Electricity 4.0

Our fastest route to Net Zero

An Introduction to IEC-62443

Schneider – Electric Cyber Solutions and Services

22/08/2024

What to do when the Threat = 1?

Presented By – Mr Victor Lough victor.lough@se.com

Your Speaker Today

30 + yrs in the OT Family

20 yrs in Cyber Security

NCSC CNI COI

Schneider Electric

Our differentiation

Ability to implement cybersecurity solutions across varying operating environments including energy management and industrial automation domains.

Vendor-agnostic solution capabilities

Understand & apply IT cybersecurity solutions within OT context and perspective

Flexible security solutions to ensure maximum value and efficiency

Customised controls based on customers' requirements

Deep understanding of OT priorities and concerns

Cyber Security What is it?

Assess

Act

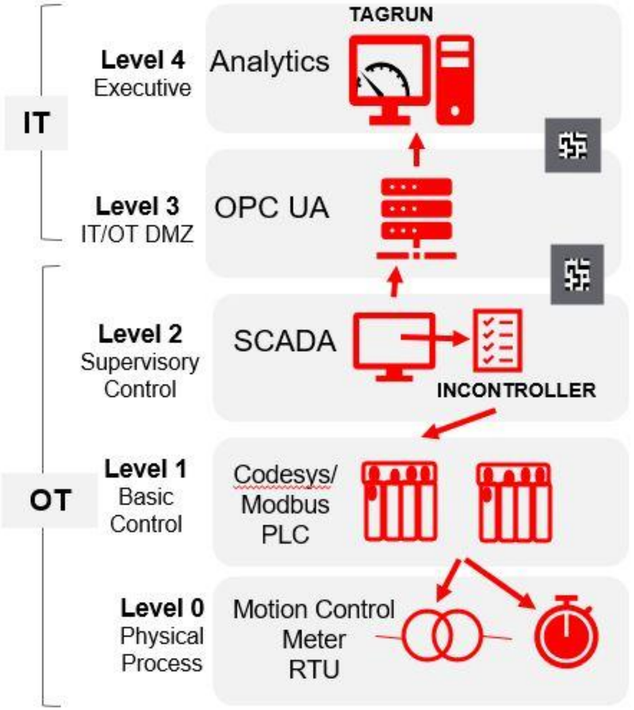
Manage

- The collection of **PEOPLE, PROCESSES, TECHNOLOGY AND PREPAREDNESS** that can be used to sustain the user, the organization, its assets, the cyber environment and the wider public.

Re-purposed from ONR Office for Nuclear Regulation Security statement

Failure is a Process not an event.....

The hostile actor has moved from Bespoke (Stuxnet), to Saville Row (Triton) to ready to Wear



APT INCONTROLLER / PIPEDREAM PUBLISHED FLOW

Target

Spread

Effect

Compromise the Insider

Compromise the Network

Compromise the Asset

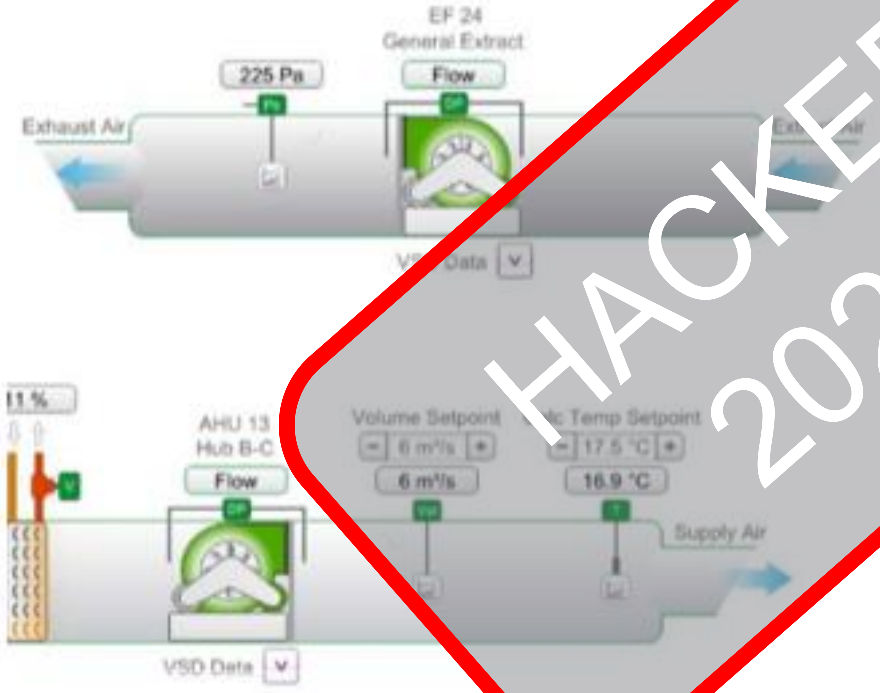
The Importance of Defence in Depth

A defensible hand lost through misunderstanding between partners.

“The Bottom Line is this: We do over 600 red teams a year. Firewalls never stopped one of them….In theory, it’s a solid thing, but it’s academic. In practice, it is operationally cumbersome-”.

Source – Senate Intelligence Committee hearing following on the so-called Solar Winds hack Quote from FireEye CEO Kevin Mandia

The importance of procurement.....



HACKED
2023

“The plant can be operated remotely … with site wide web access”.

“The BMS shall operate over the clients IT Network …”

“The web-browser access shall be totally robust and the possibility of remote 'Hacking' into the system shall be completely eliminated. ”

EU “Nearly Zero 20/10/31/ Directive

Why IEC 62443

World's only consensus-based standard automation and control system applications

Defines requirements and procedures for implementing electronically secure systems

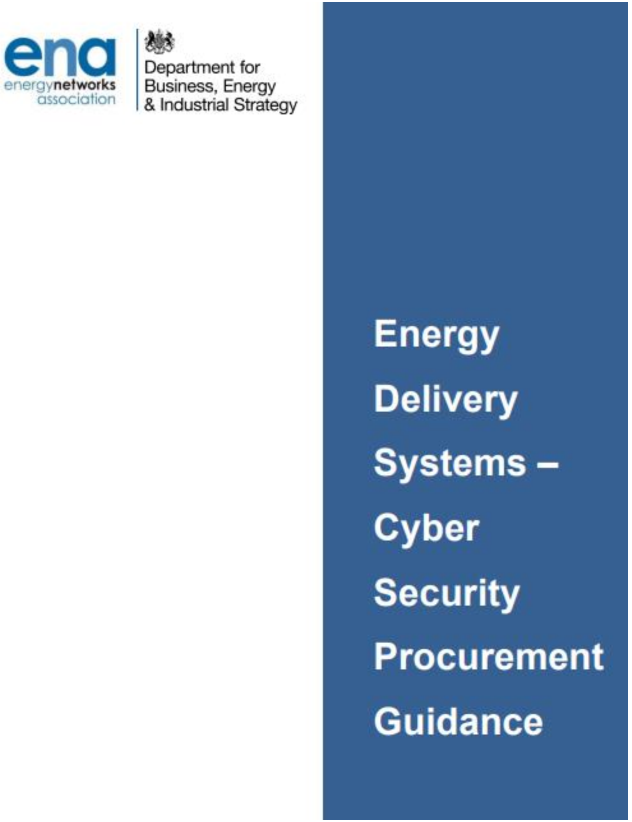
Leverage industry standards, increase productivity, lower costs & keep facilities safe

Flexible framework to address and mitigate current and future security vulnerabilities

Leverages a holistic approach, bridging the gap between operation and information technology, as well as between safety and cybersecurity

Information Source ISA GCA

ENA is a valuable Resource

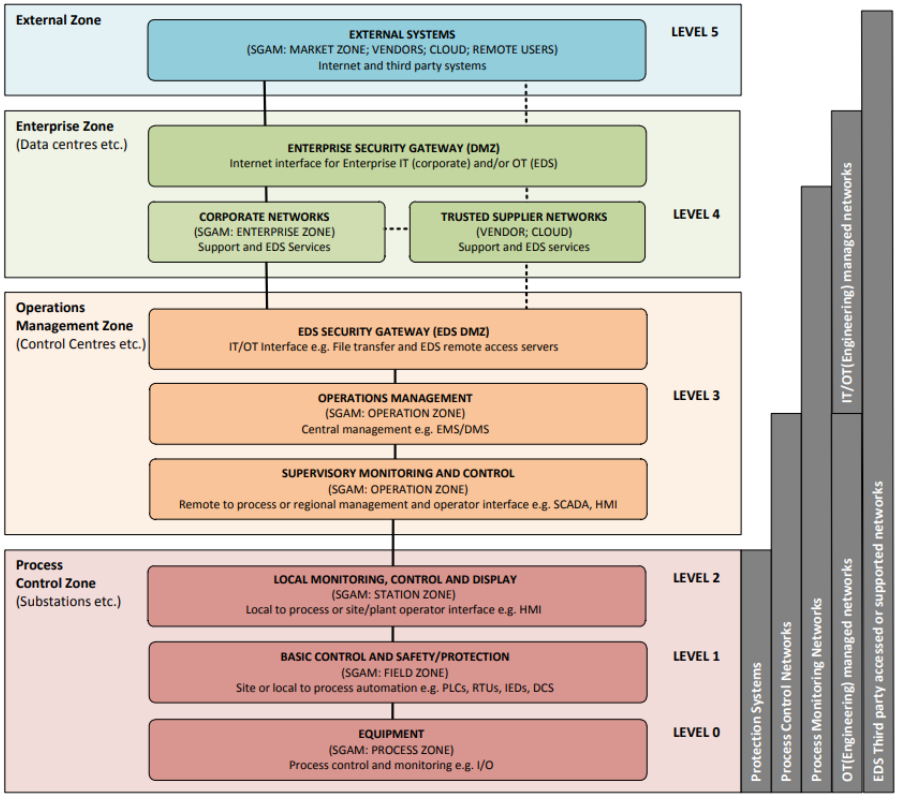


ena energynetworks association

Department for Business, Energy & Industrial Strategy

Energy Delivery Systems – Cyber Security Procurement Guidance

Figure 2 EDS Cyber Security Reference Model (EDS-CSRM)



External Zone

EXTERNAL SYSTEMS
(SGAM: MARKET ZONE; VENDORS; CLOUD; REMOTE USERS)
Internet and third party systems

LEVEL 5

Enterprise Zone
(Data centres etc.)

ENTERPRISE SECURITY GATEWAY (DMZ)
Internet interface for Enterprise IT (corporate) and/or OT (EDS)

CORPORATE NETWORKS
(SGAM: ENTERPRISE ZONE)
Support and EDS Services

TRUSTED SUPPLIER NETWORKS
(VENDOR; CLOUD)
Support and EDS services

LEVEL 4

Operations Management Zone
(Control Centres etc.)

EDS SECURITY GATEWAY (EDS DMZ)
IT/OT Interface e.g. File transfer and EDS remote access servers

OPERATIONS MANAGEMENT
(SGAM: OPERATION ZONE)
Central management e.g. EMS/DMS

LEVEL 3

SUPERVISORY MONITORING AND CONTROL
(SGAM: OPERATION ZONE)
Remote to process or regional management and operator interface e.g. SCADA, HMI

Process Control Zone
(Substations etc.)

LOCAL MONITORING, CONTROL AND DISPLAY
(SGAM: STATION ZONE)
Local to process or site/plant operator interface e.g. HMI

LEVEL 2

BASIC CONTROL AND SAFETY/PROTECTION
(SGAM: FIELD ZONE)
Site or local to process automation e.g. PLCs, RTUs, IEDs, DCS

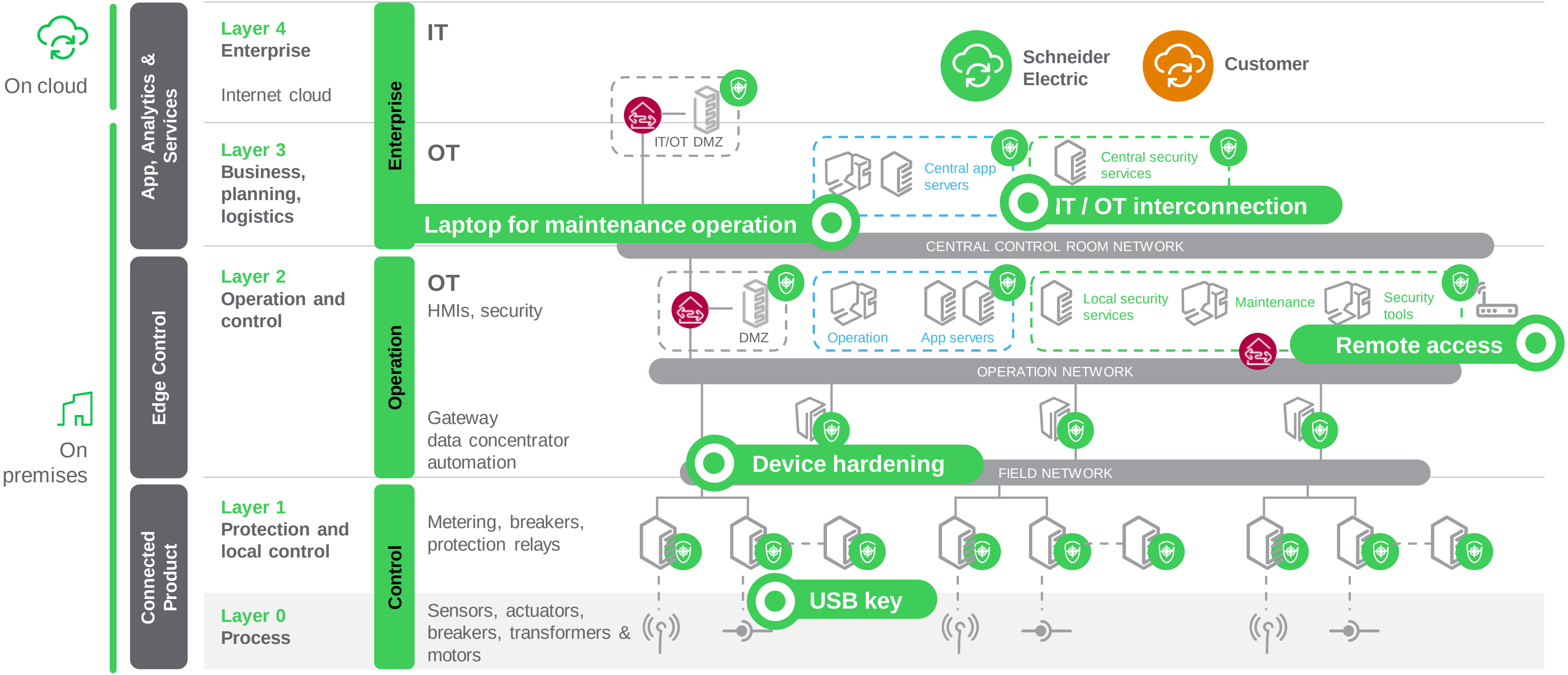
LEVEL 1

EQUIPMENT
(SGAM: PROCESS ZONE)
Process control and monitoring e.g. I/O

LEVEL 0

Protection Systems
Process Control Networks
Process Monitoring Networks
OT(Engineering) managed networks
IT/OT(Engineering) managed networks
EDS Third party accessed or supported networks

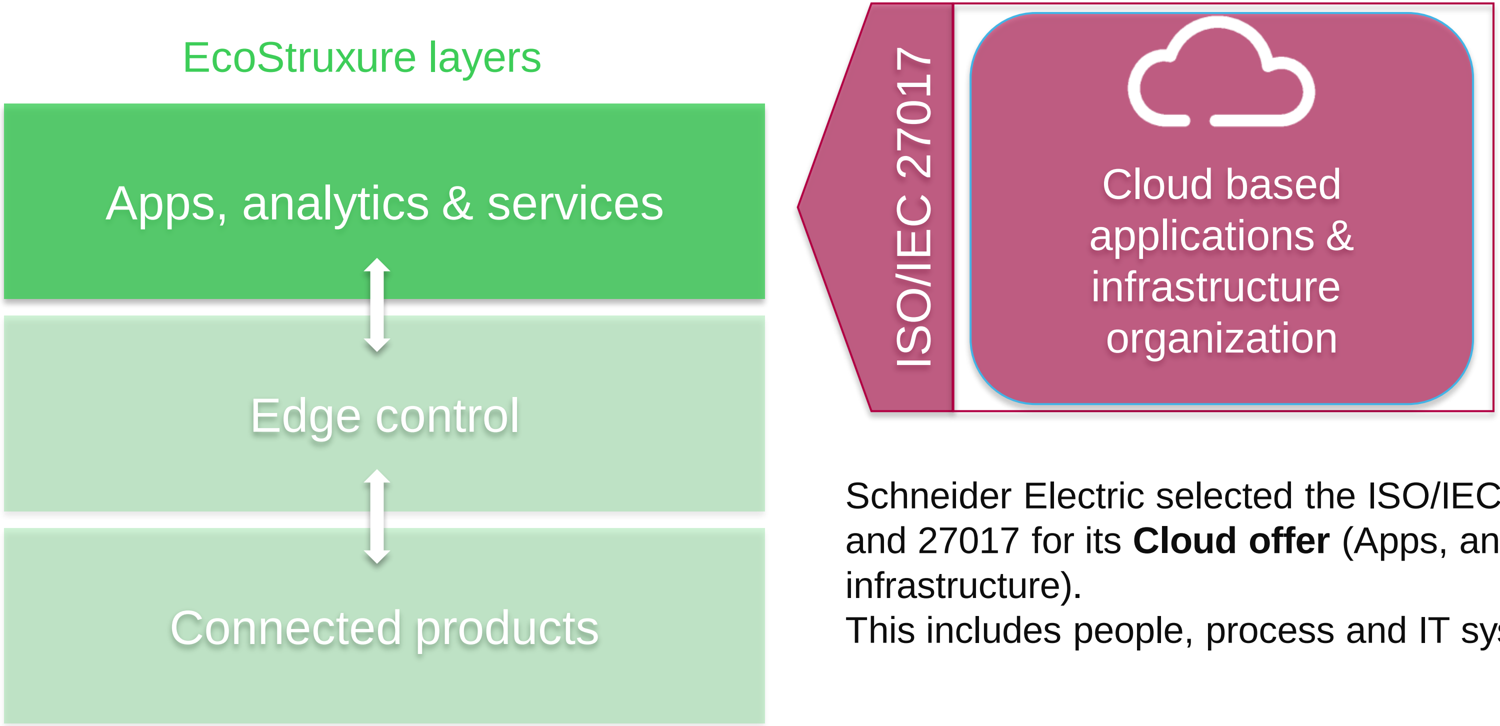
Major intrusion vectors with OT (risk points)



IT Cybersecurity Standards for the IT/Cloud

ISO/IEC 270xx

Information Security Management Systems


EcoStruxure layers
Apps, analytics & services
Edge control
Connected products
ISO/IEC 27017
Cloud based applications & infrastructure organization

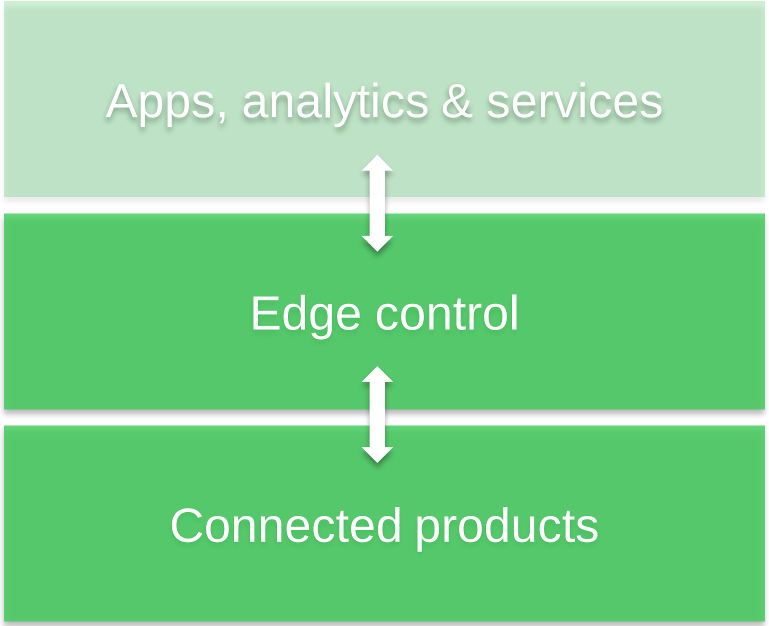
Schneider Electric selected the ISO/IEC 27001 and 27017 for its **Cloud offer** (Apps, analytics, infrastructure).
This includes people, process and IT systems

OT Cybersecurity Standards for Products and Solutions

IEC 62443 (formerly ISA99)

Security for industrial automation and control systems

EcoStruxure layers

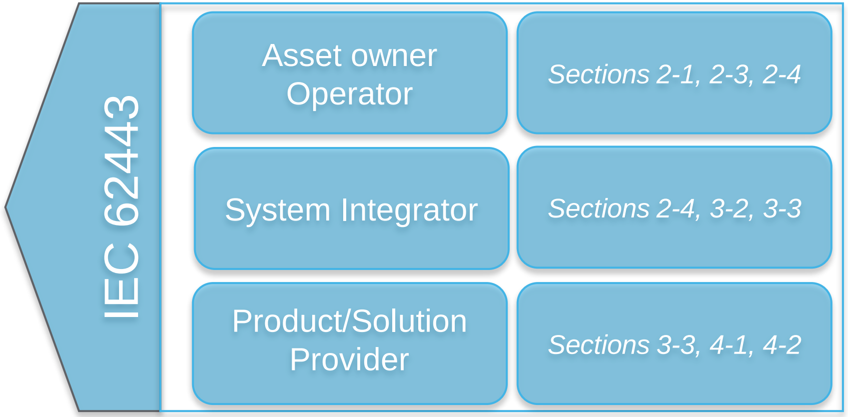


Apps, analytics & services

Edge control

Connected products

Schneider Electric selected the IEC 62443 as its core cybersecurity standard at **OT System and Product level**

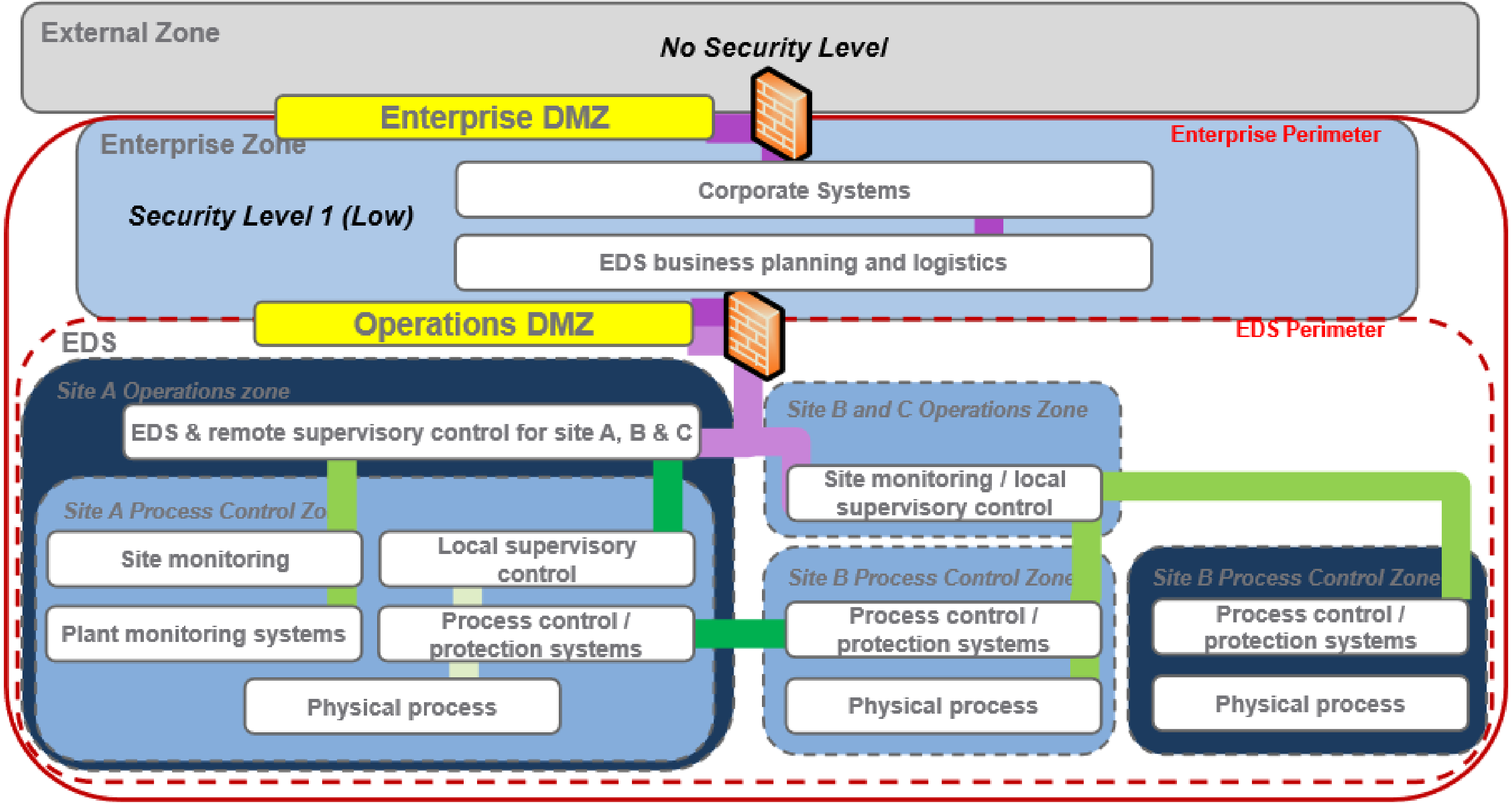


IEC 62443

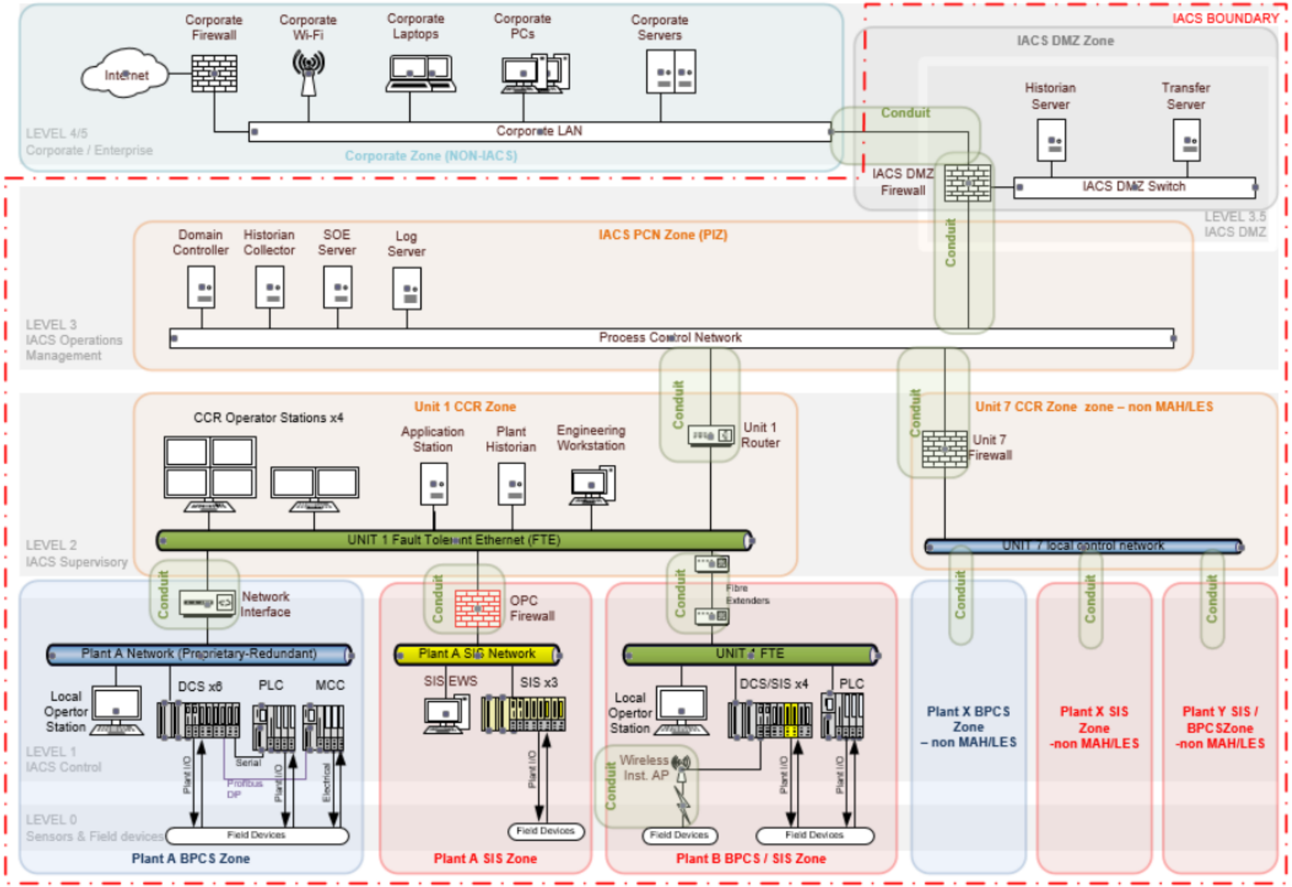
Asset owner Operator	*Sections 2-1, 2-3, 2-4*
System Integrator	*Sections 2-4, 3-2, 3-3*
Product/Solution Provider	*Sections 3-3, 4-1, 4-2*

Putting the O into OT .

Be Observant, Be Objective & Get Organised for Zones and Conduits


External Zone
No Security Level
Enterprise DMZ
Enterprise Zone
Enterprise Perimeter
Security Level 1 (Low)
Corporate Systems
EDS business planning and logistics
Operations DMZ
EDS
EDS Perimeter
Site A Operations zone
EDS & remote supervisory control for site A, B & C
Site A Process Control Zo
Site monitoring
Local supervisory control
Plant monitoring systems
Process control / protection systems
Physical process
Site B and C Operations Zone
Site monitoring / local supervisory control
Site B Process Control Zone
Process control / protection systems
Physical process
Site B Process Control Zone
Process control / protection systems
Physical process

OG 86 is a valuable Resource



IEC 62443 Foundational Requirement Categories

These seven FRs are the foundation for system (and components) capability security levels

FR 1 - IAC Identification and Authentication Control	FR 2 - UC Use Control	FR 3 - SI System Integrity	FR 4 - DC Data Confidentiality	FR 5 - RDF Restricted Data Flow	FR 6 - TRE Timely Response to Events	FR 7 - RA Resource Availability
Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the system	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the system and monitor the use of these privileges	Ensure the integrity of the system to prevent unauthorized manipulation	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Segment the control system via zones and conduits to limit the unnecessary flow of data	Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered	Ensure the availability of the system against the degradation or denial of essential services

FR1: Identification and authentication control (IAC)

Identify and authenticate all users (humans, software processes and devices), and allow them access to the system or assets.

Base Requirement		Extensions	
CR 1.1	🟩 Human Identification and Authentication	🟦 Unique Identification and authentication	🟥 Multifactor authentication for all interfaces
CR 1.2	🟦 Software process and device identification and authentication	🟧 Software Unique identification and authentication	
CR 1.3	🟩 Account Management		
CR 1.4	🟩 Identifier Management		
CR 1.5	🟩 Authenticator Management	🟧 Hardware Security for authenticators	
CR 1.6 *	🟩 Wireless access management	🟧 Explicit access request approval	
CR 1.7	🟩 Strength of password-based authentication	🟧 Password generation and lifetime restrictions for human users	🟥 Password lifetime restrictions for all users (human, software process or device)

🟩 SL1 🟦 SL2 🟧 SL3 🟥 SL4

* Applies to Network Devices only

FR1: Identification and authentication control (IAC)

Identify and authenticate all users (humans, software processes and devices), and allow them access to the system or assets.

Base Requirement		Extensions
CR 1.8	🟦 Public Key Infrastructure certificates (PKI)	
CR 1.9	🟦 Strength of public key-based authentication	🟧 Hardware security for public key-based authentication
CR 1.10	🟩 Authenticator feedback	
CR 1.11	🟩 Unsuccessful Login attempts	
CR 1.12	🟩 System Use Notification	
CR 1.13 *	🟩 Access via untrusted networks	🟧 Explicit access request approval
CR 1.14	🟦 Strength of symmetric key-based authentication	🟧 Hardware security for public key-based authentication

🟩 SL1 🟦 SL2 🟧 SL3 🟥 SL4

* Applies to Network Devices only

FR2: Use control (UC)

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

Base Requirement		Extensions			
CR 2.1	🟩 Authorization Enforcement	🟦 Authorization enforcement for all users	🟦 Permission mapping to roles	🟧 Supervisor override	🟥 Dual approval
CR 2.2	🟩 Wireless use control				
CR 2.3	🟩 Use control for portable and mobile devices				
CR 2.4 *	🟩 Mobile code	🟧 Mobile code integrity check			
CR 2.5	🟩 Session Lock				
CR 2.6	🟦 Remote session termination				
CR 2.7	🟧 Concurrent session control				

🟩 SL1 🟦 SL2 🟧 SL3 🟥 SL4

* Extension applies to software applications and embedded devices only

FR2: Use control (UC)

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

Base Requirement		Extensions	
CR 2.8	Auditable events		
CR 2.9	Audit storage capacity	Warn when audit record storage capacity threshold reached	
CR 2.10	Response to audit processing failures		
CR 2.11	Timestamps	Time synchronization	Protection of time source integrity
CR 2.12	Non-repudiation	Non-repudiation for all users	
CR 2.13 *	Use of physical diagnostic and test interfaces	Active monitoring	

SL1 SL2 SL3 SL4

* Applies to host devices, network devices and embedded devices only

Internal

FR3: System integrity (SI)

Ensure the integrity of the component to prevent unauthorized manipulation.

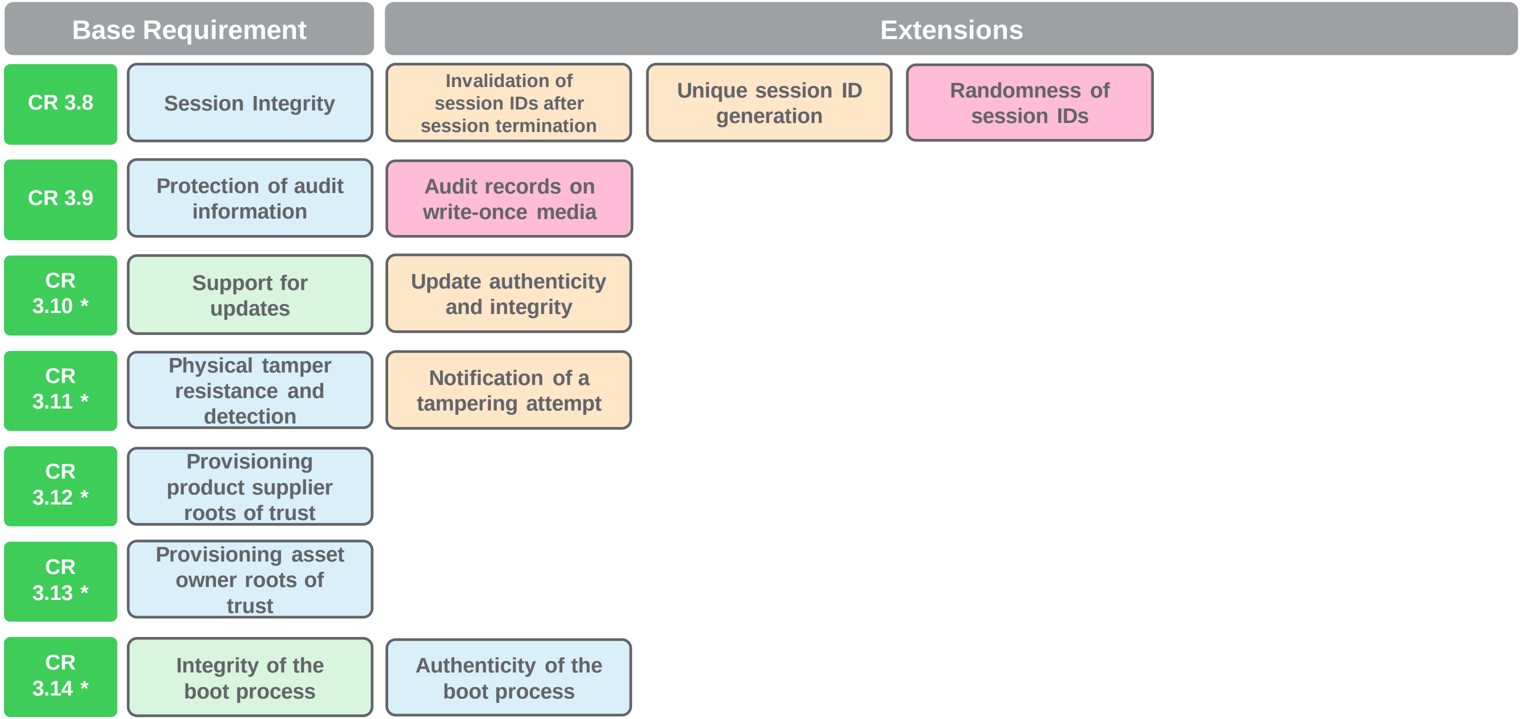
Base Requirement		Extensions	
CR 3.1	Communication Integrity	Communication authentication / Cryptographic integrity protection	
CR 3.2 *	Protection from malicious code	Report version of code protection	
CR 3.3	Security Functionality Verification	Security functionality verification during normal operation	
CR 3.4	Software & Information Integrity	Authenticity of software and information	Automated notification of integrity violations
CR 3.5	Input Validation		
CR 2.6	Deterministic output		
CR 3.7	Error Handling		

SL1 SL2 SL3 SL4

* Extension applies to host devices only.

FR3: System integrity (SI)

Ensure the integrity of the component to prevent unauthorized manipulation.



Base Requirement		Extensions		
CR 3.8	Session Integrity	Invalidation of session IDs after session termination	Unique session ID generation	Randomness of session IDs
CR 3.9	Protection of audit information	Audit records on write-once media		
CR 3.10 *	Support for updates	Update authenticity and integrity		
CR 3.11 *	Physical tamper resistance and detection	Notification of a tampering attempt		
CR 3.12 *	Provisioning product supplier roots of trust			
CR 3.13 *	Provisioning asset owner roots of trust			
CR 3.14 *	Integrity of the boot process	Authenticity of the boot process		

SL1 SL2 SL3 SL4

* Applies to embedded devices, host devices and network devices only.

Internal

FR4: Data confidentiality (DC)

Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

Base Requirement		Extensions	
CR 4.1	Information Confidentiality		
CR 4.2	Information Persistence	Erase of shared memory resources	Erase verification
CR 4.3	Use of Cryptography		

SL1 SL2 SL3 SL4

FR5: Restricted data flow (RDF)

Segment the control system via zones and conduits to limit the unnecessary flow of data

Base Requirement		Extensions		
CR 5.1	Network Segmentation			
CR 5.2 *	Zone boundary protection	Deny all, permit by exception	Island mode	Fail close
CR 5.3 *	General purpose, person-to-person communications restrictions			

SL1 SL2 SL3 SL4

* Applies to network devices only.

FR6: Timely response to events (TRE)

Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

Base Requirement		Extensions
CR 6.1	Audit Log accessibility	Programmatic access to audit logs
CR 6.2	Continuous monitoring	

SL1 SL2 SL3 SL4

FR7: Resource Availability (RA)

Ensure the availability of the application or device against the degradation or denial of essential services.

Base Requirement		Extensions	
CR 7.1	🟩 Denial of Service Protection	🟦 Manage communication load from component	
CR 7.2	🟩 Resource Management		
CR 7.3	🟩 Control system backup	🟦 Backup integrity verification	🟧 Local backup
CR 7.4	🟩 Control system recovery and reconstitution		
CR 7.6	🟩 Manage network and security configuration settings	🟧 Machine-readable reporting of current security settings	
CR 7.7	🟩 Least functionality		
CR 7.8	🟦 Control system component inventory		

🟩 SL1 🟦 SL2 🟧 SL3 🟥 SL4

* CR 7.5: Emergency Power removed from standard.

IEC62443-4-2 - Fundamental Requirements (FR) – SL1

FR	FR 1 - IAC Identification and Authentication Control	FR 2 - UC Use Control	FR 3 - SI System Integrity	FR 4 - DC Data Confidentiality	FR 5 - RDF Restricted Data Flow	FR 6 - TRE Timely Response to Events	FR 7 - RA Resource Availability
Features	Human Identification and Authentication	Authorization Enforcement	Communication Integrity	Information Confidentiality	Network Segmentation	Audit Log accessibility	Denial of Service Protection
	Account Management	Wireless use control	Macilious code protection	Use of Cryptography			Resource Management
	Identifier Management	Use control for portable and mobile devices	Security Functionality Verification				Control system backup
	Authenticator Management	Mobile code	Support for updates				Control system recovery and reconstitution
	Password-based authentication	Session Lock	Input Validation				Least functionality
	Authenticator feedback	Auditable events	Deterministic output				Control system component inventory
	Unsuccessful Login attempts	Timestamps	Error Handling				Manage network and security configuration settings
	System Use Notification	Audit storage capacity					
		Response to audit processing failures					

Internal

IEC62443-4-2 - Fundamental Requirements (FR) – SL2

FR	FR 1 - IAC Identification and Authentication Control	FR 2 - UC Use Control	FR 3 - SI System Integrity	FR 4 - DC Data Confidentiality	FR 5 - RDF Restricted Data Flow	FR 6 - TRE Timely Response to Events	FR 7 - RA Resource Availability
Features	Public Key Infrastructure certificates(PKI)	Use of physical diagnostic and test interfaces	Software & Information Integrity	Information Persistence		Continuous monitoring	Manage communication load from component
	Software process and device identification and authentication	Authorization enforcement for all users	Authenticity of software and information				Backup integrity verification
	Unique identification and authentication	Permission mapping to roles	Session Integrity				Control system component inventory
	Strength of public key-based authentication	Remote session termination	Physical tamper resistance and detection				
	Strength of symmetric key-based authentication		Protection of audit information				
			Provisioning product supplier/ Owner roots of trust				
			Authenticity of the boot process				

IEC62443-4-2 - Fundamental Requirements (FR) – SL3

FR

Features

FR 1 - IAC Identification and Authentication Control

- Hardware Security for authenticators
- Software Unique identification and authentication
- Password generation and lifetime restrictions for human users
- Hardware security for public key-based authentication
- Hardware security for symmetric key-based authentication

FR 2 - UC Use Control

- Supervisor override
- Mobile code integrity check
- Concurrent session control
- Warn when audit record storage capacity threshold reached
- Time synchronization
- Non-repudiation
- Non-repudiation of all user
- Active monitoring
- Invalidation of session IDs after session termination

FR 3 - SI System Integrity

- Update authenticity and integrity
- Notification of a tampering attempt
- Communication authentication / Cryptographic integrity protection
- Unique session ID generation
- Invalidation of session IDs after session termination

FR 4 - DC Data Confidentiality

- Erase verification
- Erase of shared memory resources

FR 5 - RDF Restricted Data Flow

FR 6 - TRE Timely Response to Events

- Programmatic access to audit logs

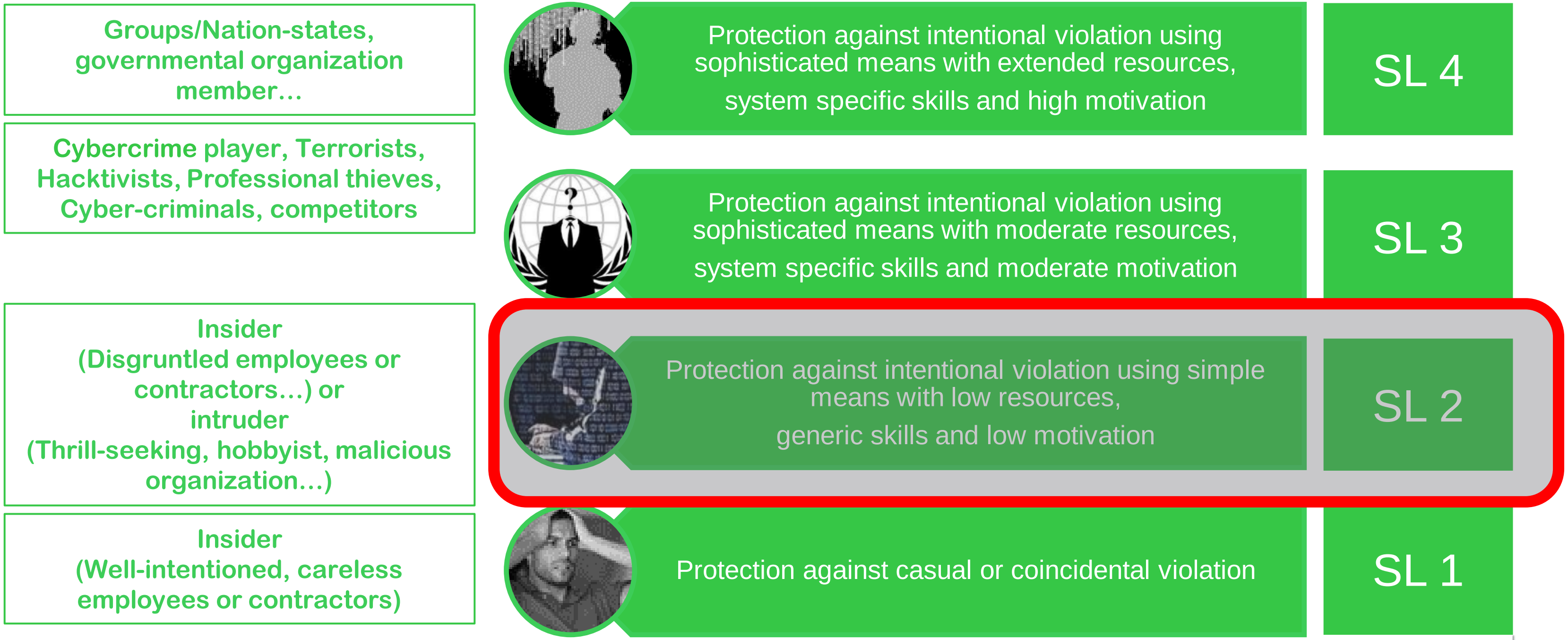
FR 7 - RA Resource Availability

- Local backup
- Machine-readable reporting of current security settings

L USE ONLY

Establish Content- IEC 62443

Security levels define the cybersecure functions embedded in OT Systems, it increase the deployed robustness and make it resistant to the Cyber threats.



Groups/Nation-states, governmental organization member…

Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

SL 4

Cybercrime player, Terrorists, Hacktivists, Professional thieves, Cyber-criminals, competitors

Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation

SL 3

Insider (Disgruntled employees or contractors…) or intruder (Thrill-seeking, hobbyist, malicious organization…)

Protection against intentional violation using simple means with low resources, generic skills and low motivation

SL 2

Insider (Well-intentioned, careless employees or contractors)

Protection against casual or coincidental violation

SL 1

Internal

Cybersecurity Gap Analysis in practice

FR 7 – Resource Availability

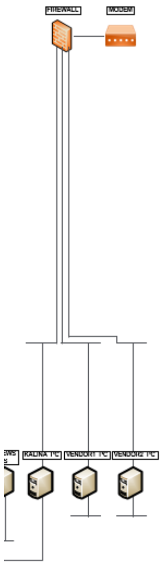
Major gaps identified / proposed approach

Gaps

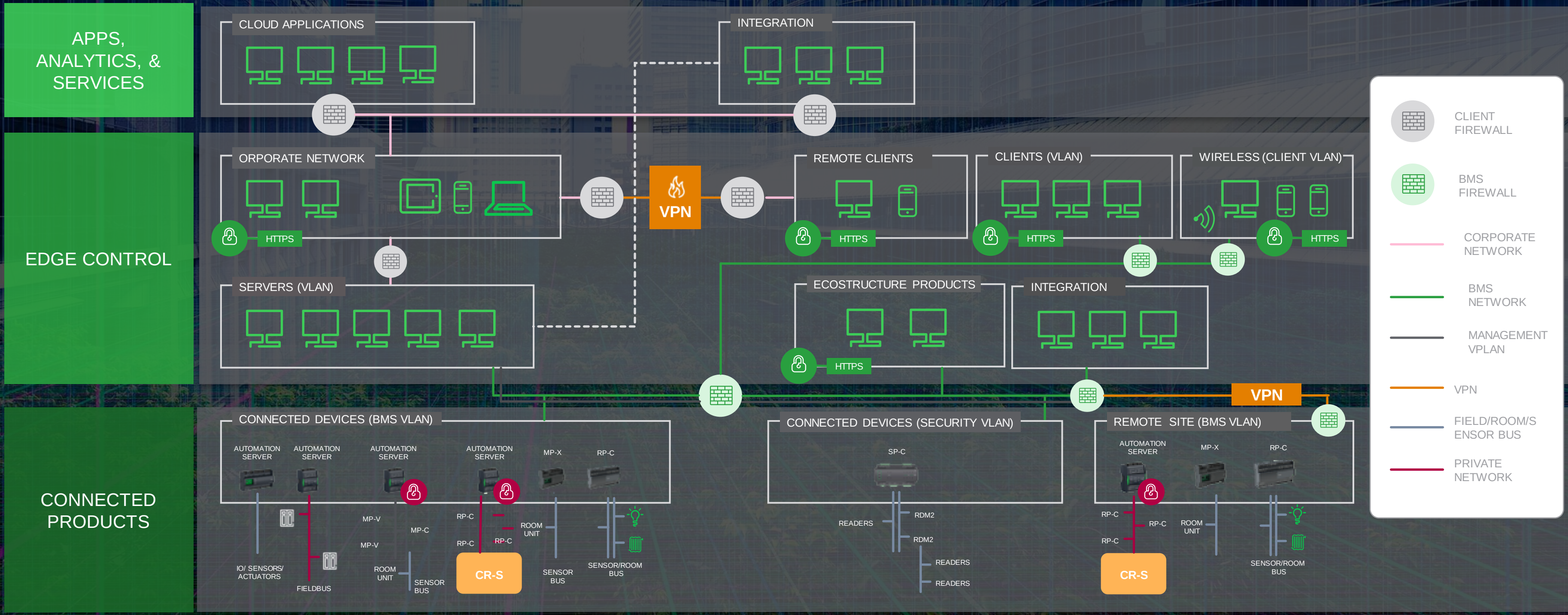
- Capability of system to operate in degraded mode in case of DoS attack can't be guaranteed
- Communications load management to mitigate DoS events consequences, not in place
- Mechanism to prevent resource exhaustion for security functions, not in place
- Backup/restore of legacy machines not effective
- Verification of backups reliability for legacy machines not possible
- Recovery after disruption or failure not guarenteed

Improvements

- Verify if all system components support protection against DoS attacks and replace them if needed
- Implement Network Performance Monitoring and traffic limiting setups across network devices
- Implement resource exhaustion protection i.e. for switch port mirroring and log storage
- Update all stations to latest approved MS OS and hardware specs; use only one sw solution (Veritas), perform verification of all backup images; execute restore tests on spare workstations/servers in stock; implement disaster recovery solution/service by SE



Schneider's cybersecurity approach for Buildings



In Summary

Est Content / Resilience Plan for OT

Exercise your Incident Response Plan

Harden your Network

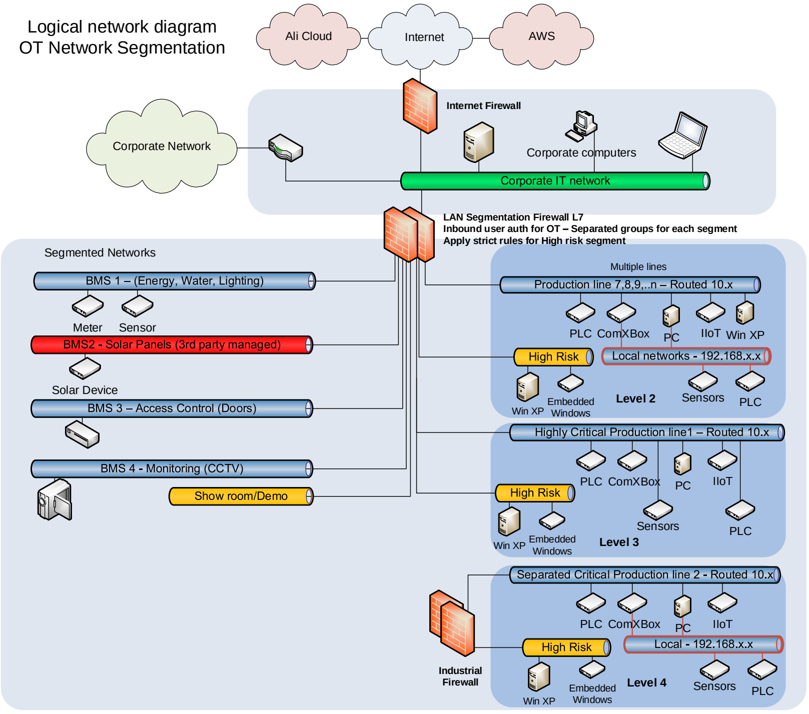
Create an “As-Operated” OT Network Map

Understand and Evaluate your “As-Operated” OT Cyber Risk

Implement a Continuous and Vigilant System Monitoring Program.

What some of our customers have to say ?

Logical network diagram
OT Network Segmentation


Ali Cloud
Internet
AWS
Internet Firewall
Corporate Network
Corporate computers
Corporate IT network
LAN Segmentation Firewall L7
Inbound user auth for OT – Separated groups for each segment
Apply strict rules for High risk segment
Segmented Networks
BMS 1 – (Energy, Water, Lighting)
Meter
Sensor
BMS2 - Solar Panels (3rd party managed)
Solar Device
BMS 3 – Access Control (Doors)
BMS 4 - Monitoring (CCTV)
Show room/Demo
Multiple lines
Production line 7,8,9,..n – Routed 10.x
PLC
ComXBox
PC
IIoT
Win XP
High Risk
Local networks - 192.168.x.x
Win XP
Embedded Windows
Level 2
Sensors
PLC
Highly Critical Production line1 – Routed 10.x
PLC
ComXBox
PC
IIoT
High Risk
Sensors
PLC
Win XP
Embedded Windows
Level 3
Separated Critical Production line 2 - Routed 10.x
PLC
ComXBox
PC
IIoT
High Risk
Local - 192.168.x.x
Industrial Firewall
Win XP
Embedded Windows
Level 4
Sensors
PLC

The SE Cyber security team did an exceptional job in **demystifying** the solution space and helping our many **IT & Instrument** system stakeholders, as well as our other instrument systems vendors quickly land on a **common** solution which **best fits** our business

David Taylor Principle Instrument Engineer

Internal

Laying the Right Cyber Pathway....

Protecting your 2492 Carat Crown Jewels

Impose Cost on the Adversary

Understand the Consequence

Enhance Business Resilience

Schneider - Electric Cyber Security Solutions & Services

Victor Lough

Cyber Security Business Lead

Contact

Victor.Lough@SE.com

Life Is On | Schneider Electric