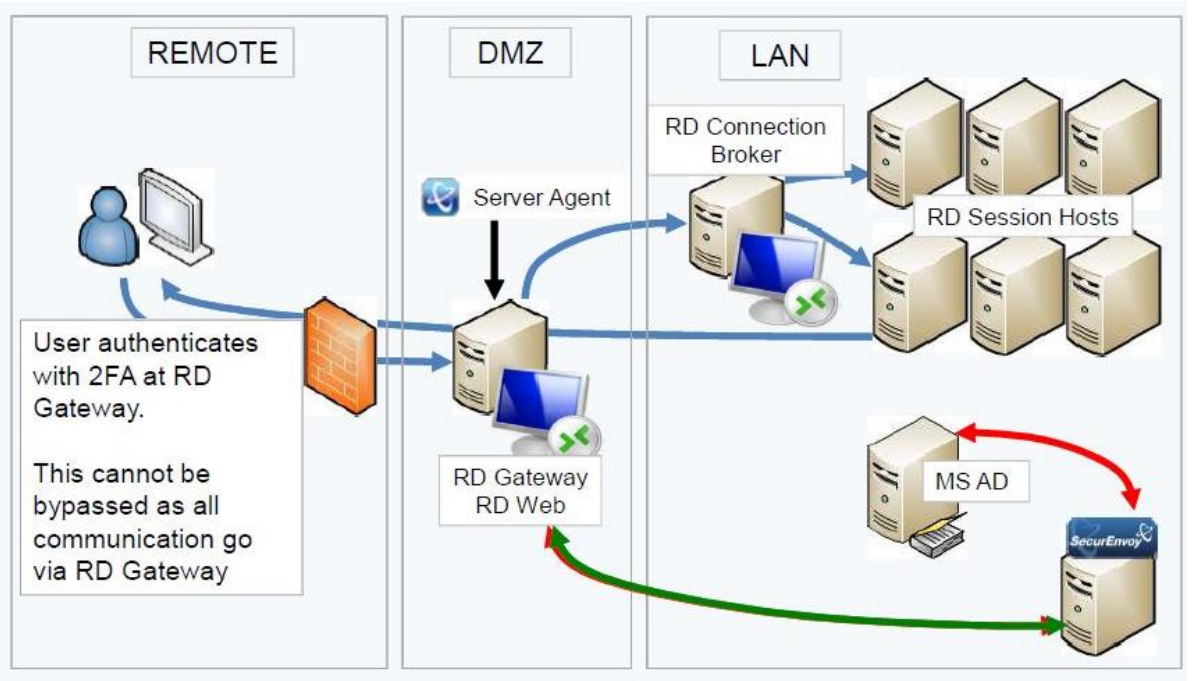


Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation



Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

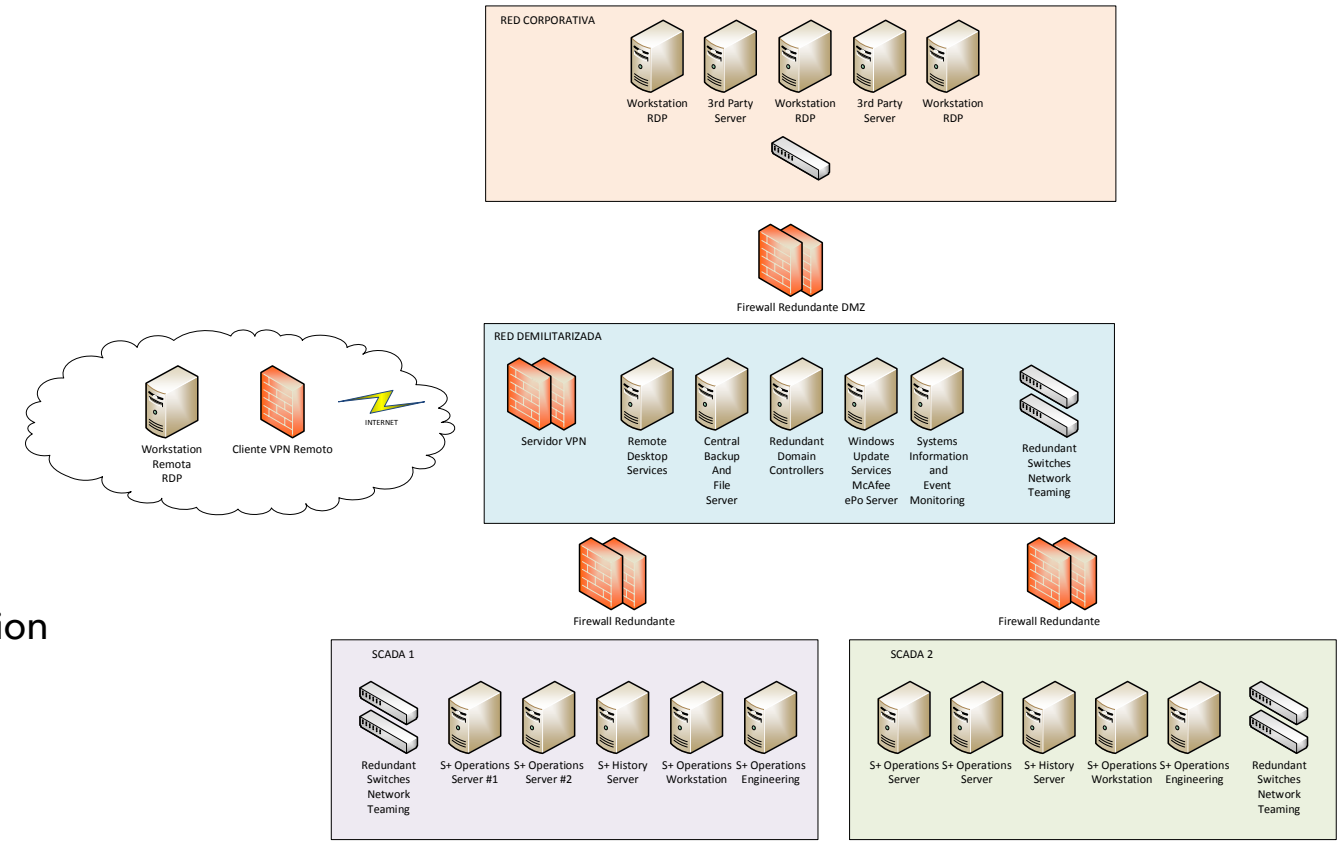
- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

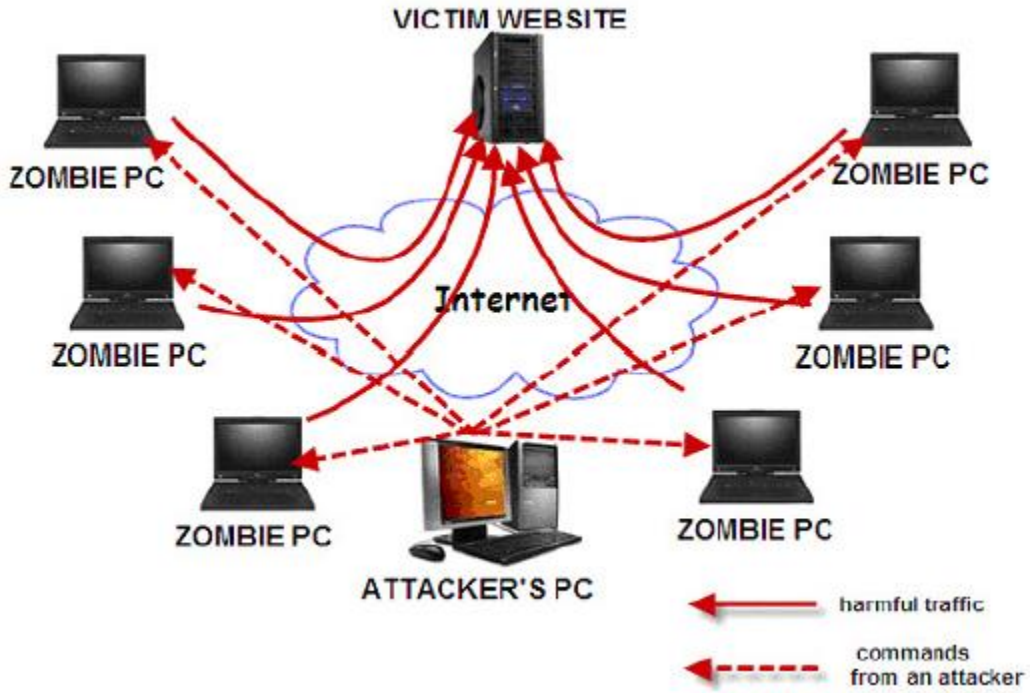


Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

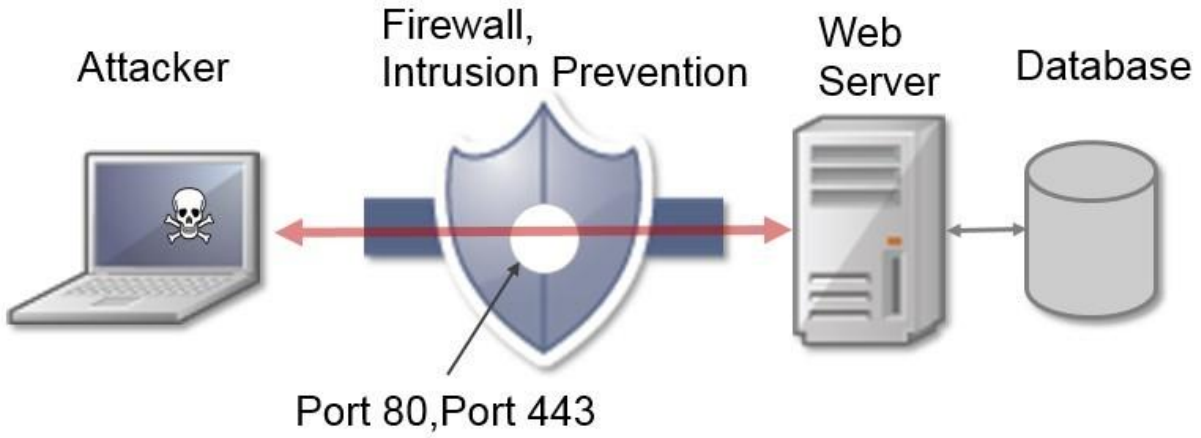


Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

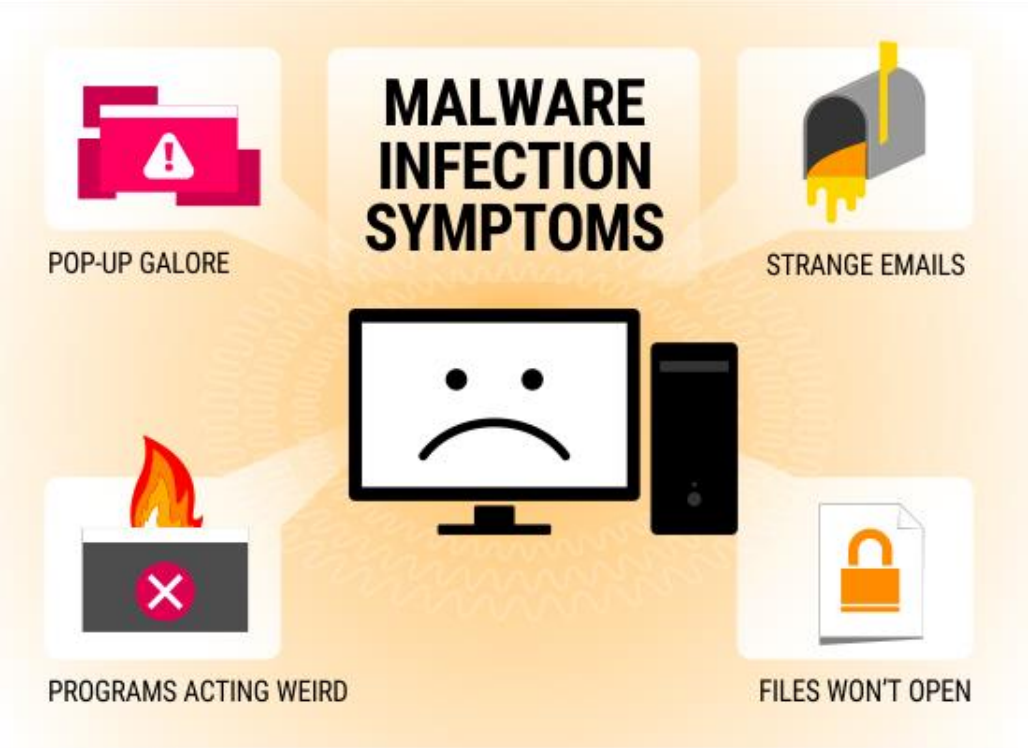


Ciberseguridad en sistemas de control industrial

Los desafíos de la ciberseguridad

Common Threats in Operational Technology

- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Policies and Procedures
- Lack of Network Segmentation
- DDoS Attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation



XI Jornadas Técnicas ABB en Chile

Medidas base de seguridad para un ICS

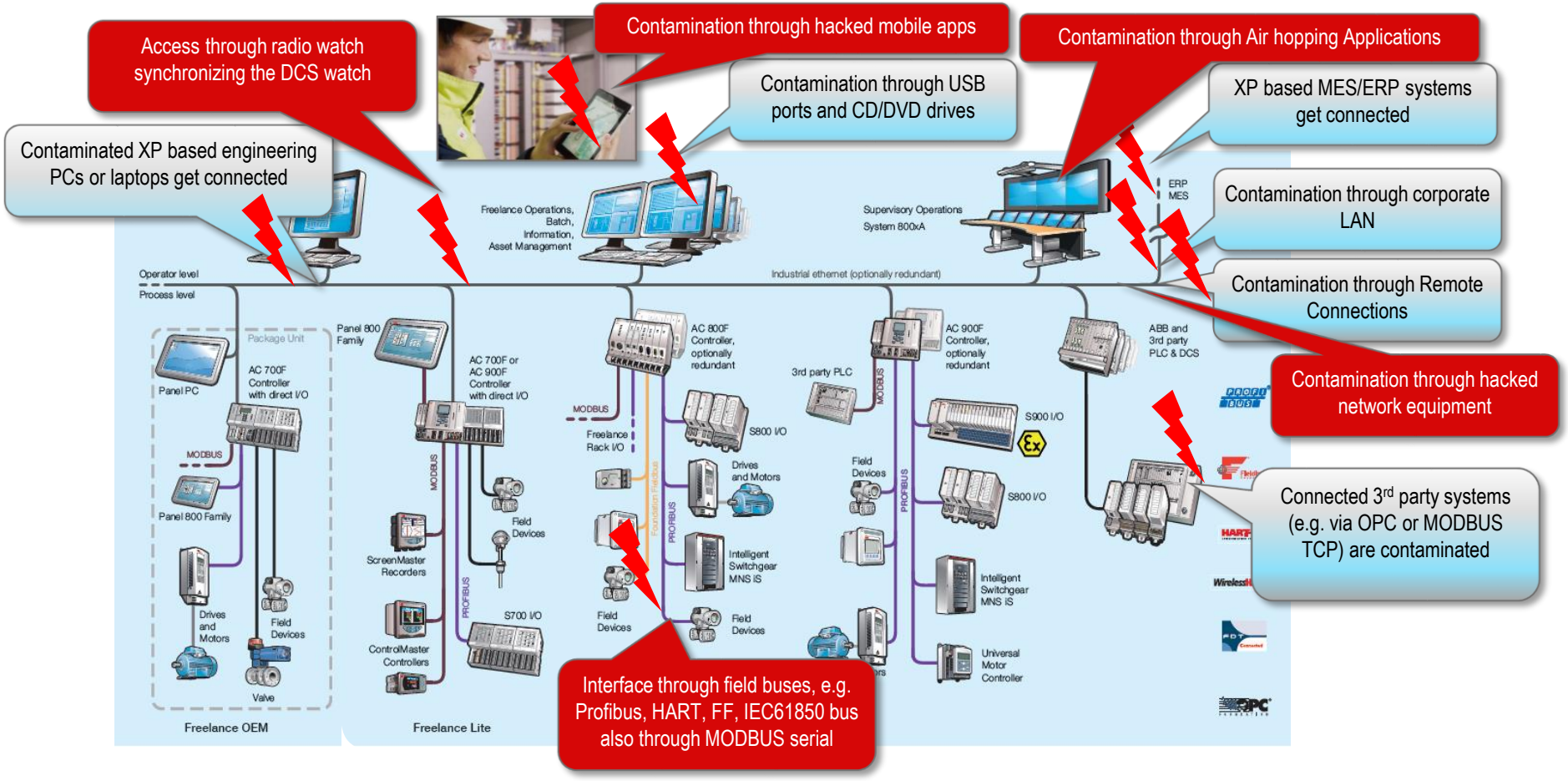
Ciberseguridad en sistemas de control industrial

Medidas base de seguridad para un ICS

	Traditional IT	Industrial IOT
What is being Protected	Data	Physical Process
Impact Area	Disclosure of information; Financial Loss	Safety, Availability, Financial, Environment
Security Objective	Confidentiality, Privacy	Availability, Integrity
Operating Systems	Windows, Linux, …	Windows at HMI, RTOS at field devices
Availability Requirements	99%	99.9% - 99.999% (downtime per year: 8.76 hours to 5.26 min)
System Lifetime	3 – 10 Years	5 – 25 Years
Logging and Forensics	Standard practice	Limited
Patching	Standard schedule; can be expedited	Non-standard; could be a long time between updates

Ciberseguridad en sistemas de control industrial

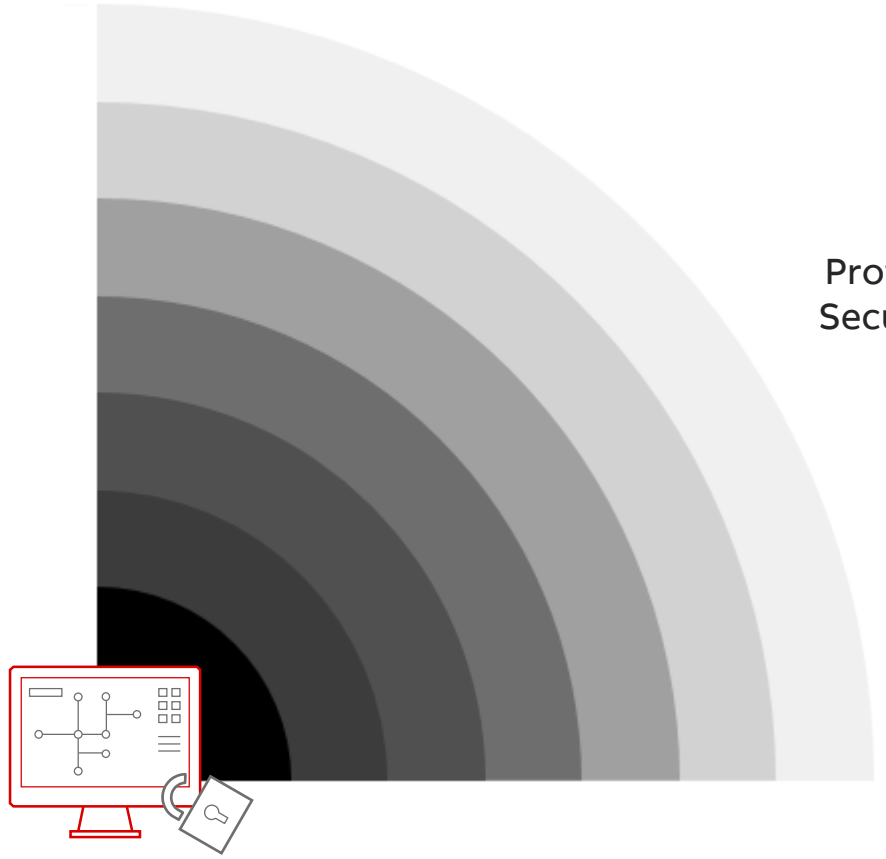
Medidas base de seguridad para un ICS



Ciberseguridad en sistemas de control industrial

Medidas base de seguridad para un ICS

- Physical Security
- Procedures and Policies
- Microsoft Firewall
- Computer Policies
- Account Management
- Security Updates
- Antivirus Solutions



Protect Against
Security Threats

Control System

Ciberseguridad en sistemas de control industrial

Medidas base de seguridad para un ICS

- Network Segmentation
- Logging
- Backups of critical software installers including a SHA256 digital hash
- Securely stored backups of project files and device configuration files with appropriate digital hashes
- Test and apply patches when operations schedules allow, prioritize based on greatest impact
- Limit remote connections
- Limit access privileges required
- Two form authentication on remote connections
- Identify communication protocols in use, ensure legacy protocol support, eliminate unused protocols

Ciberseguridad en sistemas de control industrial

Medidas base de seguridad para un ICS

- Application Whitelisting
- DMZ
- Central logging and data aggregation
- Endpoint security technologies
- Intrusion detection systems

Ciberseguridad en sistemas de control industrial

Medidas base de seguridad para un ICS

- Train defenders to hunt for odd communications patterns (new IP comms, abnormal ICS protocol communications)
- At network traffic choke points, ensure network captures are collected, baselined and analysed to identify anomalous communications. Monitor all outbound.
- Network security monitoring.
- Plan and train incident response for IT/OT personnel, gather forensic evidence while restoring operations.
- On detection of suspicious activity, disable all unnecessary remote access connections.
- Backup and recovery tools.

XI Jornadas Técnicas ABB en Chile

Servicios digitales de ABB

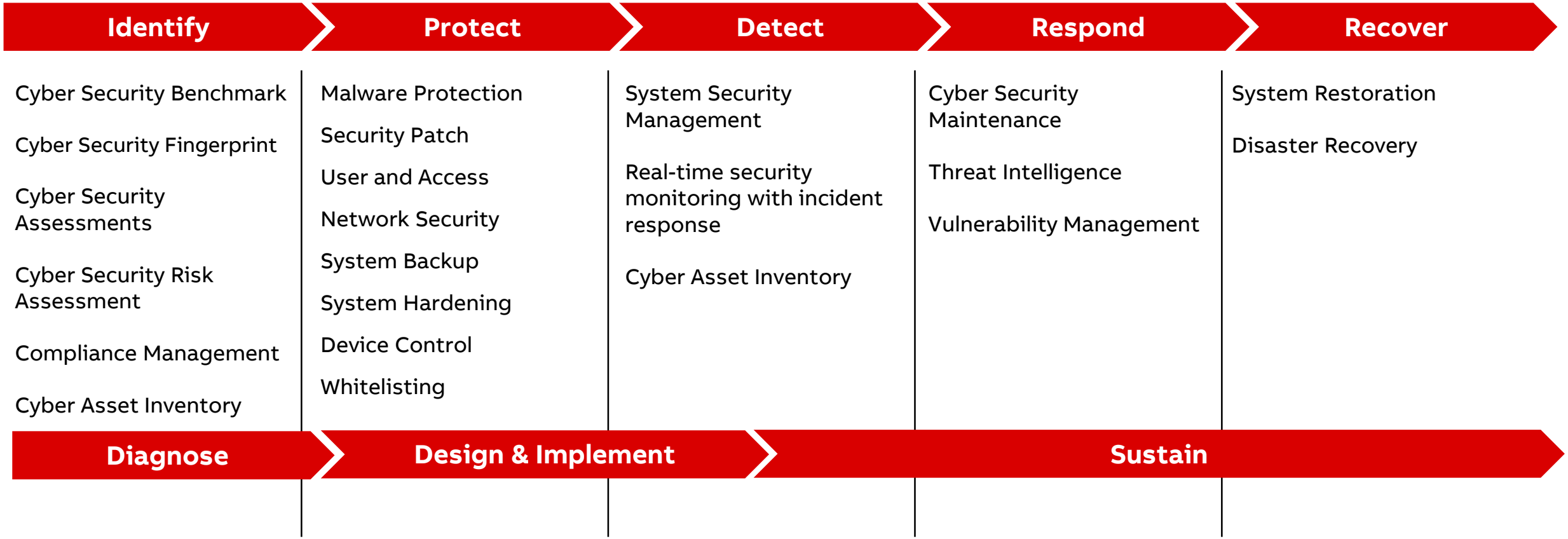
Ciberseguridad en sistemas de control industrial

Servicios digitales de ABB

Identify	Protect	Detect	Respond	Recover
Know where to fix	**Know how and what to fix**	**Ability to detect**	**Ability to help**	**Ability to restoration**
First identifying what needs to be protected	**Implement solutions for protection**	**Monitor to notify breaches and vulnerabilities**	**Respond to help if compromised**	**Proper backup and recovery**
Perform Benchmarks, Fingerprints or assessments	Our cyber security service portfolio protects your system from intrusion	Continuous security monitoring to predict unwanted Incidents	We can offer on demand incident response	Ensures that you have a maintained backup system with recovery features

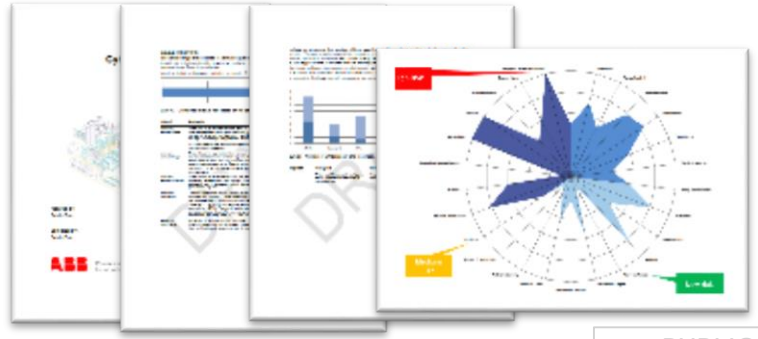
Ciberseguridad en sistemas de control industrial

Servicios digitales de ABB



Cyber Security Fingerprint

Diagnose



Overview

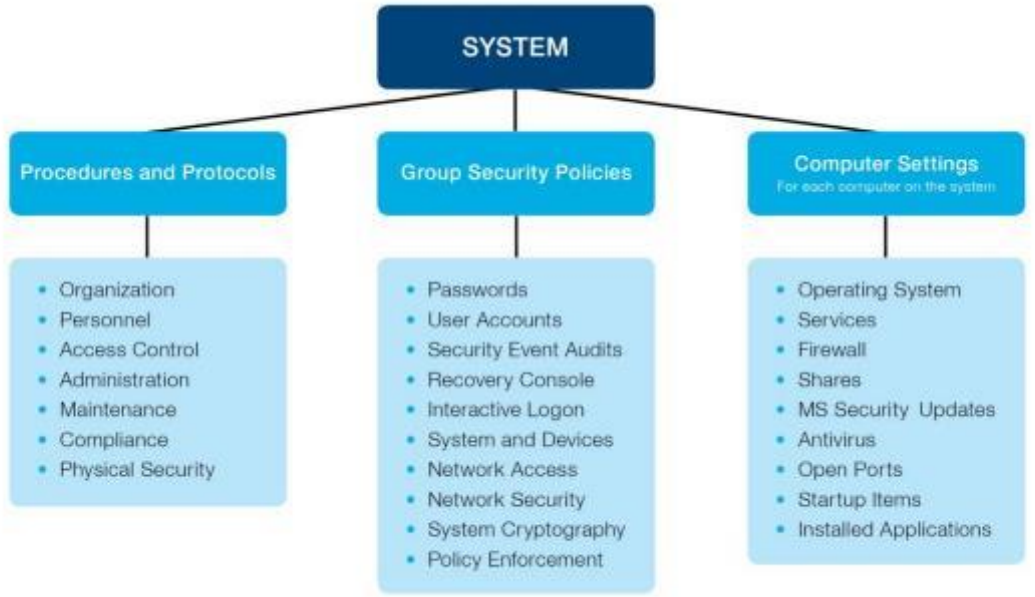
Provides a comprehensive view of your site's control systems cyber security status based on predefined KPI's for procedures and protocols, Group security policies and computer settings.

Identifies strengths and weaknesses for defending against an attack within your plant's control systems, both ABB and none-ABB systems.

The fingerprint is carried out by ABB.

The survey output is analyzed by ABB experts, who report the results and suggest improvements.

Supplies a solid foundation from which to build a sustainable cyber security strategy.

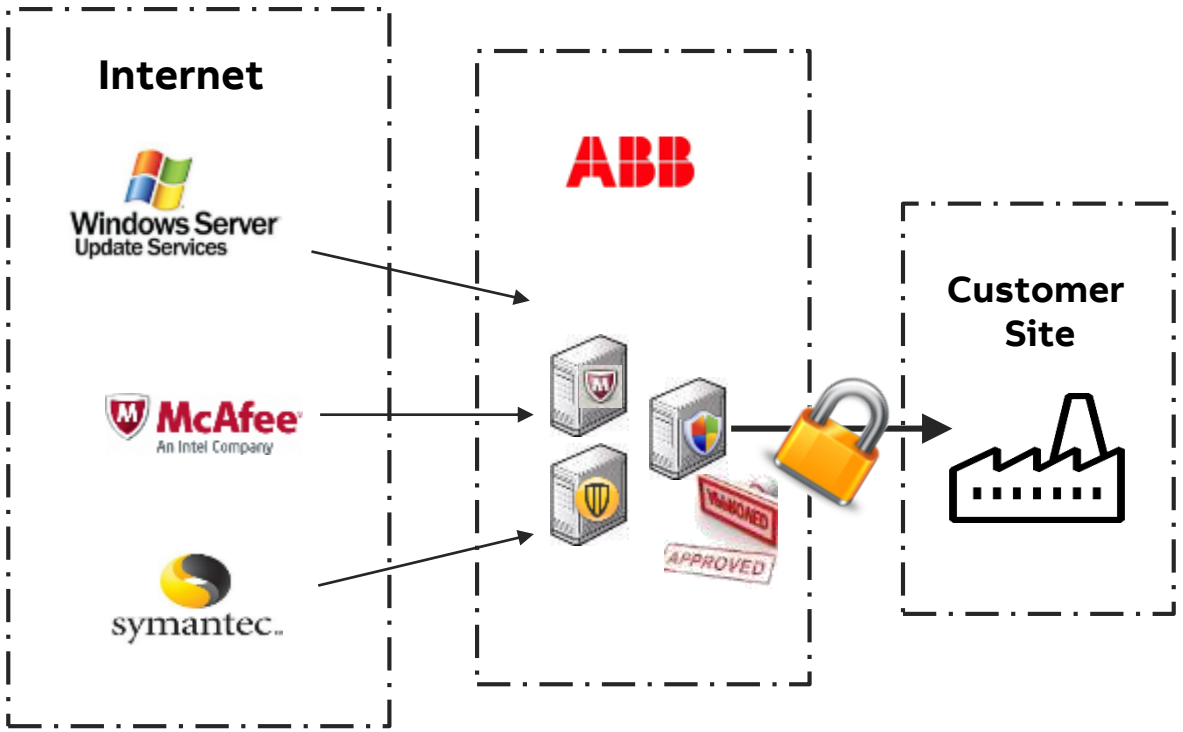


To get more information about our services please visit our web page on abb.com

Security Update and Antivirus

Protect

Security Update Process



Benefits

Should I patch my QCS systems? YES

Manual options through **My Control System (MCS)**

Centralize the solution - WSUS and ePO

Enhanced security against possible cyber threats and malware

Minimize delays of security updates after validation

– Systems are updated according to ABB's recommendation

Increased protection of investment and intellectual property

Fulfills Security regulation and insurances requirements

Increased productivity

– Highly automated process with minimized user efforts

– No error prone manual work

ABB Security Workplace

Ensure control system security without impact to safety, process or availability

Protect

Automates routine security maintenance tasks and provides operators with control and visibility into patch level, frequency of backups and key hardening measures.

Secure, backup and recover

- Offline patch management utility
- Identify missing and unqualified patches
- Antivirus, disaster recovery and whitelisting
- Configure and automates backup routines and schedules
- Details system hardening status and secured deployment
- Status monitoring dashboard prioritizes details for each node with stoplight color coded indicators
- Supports System 800xA and Symphony Plus

Scope of supply

- Management console automates deployment of patches that have been tested and validated for ABB control systems
- McAfee centrally managed endpoint protection against virus and spyware
- Installed by ABB cyber security experts
- Software maintenance updates during the subscription period

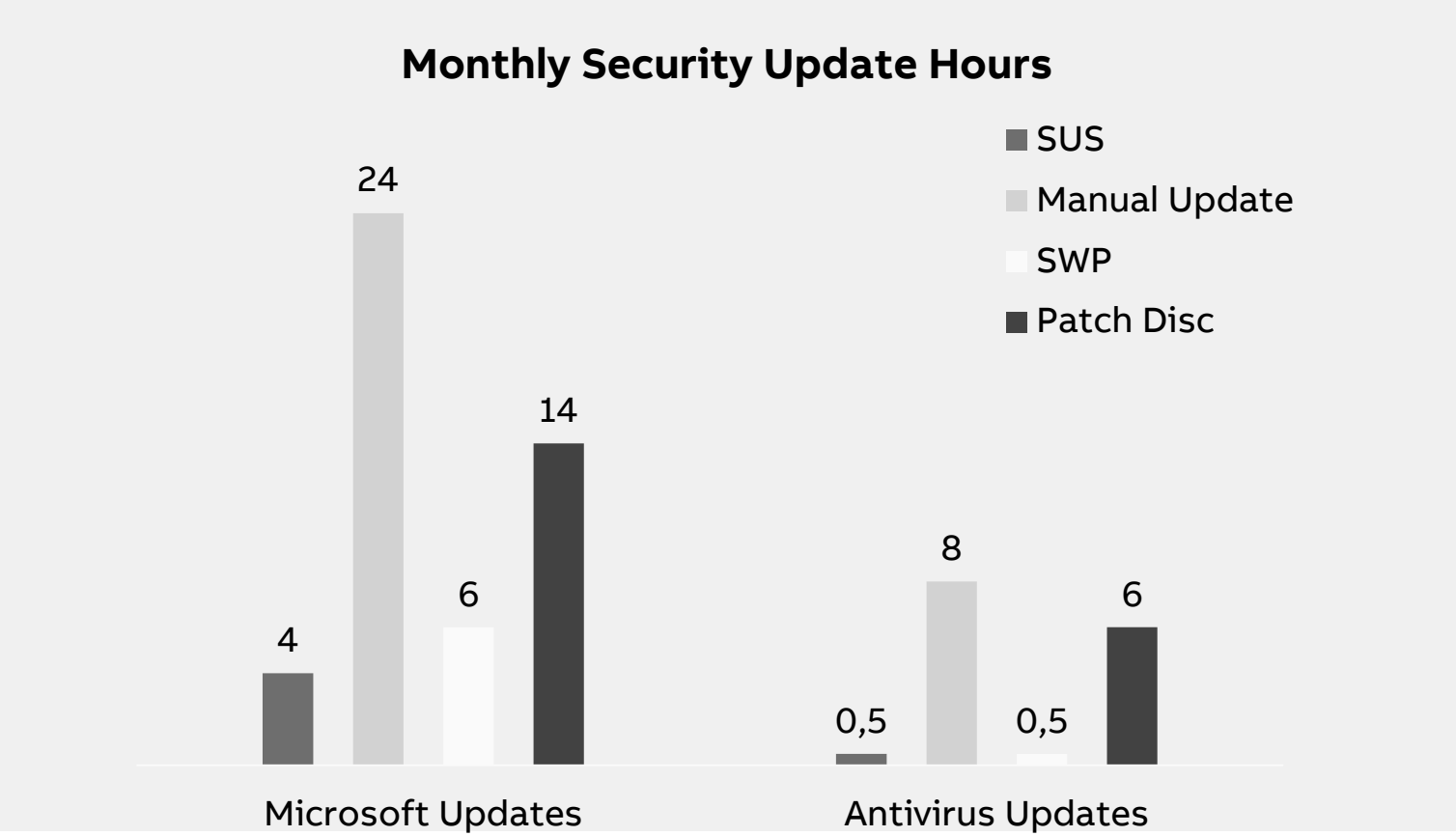
Requires current Automation Sentinel and ABB Ability Security Patch Management subscription

ABB Cyber Security

ABB Solutions vs Manual Updates

Average System Update Time

- Security Update Hours based on 10 servers and 12 clients
- Security Update Hours based on Patching on a monthly basis
- Antivirus Definitions updated monthly
  - SUS Daily



Backup and Recovery Management

Implement

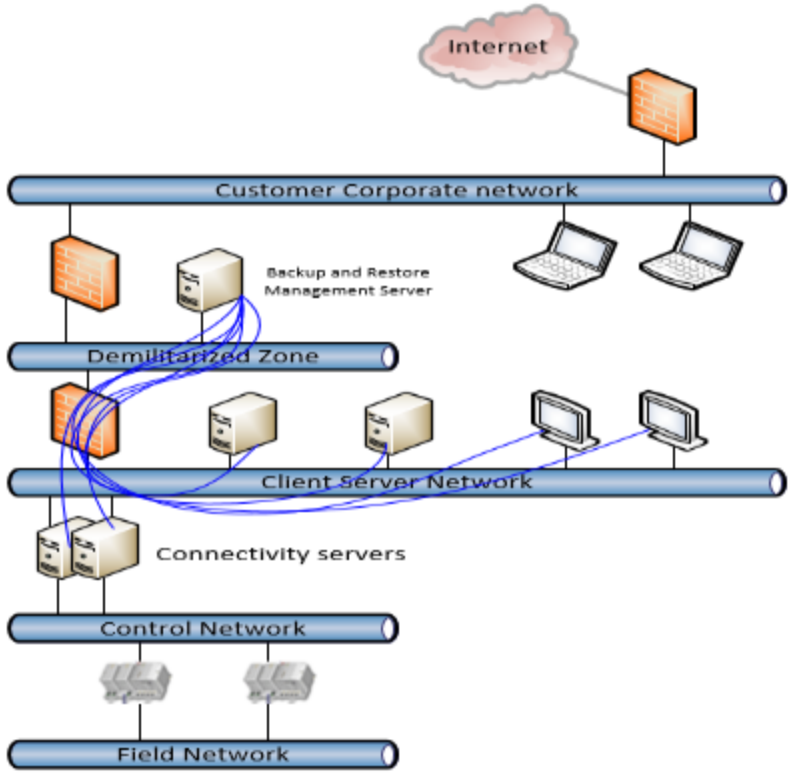
PUBLIC

Overview

If the worst does happen, and cyber-attack or natural disaster strikes, then ABB's backup and emergency response services enable a rapid recovery to normal operations.

This service includes implementation of management systems that handle backup and restore.

ABB's back-up solutions ensure the integrity, and availability, of critical data and the system, no matter what happens to the original.



To get more information about our services please visit our web page on abb.com

Device Control

Protect

PUBLIC

Overview

Utilizing an extension of the Centralized Antivirus Solution to prevent unauthorized use of removable media. As part of the McAfee ePolicy Orchestrator, Device Control offers event monitoring and incident management in real-time.

Device Control enables the customer to monitor and control data data transfers from all desktop and laptop machines, even when they are not connected to the network.

This service includes implementation and deployment of agents that handle removable media security.

ABB's Device Control solution ensures only approved removable media, have access to the system.

To get more information about our services please visit our web page on abb.com

Whitelisting and Application Control

Protect

Antivirus: Blacklisting	Application: Whitelisting
Block “known” malware	Allow known SW to run
Ongoing battle	Easier task

- Central Management and Distribution:
  - Application Certificates
  - Policies (Monitor/Block)
  - Log collection

- Premade Application Certificates for
  - Windows and other required 3rd party SW
  - ABB SW

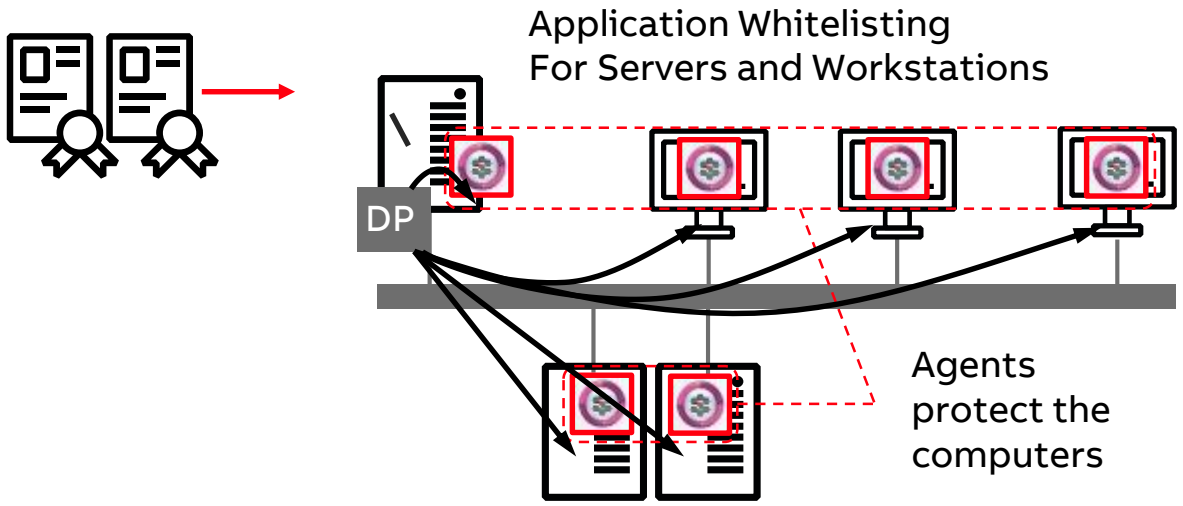
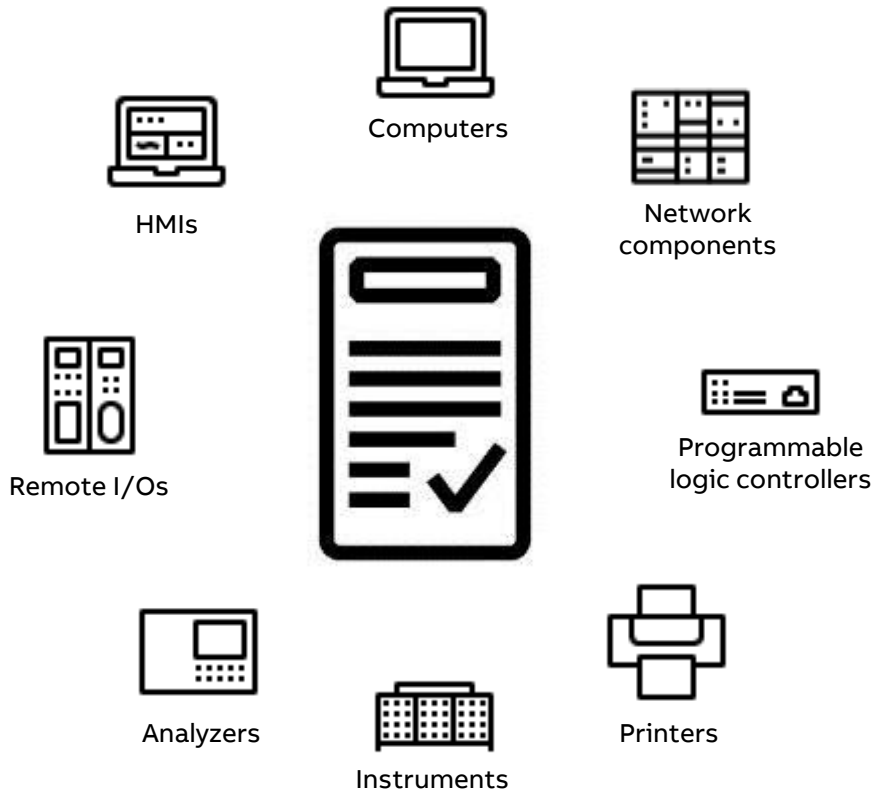


ABB Ability™ Cyber Security Asset Inventory

Detect

ABB Ability™ Cyber Security Asset Inventory uses technology that automatically identifies and captures information from cyber assets such as computers, network components, controllers, remote I/Os, instruments, analyzers, HMIs, printers and other assets connected to the control system network.

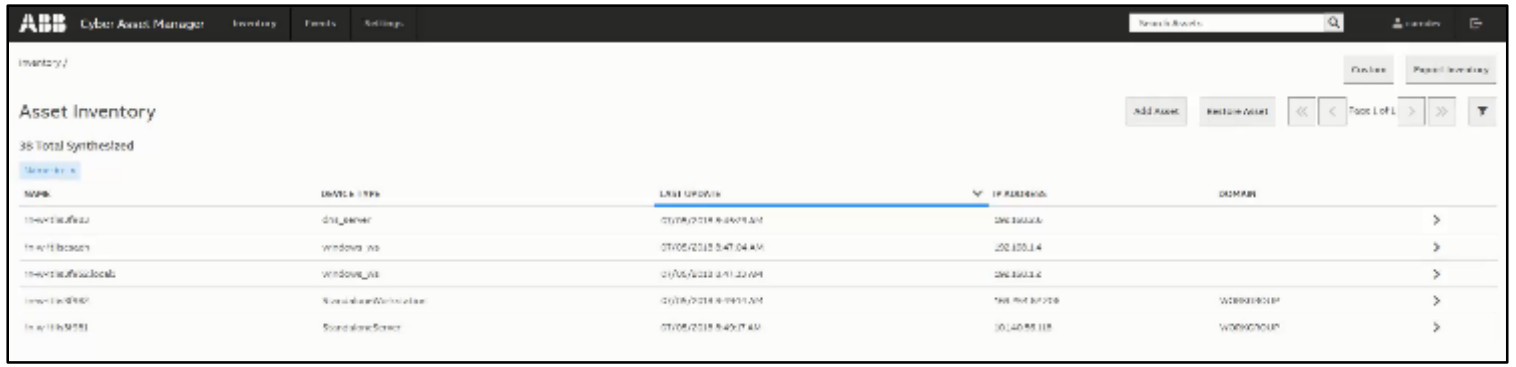
Cyber Asset Inventory provides up-to-date information on control networks, and can help in decision-making on issues of cyber security, asset lifecycle and asset management.

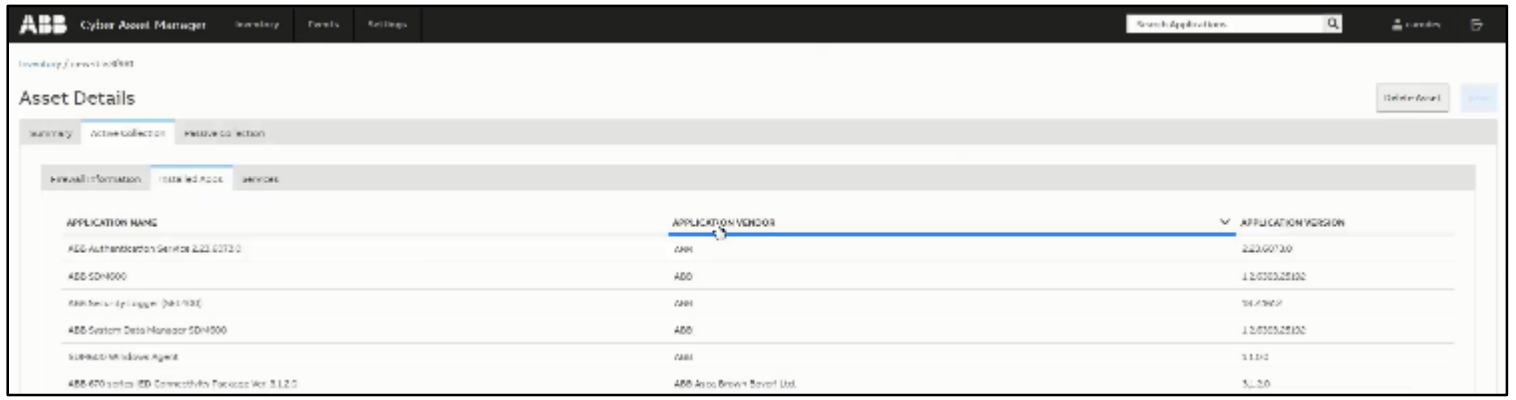


Cyber Security Asset Inventory provides a clear path to users

Web based User Interface

- ✓ Only authenticated users get access
- ✓ Data from network or devices are seamlessly displayed
- ✓ Users navigate data and go from over views details
- ✓ Views can be filtered and sorted.
- ✓ Search for a specific application* among all assets is possible
- ✓ Data can be exported and printed
- ✓ Event list that shows added, removed and updated assets is generated
- ✓ Connection to company email server to send notifications to users is possible





* example. Search works for all types of data

XI Jornadas Técnicas ABB en Chile

Conclusión

3 stages to protect digital systems

People process and technology: each must be leveraged to protect digital systems

People

- People are critical in preventing and protecting against cyber threats
- Organizations need competent people to implement and sustain cyber security technology and processes

Process

- Policies and procedures are key for an effective security strategy
- Processes should adapt to changes as cyber threats evolve

Technology

- Technology is important in preventing and mitigating cyber risks
- Technology needs people, processes and procedures to mitigate risks

Cyber Security

In closing

Final Thoughts

"The right people will choose the right tools, but untrained people will use tools incorrectly even when they are the right ones."

Robert M. Lee - 2016*

Questions

Contact

If you have further questions, please contact:

Ivan Granados

IAEN Cybersecurity Engineer
ivan.granados@cl.abb.com

Links to:

- Cyber Security on ABB.COM

* Robert M. Lee is CEO and Founder of Dragos and a SANS Certified Instructor. Former USAF Cyberwarfare Operations Officer.


ABB