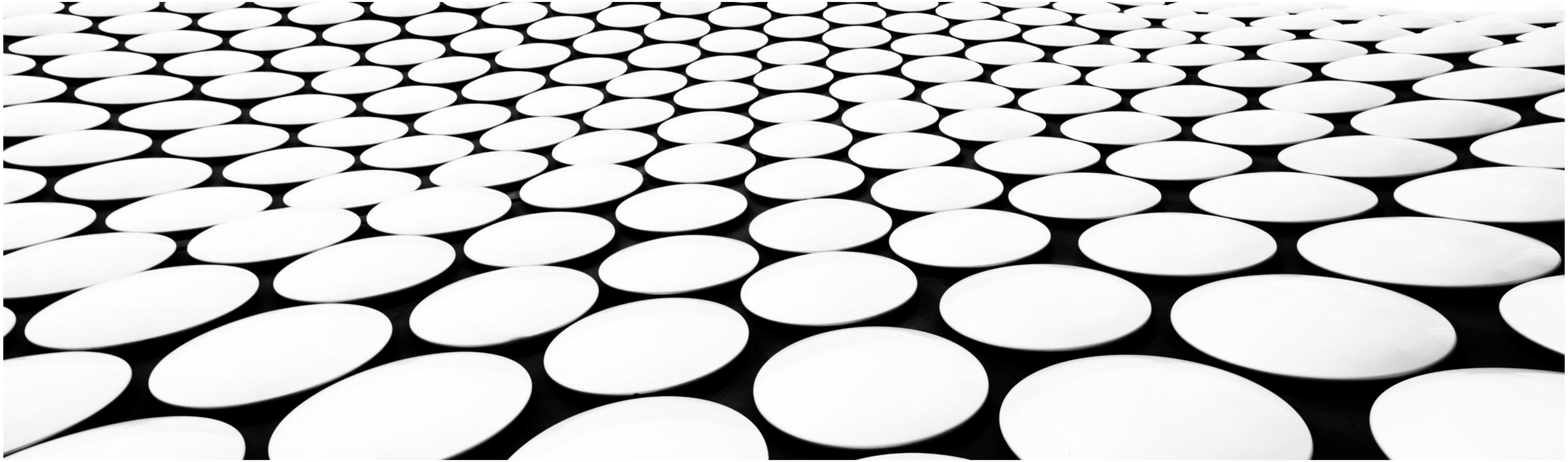
PRACTICAL APPLICATION OF ISA/IEC 62443

NZ ICS/OT CYBER SUMMIT 2025

βLARGE
MISSION CRITICAL CYBER SECURITY



/whois @beLarge

A cyber security architecture enthusiast, infrastructure tourist, CTI Nerd and "cyber hype guy"

BLARGE
MISSION CRITICAL CYBER SECURITY

- Director and Principal Cyber Security Architect at BLARGE & Director OT Cyber Threat Intelligence at Ravinn
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Proud member of Professionals Australia
  The Union for STEM Workers – join your #STEMUNION
- Experience in Electricity Generation & Transmission, Railway, Aviation, Emergency Services and Consulting industries
- Bach Eng (Telecomms) QUT First Class Honours and
  Master Business (Applied Finance) with Distinction QUT

SABSA® Chartered Architect Foundation SCF

GIAC Industrial Cyber Security Professional GICSP

GIAC Response and Industrial Defense GRID

GIAC Cyber Threat Intelligence GCTI

GIAC Security Operations Manager GSOM

ISA/IEC 62443 Cybersecurity Expert ISA

alc Cyber Security Foundation+Practitioner™ CERTIFIED

Why *this* presentation?

Agenda

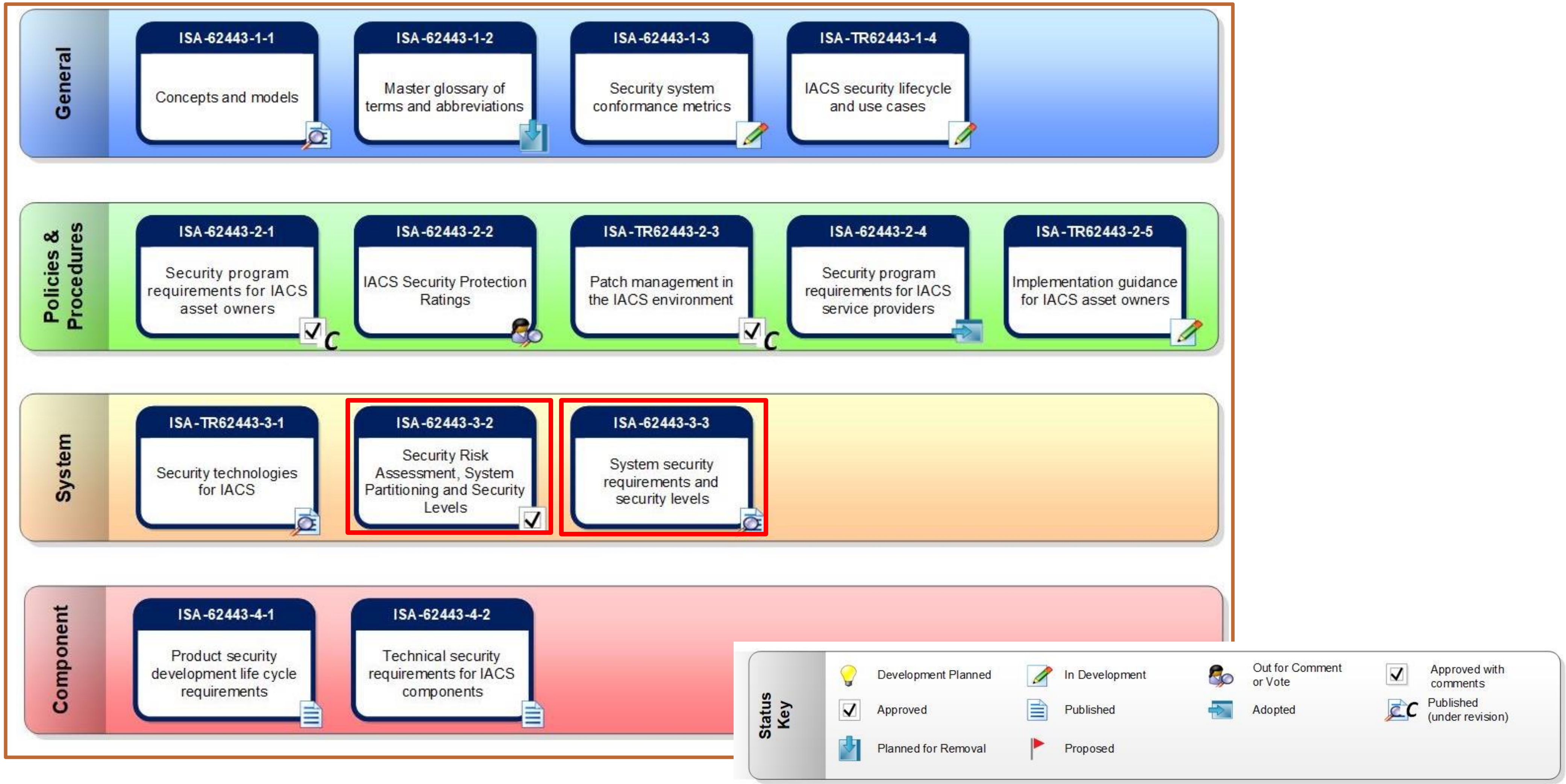
- Quick overview of ISA/IEC 62443
- How to Apply 3-2 and 3-3 to your projects
- Technology Selection

OVERVIEW OF THE ISA/IEC 62443 STANDARDS SERIES

OVERVIEW OF ISA/IEC 62443

- ISA/IEC 62443 is a Framework of Cyber Security Standards for Industrial Automation and Control Systems (IACS)
- ISA 99 is the Working group and the standards were originally published with ANSI as ISA 99 but are now published in partnership with the IEC and are designated ISA/IEC 62443
- You might see ISA 95 – Enterprise-Control System Integration – it is based on the Purdue Model but it is separate to ISA 62443
- ISA 62443 is referenced by the NIST Cyber Security Framework but only 2 of the 14 publications referenced (Part 2-1 and Part 3-3)

STANDARD SERIES MATRIX



General

- ISA-62443-1-1: Concepts and models
- ISA-62443-1-2: Master glossary of terms and abbreviations
- ISA-62443-1-3: Security system conformance metrics
- ISA-TR62443-1-4: IACS security lifecycle and use cases

Policies & Procedures

- ISA-62443-2-1: Security program requirements for IACS asset owners
- ISA-62443-2-2: IACS Security Protection Ratings
- ISA-TR62443-2-3: Patch management in the IACS environment
- ISA-62443-2-4: Security program requirements for IACS service providers
- ISA-TR62443-2-5: Implementation guidance for IACS asset owners

System

- ISA-TR62443-3-1: Security technologies for IACS
- ISA-62443-3-2: Security Risk Assessment, System Partitioning and Security Levels
- ISA-62443-3-3: System security requirements and security levels

Component

- ISA-62443-4-1: Product security development life cycle requirements
- ISA-62443-4-2: Technical security requirements for IACS components

Status Key

- Development Planned
- In Development
- Out for Comment or Vote
- Approved with comments
- Approved
- Published
- Adopted
- Published (under revision)
- Planned for Removal
- Proposed

HIERARCHY AND LIFECYLE VIEW

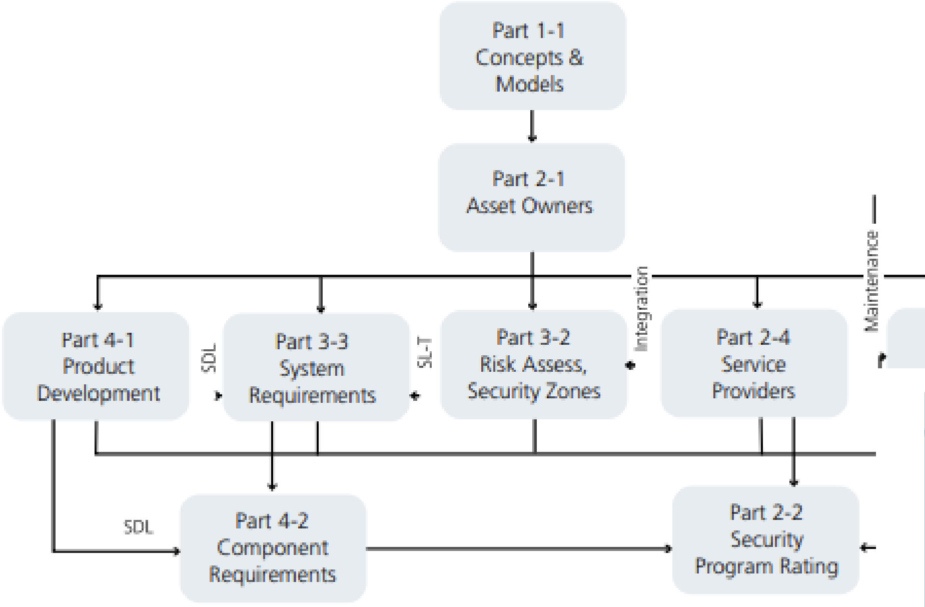
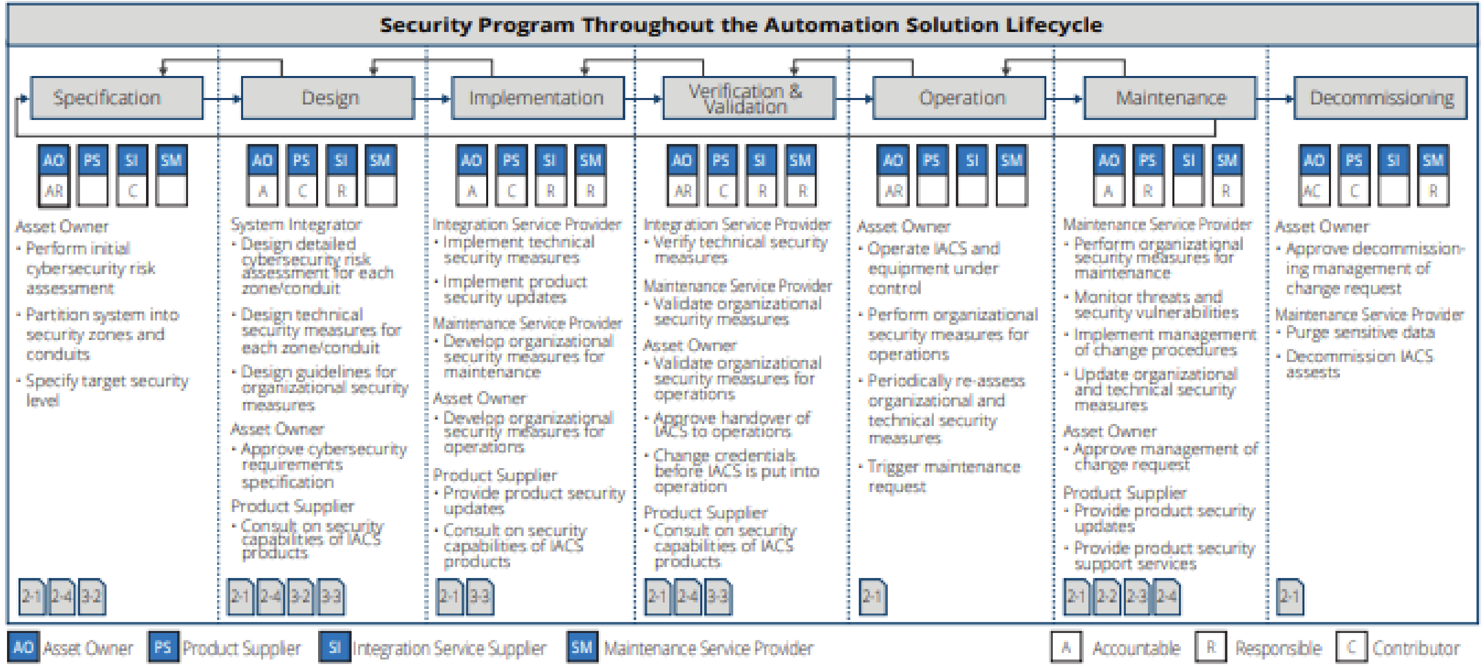


Figure 5: ISA/IEC 62443 Standards – Hierarchical Vie



Security Program Throughout the Automation Solution Lifecycle

	Specification	Design	Implementation	Verification & Validation	Operation	Maintenance	Decommissioning
AO	AR	A	A	AR	AR	A	AC
PS		C	C	C		R	C
SI	C	R	R	R			
SM			R	R		R	R

Specification

Asset Owner
- Perform initial cybersecurity risk assessment
- Partition system into security zones and conduits
- Specify target security level

2-1 2-4 3-2

Design

System Integrator
- Design detailed cybersecurity risk assessment for each zone/conduit
- Design technical security measures for each zone/conduit
- Design guidelines for organizational security measures

Asset Owner
- Approve cybersecurity requirements specification

Product Supplier
- Consult on security capabilities of IACS products

2-1 2-4 3-2 3-3

Implementation

Integration Service Provider
- Implement technical security measures
- Implement product security updates

Maintenance Service Provider
- Develop organizational security measures for maintenance

Asset Owner
- Develop organizational security measures for operations

Product Supplier
- Provide product security updates
- Consult on security capabilities of IACS products

2-1 3-3

Verification & Validation

Integration Service Provider
- Verify technical security measures

Maintenance Service Provider
- Validate organizational security measures

Asset Owner
- Validate organizational security measures for operations
- Approve handover of IACS to operations
- Change credentials before IACS is put into operation

Product Supplier
- Consult on security capabilities of IACS products

2-1 2-4 3-3

Operation

Asset Owner
- Operate IACS and equipment under control
- Perform organizational security measures for operations
- Periodically re-assess organizational and technical security measures
- Trigger maintenance request

2-1

Maintenance

Maintenance Service Provider
- Perform organizational security measures for maintenance
- Monitor threats and security vulnerabilities
- Implement management of change procedures
- Update organizational and technical security measures

Asset Owner
- Approve management of change request

Product Supplier
- Provide product security updates
- Provide product security support services

2-1 2-2 2-3 2-4

Decommissioning

Asset Owner
- Approve decommissioning management of change request

Maintenance Service Provider
- Purge sensitive data
- Decommission IACS assests

2-1

AO	Asset Owner	A	Accountable
PS	Product Supplier	R	Responsible
SI	Integration Service Supplier	C	Contributor
SM	Maintenance Service Provider		

APPLYING 62443 TO YOUR PROJECT

USING PART 3-2 AND PART 3-3

ASSESS, DESIGN & IMPLEMENT, OPERATE & MAINTAIN

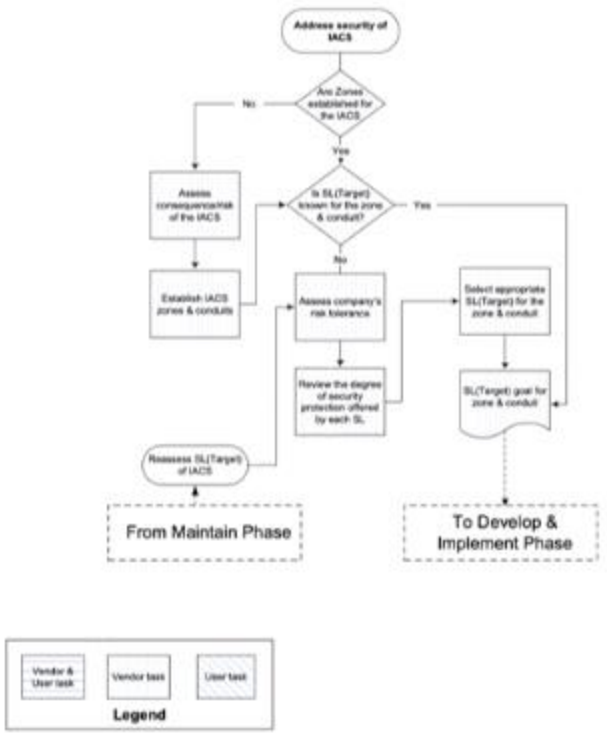

Address security of IACS
Are Zones established for the IACS
No
Yes
Assess consequence/risk of the IACS
Establish IACS zones & conduits
Is SL(Target) known for the zone & conduit?
Yes
No
Assess company's risk tolerance
Review the degree of security protection offered by each SL
Select appropriate SL(Target) for the zone & conduit
SL(Target) goal for zone & conduit
Reassess SL(Target) of IACS
From Maintain Phase
To Develop & Implement Phase
Vendor & User task
Vendor task
User task
Legend

Figure 9 – Security Level Lifecycle – Assess Phase

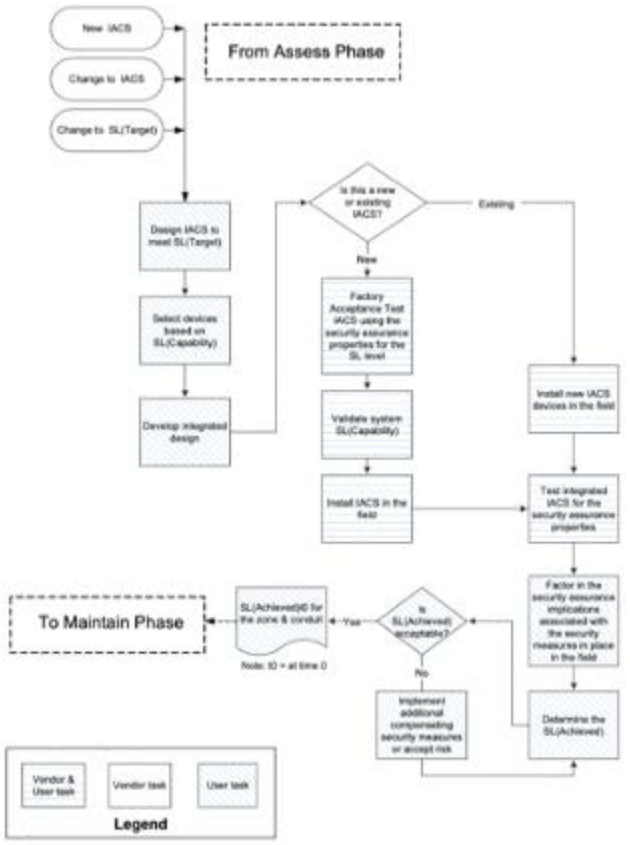

New IACS
Change to IACS
Change to SL(Target)
From Assess Phase
Design IACS to meet SL(Target)
Select devices based on SL(Capability)
Develop integrated design
Is this a new or existing IACS?
Existing
New
Factory Acceptance Test IACS using the security assurance properties for the SL level
Validate system SL(Capability)
Install IACS in the field
Install new IACS devices in the field
Test integrated IACS for the security assurance properties
Factor in the security assurance implications associated with the security measures in place in the field
Determine the SL(Achieved)
Is SL(Achieved) acceptable?
Yes
No
Implement additional compensating security measures or accept risk
SL(Achieved)t0 for the zone & conduit
Note: t0 = at time 0
To Maintain Phase
Vendor & User task
Vendor task
User task
Legend

Figure 10 – Security Level Lifecycle – Implement Phase

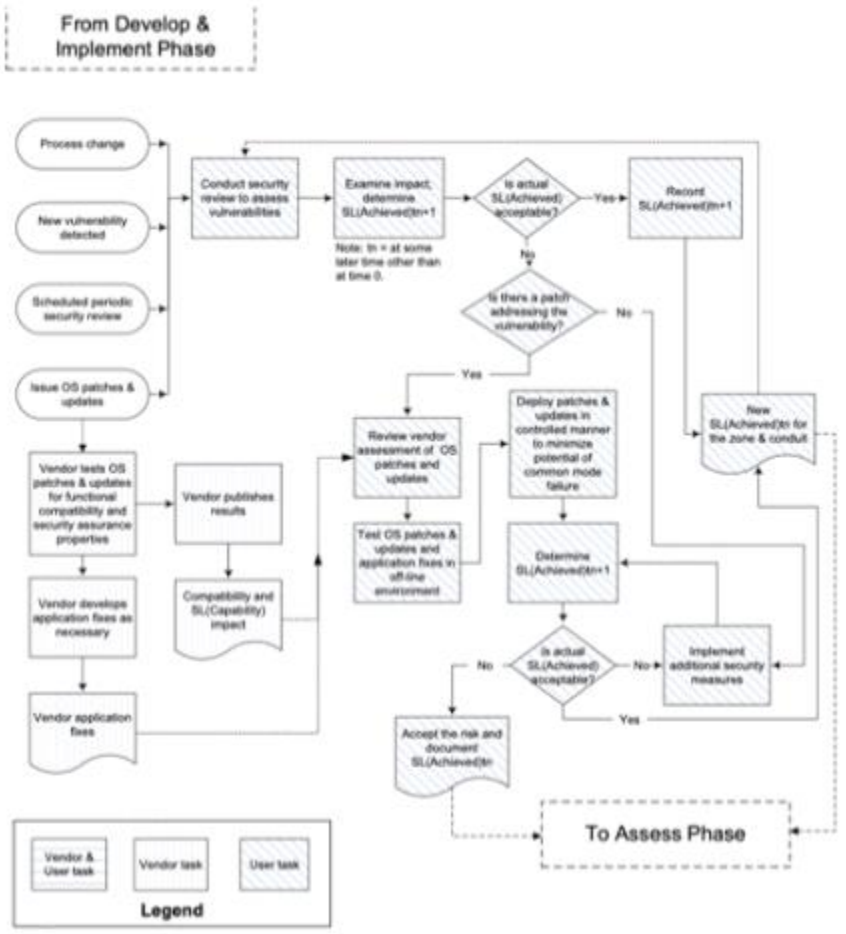

From Develop & Implement Phase
Process change
New vulnerability detected
Scheduled periodic security review
Issue OS patches & updates
Conduct security review to assess vulnerabilities
Examine impact, determine SL(Achieved)tn+1
Note: tn = at some later time other than at time 0.
Is actual SL(Achieved) acceptable?
Yes
Record SL(Achieved)tn+1
No
Is there a patch addressing the vulnerability?
No
Yes
Vendor tests OS patches & updates for functional compatibility and security assurance properties
Vendor publishes results
Compatibility and SL(Capability) impact
Vendor develops application fixes as necessary
Vendor application fixes
Review vendor assessment of OS patches and updates
Test OS patches & updates and application fixes in off-line environment
Deploy patches & updates in controlled manner to minimize potential of common mode failure
Determine SL(Achieved)tn+1
Is actual SL(Achieved) acceptable?
No
No
Yes
Implement additional security measures
New SL(Achieved)tn for the zone & conduit
Accept the risk and document SL(Achieved)tn
To Assess Phase
Vendor & User task
Vendor task
User task
Legend

Figure 11 – Security Level Lifecycle – Maintain Phase

Ref – ISA/IEC 62443-1-1

ZONE AND CONDUIT DEFINITIONS

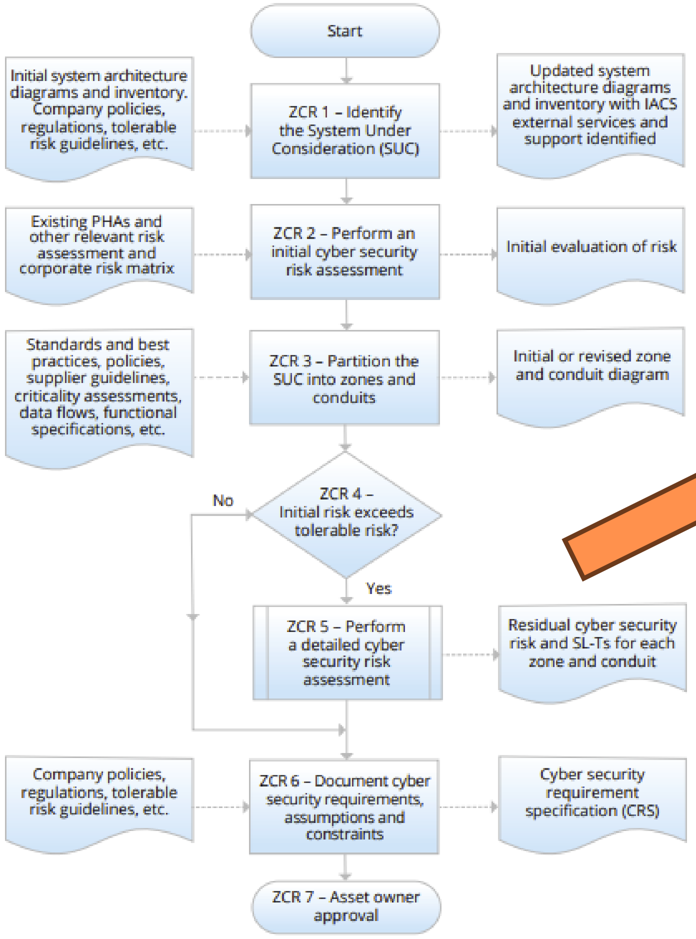
- Zone
  - grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (For example, least privilege principles) or responsible organisation
- Conduit
  - Logical grouping of communication channels that share a common security requirements connecting two or more zones
- Channel
  - Specific logical or physical communication link between assets

NIST CSF – ID.AM-03

- “ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained”

Ref - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

3-2 – RISK PROCESS ON A PAGE



Start

Initial system architecture diagrams and inventory. Company policies, regulations, tolerable risk guidelines, etc.

ZCR 1 – Identify the System Under Consideration (SUC)

Updated system architecture diagrams and inventory with IACS external services and support identified

Existing PHAs and other relevant risk assessment and corporate risk matrix

ZCR 2 – Perform an initial cyber security risk assessment

Initial evaluation of risk

Standards and best practices, policies, supplier guidelines, criticality assessments, data flows, functional specifications, etc.

ZCR 3 – Partition the SUC into zones and conduits

Initial or revised zone and conduit diagram

ZCR 4 – Initial risk exceeds tolerable risk?

No

Yes

ZCR 5 – Perform a detailed cyber security risk assessment

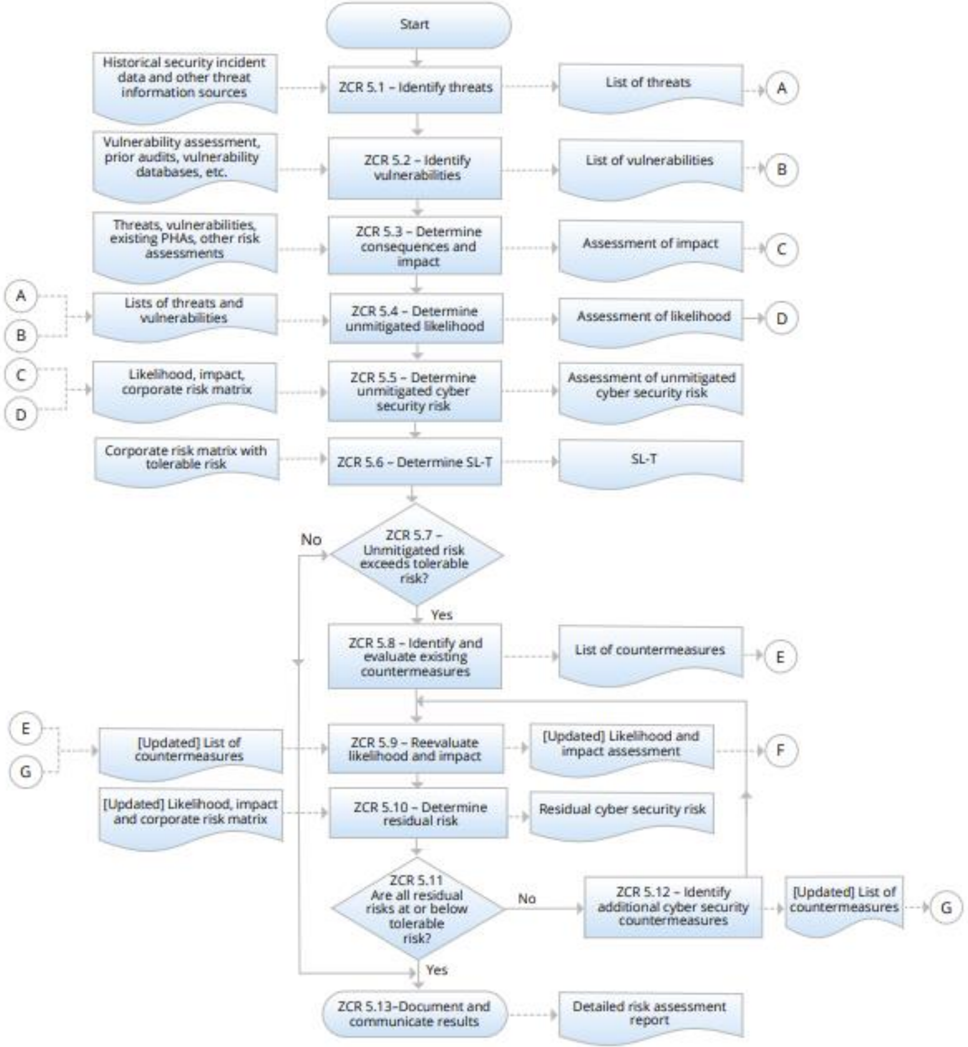
Residual cyber security risk and SL-Ts for each zone and conduit

Company policies, regulations, tolerable risk guidelines, etc.

ZCR 6 – Document cyber security requirements, assumptions and constraints

Cyber security requirement specification (CRS)

ZCR 7 – Asset owner approval



Start

Historical security incident data and other threat information sources

ZCR 5.1 – Identify threats

List of threats

A

Vulnerability assessment, prior audits, vulnerability databases, etc.

ZCR 5.2 – Identify vulnerabilities

List of vulnerabilities

B

Threats, vulnerabilities, existing PHAs, other risk assessments

ZCR 5.3 – Determine consequences and impact

Assessment of impact

C

A

B

Lists of threats and vulnerabilities

ZCR 5.4 – Determine unmitigated likelihood

Assessment of likelihood

D

C

D

Likelihood, impact, corporate risk matrix

ZCR 5.5 – Determine unmitigated cyber security risk

Assessment of unmitigated cyber security risk

Corporate risk matrix with tolerable risk

ZCR 5.6 – Determine SL-T

SL-T

No

ZCR 5.7 – Unmitigated risk exceeds tolerable risk?

Yes

ZCR 5.8 – Identify and evaluate existing countermeasures

List of countermeasures

E

E

G

[Updated] List of countermeasures

ZCR 5.9 – Reevaluate likelihood and impact

[Updated] Likelihood and impact assessment

F

[Updated] Likelihood, impact and corporate risk matrix

ZCR 5.10 – Determine residual risk

Residual cyber security risk

ZCR 5.11 Are all residual risks at or below tolerable risk?

No

ZCR 5.12 – Identify additional cyber security countermeasures

[Updated] List of countermeasures

G

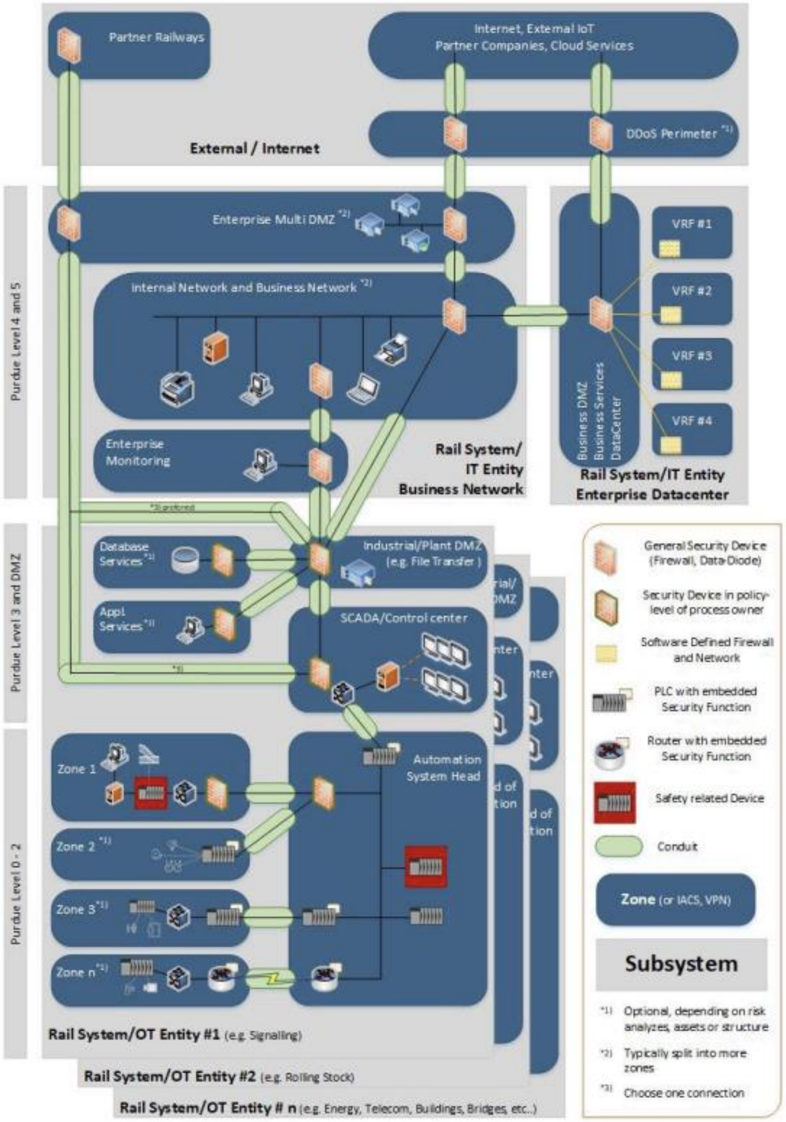
Yes

ZCR 5.13-Document and communicate results

Detailed risk assessment report

PARTITIONING THE SUC

- ZCR 3.1 Establish Zones and Conduits
- ZCR 3.2 Separate business and IACS assets
- ZCR 3.3 Separate Safety related assets
- ZCR 3.4 Separate temporarily connected devices
- ZCR 3.5 Separate wireless devices
- ZCR 3.6 Separate devices connected via external networks


Partner Railways
Internet, External IoT
Partner Companies, Cloud Services
DDoS Perimeter *1)
External / Internet
Purdue Level 4 and 5
Enterprise Multi DMZ *2)
Internal Network and Business Network *2)
VRF #1
VRF #2
VRF #3
VRF #4
Business DMZ
Business Services
DataCenter
Enterprise Monitoring
Rail System/ IT Entity Business Network
Rail System/IT Entity Enterprise Datacenter
*3) preferred
Purdue Level 3 and DMZ
Database Services *1)
Industrial/Plant DMZ (e.g. File Transfer)
Appl Services *1)
SCADA/Control center
*3)
Purdue Level 0 - 2
Zone 1
Automation System Head
Zone 2 *1)
Zone 3 *1)
Zone n *1)
Rail System/OT Entity #1 (e.g. Signaling)
Rail System/OT Entity #2 (e.g. Rolling Stock)
Rail System/OT Entity # n (e.g. Energy, Telecom, Buildings, Bridges, etc..)
General Security Device (Firewall, Data-Diode)
Security Device in policy-level of process owner
Software Defined Firewall and Network
PLC with embedded Security Function
Router with embedded Security Function
Safety related Device
Conduit
Zone (or IACS, VPN)
Subsystem
*1) Optional, depending on risk analyzes, assets or structure
*2) Typically split into more zones
*3) Choose one connection

Ref - https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways

SECURITY LEVEL DEFINITIONS

- **Target (SL-T)** are the desired level of security for a particular Automation Solution. They are determined as the result of the Risk Assessment process (Part 3-2) and are documented in the Cybersecurity Requirements Specification. SL-T are used to select products and additional countermeasures during the Integration phase of the IACS lifecycle
- **Capability (SL-C)** are the security levels that systems or Components can provide when properly configured. These levels state that a particular system or Component is capable of meeting the SL-T natively without additional compensating countermeasures.
- **Achieved (SL-A)** are the actual levels of security for a particular Automation Solution. These are measured after the Automation Solution is commissioned and in operation.

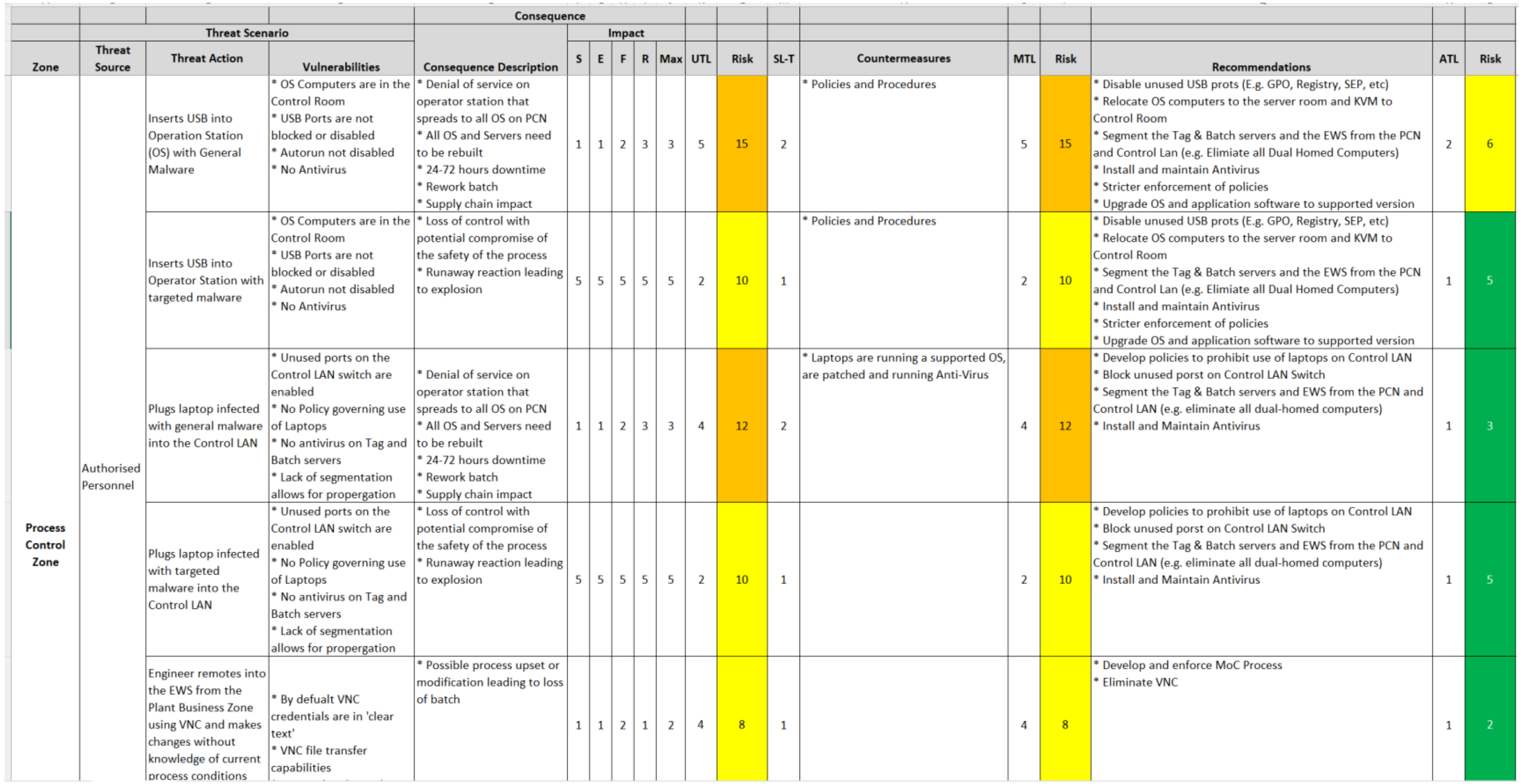
SL-1 Prevent the unauthorized disclosure of information **via eavesdropping or casual exposure**

SL-2 Prevent the unauthorized disclosure of information to an entity actively searching for it **using simple means with low resources, generic skills, and low motivation**

SL-3 Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with **moderate resources, IACS-specific skills, and moderate motivation**

SL-4 Prevent the unauthorized disclosure of information to an entity actively searching for it using **sophisticated means with extended resources, IACS-specific skills, and high motivation**

EXAMPLE 62443 RISK WORKBOOK



				Consequence														
	Threat Scenario				Impact													
Zone	Threat Source	Threat Action	Vulnerabilities	Consequence Description	S	E	F	R	Max	UTL	Risk	SL-T	Countermeasures	MTL	Risk	Recommendations	ATL	Risk
Process Control Zone	Authorised Personnel	Inserts USB into Operation Station (OS) with General Malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No Antivirus	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24-72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	5	15	2	* Policies and Procedures	5	15	* Disable unused USB prots (E.g. GPO, Registry, SEP, etc) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and the EWS from the PCN and Control Lan (e.g. Elimiate all Dual Homed Computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	2	6
		Inserts USB into Operator Station with targeted malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No Antivirus	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Policies and Procedures	2	10	* Disable unused USB prots (E.g. GPO, Registry, SEP, etc) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and the EWS from the PCN and Control Lan (e.g. Elimiate all Dual Homed Computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	1	5
		Plugs laptop infected with general malware into the Control LAN	* Unused ports on the Control LAN switch are enabled * No Policy governing use of Laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propergation	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24-72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	4	12	2	* Laptops are running a supported OS, are patched and running Anti-Virus	4	12	* Develop policies to prohibit use of laptops on Control LAN * Block unused porst on Control LAN Switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and Maintain Antivirus	1	3
		Plugs laptop infected with targeted malware into the Control LAN	* Unused ports on the Control LAN switch are enabled * No Policy governing use of Laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propergation	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1		2	10	* Develop policies to prohibit use of laptops on Control LAN * Block unused porst on Control LAN Switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and Maintain Antivirus	1	5
		Engineer remotes into the EWS from the Plant Business Zone using VNC and makes changes without knowledge of current process conditions	* By defualt VNC credentials are in 'clear text' * VNC file transfer capabilities	* Possible process upset or modification leading to loss of batch	1	1	2	1	2	4	8	1		4	8	* Develop and enforce MoC Process * Eliminate VNC	1	2

Where:

UTL – Unmitigated Threat Likelihood

SL-T Security Level Target

MTL – Mitigated Threat Likelihood

ATL – Adjusted Threat Likelihood

Ref – ISA IC33 training

CYBER SECURITY REQUIREMENTS SPECIFICATION (CSRS)

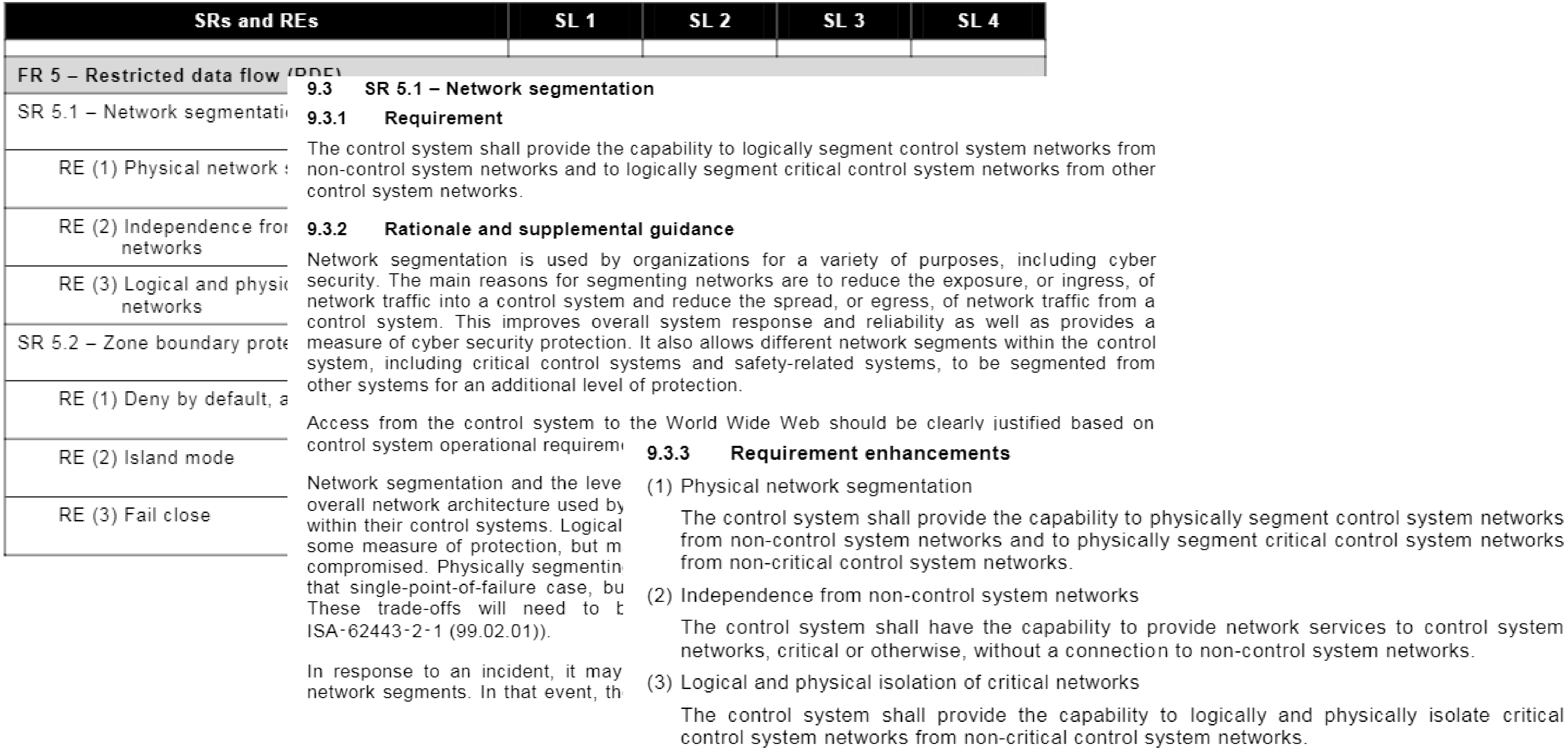
- ZCR 6.2 SuC Description
- ZCR 6.3 Zone and Conduit drawings
- ZCR 6.4 Zone and Conduit Characteristics
- ZCR 6.5 Operating environment assumptions
- ZCR 6.6 Threat environment
- ZCR 6.7 Organisational security policies
- ZCR 6.8 Tolerable Risk
- ZCR 6.9 Regulatory requirements

PART 3-3 FR COUNTS

- FR 1 – Identification and Authentication Control (IAC)
- FR 2 – Use Control (UC)
- FR 3 – System Integrity (SI)
- FR 4 – Data Confidentiality (DC)
- FR 5 – Restricted Data Flow (RDF)
- FR 6 – Timely Response to Events (TRE)
- FR 7 – Resource Availability (RA)

Foundational Requirement	Count SL-1	Count SL-2	Count SL-3	Count SL-4
IAC	10	6	6	2
UC	8	4	9	3
SI	6	4	6	3
DC	2	2	1	1
RDF	4	2	4	1
TRE	1	1	1	-
RA	7	3	3	-

EXAMPLE 3-3



SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
SR 5.1 – Network segmentati				
RE (1) Physical network s				
RE (2) Independence fro networks				
RE (3) Logical and physic networks				
SR 5.2 – Zone boundary prote				
RE (1) Deny by default, a				
RE (2) Island mode				
RE (3) Fail close				

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirem

Network segmentation and the leve overall network architecture used by within their control systems. Logical some measure of protection, but m compromised. Physically segmentin that single-point-of-failure case, bu These trade-offs will need to b ISA‑62443‑2‑1 (99.02.01)).

In response to an incident, it may network segments. In that event, th

9.3.3 Requirement enhancements

(1) Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

(2) Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

(3) Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

ALL OF FR5 – RESTRICTED DATA FLOW

- SR 5.1 – Network segmentation (SL-1)
  - SR 5.1 RE 1 – Physical network segmentation (SL-2)
  - SR 5.1 RE 2 – Independence from non-control system networks (SL-3)
  - SR 5.1 RE 3 – Logical and physical isolation of critical networks (SL-4)
- SR 5.2 – Zone boundary protection (SL-1)
  - SR 5.2 RE 1 – Deny by default, allow by exception (SL-2)
  - SR 5.2 RE 2 – Island mode (SL-3)
  - SR 5.2 RE 3 – Fail close (SL-3)
- SR 5.3 – General purpose person-to-person communication restrictions (SL-1)
  - SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications (SL-3)
- SR 5.4 – Application partitioning (SL-1)

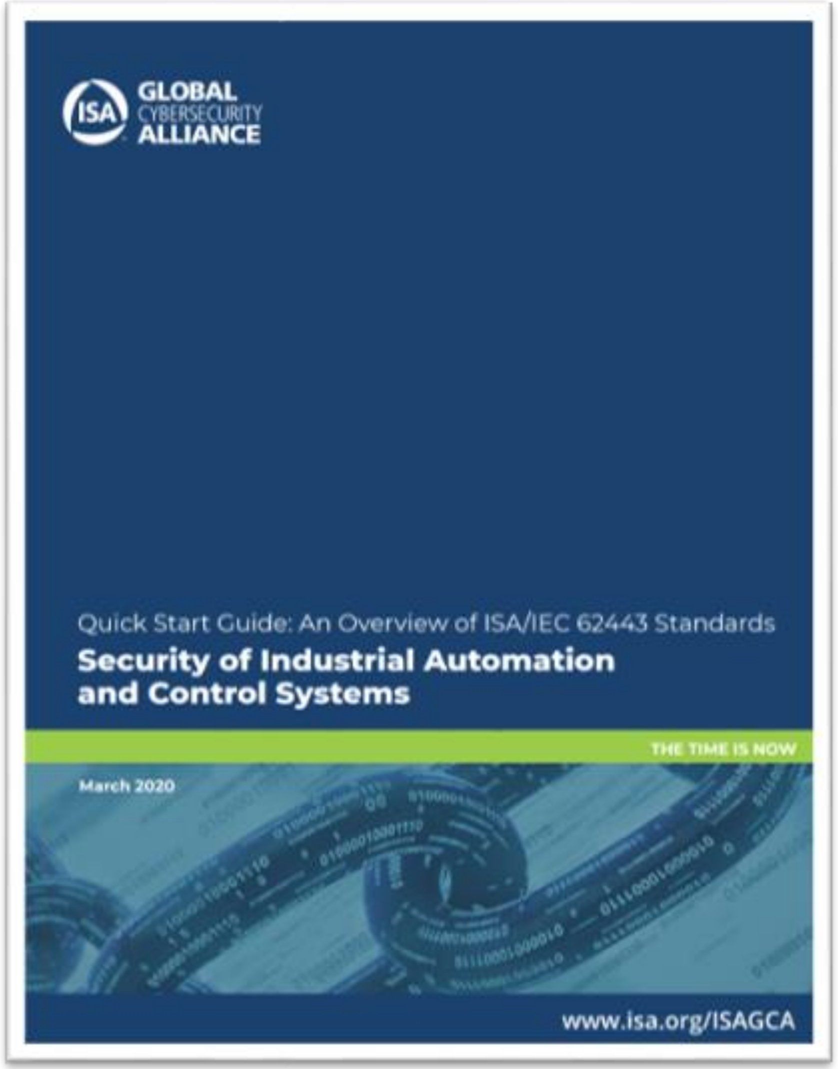
SECURITY SERVICES = PEOPLE, PROCESS AND TECHNOLOGY

- People
  - Do your team have the appropriate Knowledge, Skills and Ability (training)
- Process
  - Have appropriate processes been defined for example review of Segmentation Policies?
- Technology
  - What security technologies will you use?

TECHNOLOGY SELECTION

Technology	Considerations
Access Control List (ACL)	• Difficult to manage at scale • Limited Jitter • Good for defense in depth at lower levels of the ICS networks (delay control)
Next Generation Firewall (NGFW)	• Most common control at the edge (IT/OT, Large site boundary) • Most familiar control
Data Diode	• Hardware enforced one way direction – very high assurance
Software Defined Networking	• Emerging capability, some OT Vendors are doing this
Zero Trust	• Early Days and could be useful for specific use cases and tying identity, advanced conditional security policy and network segmentation together

FURTHER RESOURCES



ISA GLOBAL CYBERSECURITY ALLIANCE

Quick Start Guide: An Overview of ISA/IEC 62443 Standards

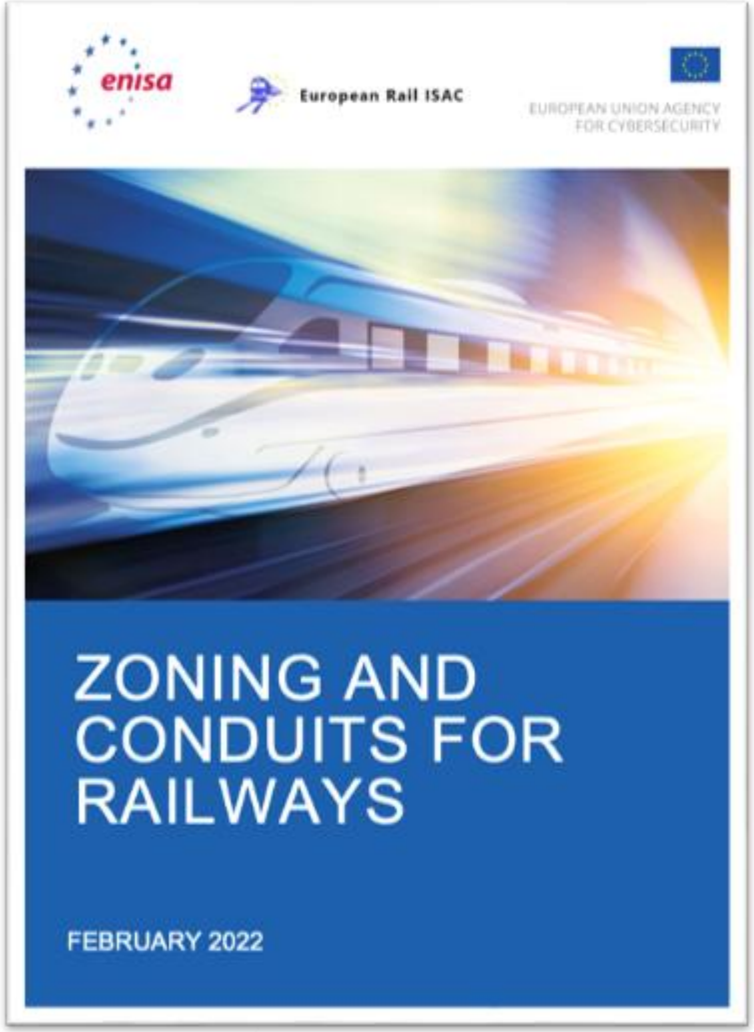
Security of Industrial Automation and Control Systems

THE TIME IS NOW

March 2020

www.isa.org/ISAGCA

https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf



enisa

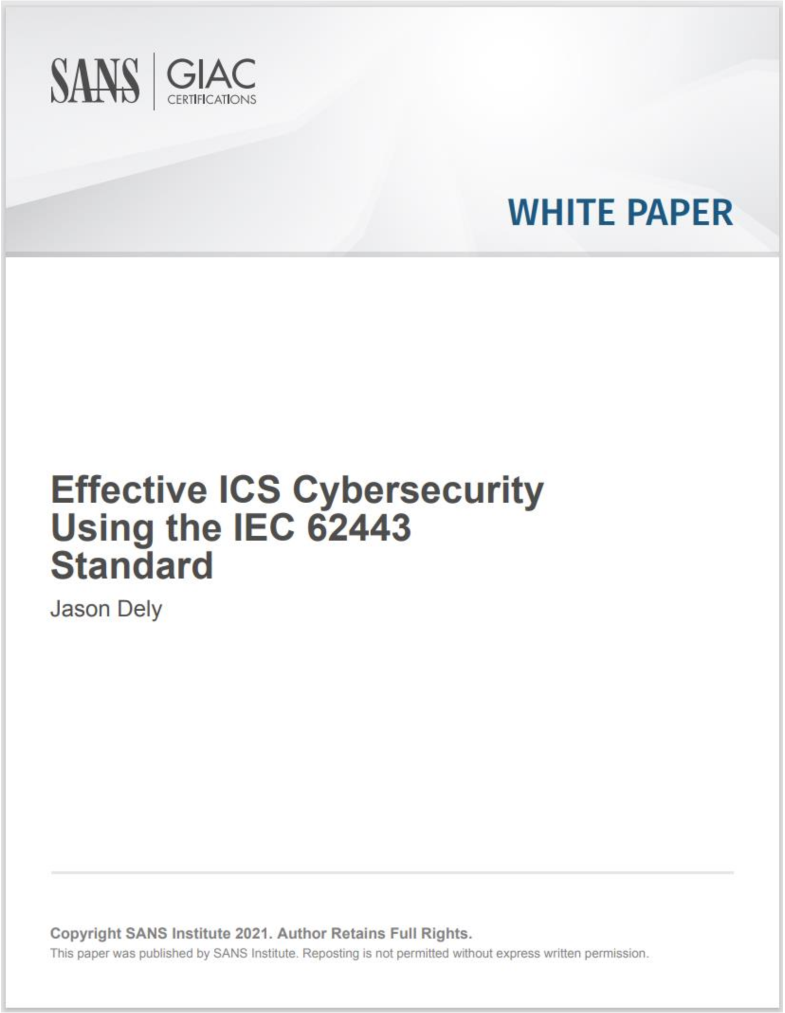
European Rail ISAC

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ZONING AND CONDUITS FOR RAILWAYS

FEBRUARY 2022

https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways



SANS | GIAC CERTIFICATIONS

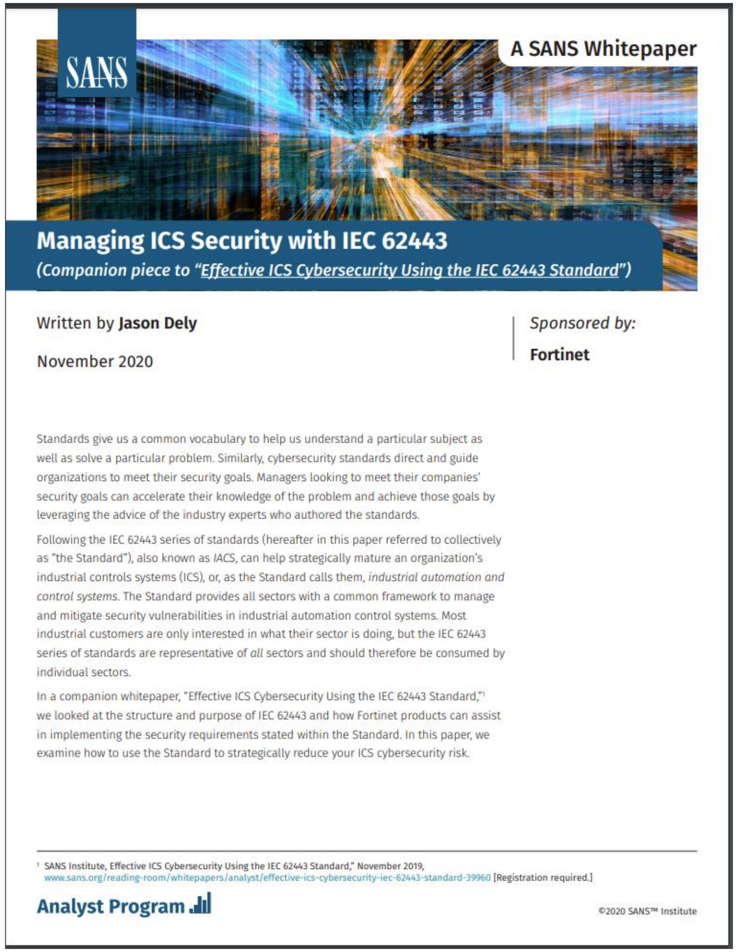
WHITE PAPER

Effective ICS Cybersecurity Using the IEC 62443 Standard

Jason Dely

Copyright SANS Institute 2021. Author Retains Full Rights.
This paper was published by SANS Institute. Reposting is not permitted without express written permission.

https://www.sans.org/white-papers/39990/



SANS

A SANS Whitepaper

Managing ICS Security with IEC 62443

(Companion piece to "Effective ICS Cybersecurity Using the IEC 62443 Standard")

Written by **Jason Dely**

November 2020

Sponsored by:
Fortinet

Standards give us a common vocabulary to help us understand a particular subject as well as solve a particular problem. Similarly, cybersecurity standards direct and guide organizations to meet their security goals. Managers looking to meet their companies' security goals can accelerate their knowledge of the problem and achieve those goals by leveraging the advice of the industry experts who authored the standards.

Following the IEC 62443 series of standards (hereafter in this paper referred to collectively as "the Standard"), also known as *IACS*, can help strategically mature an organization's industrial controls systems (ICS), or, as the Standard calls them, *industrial automation and control systems*. The Standard provides all sectors with a common framework to manage and mitigate security vulnerabilities in industrial automation control systems. Most industrial customers are only interested in what their sector is doing, but the IEC 62443 series of standards are representative of *all* sectors and should therefore be consumed by individual sectors.

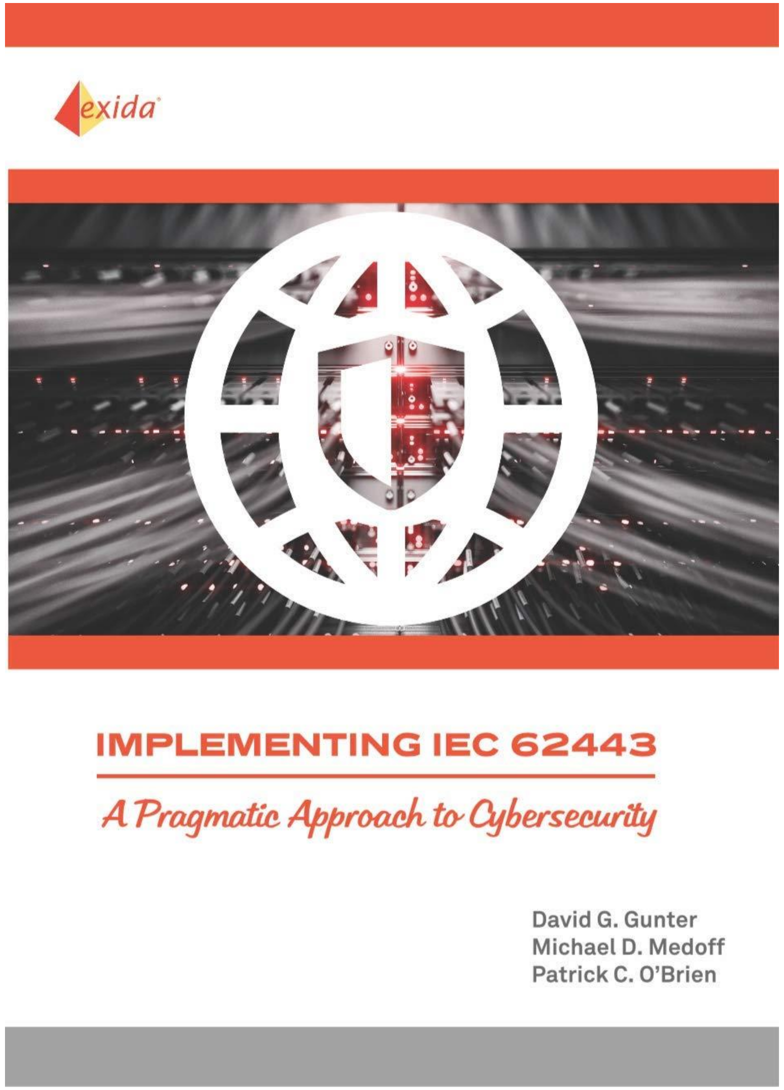
In a companion whitepaper, "Effective ICS Cybersecurity Using the IEC 62443 Standard,"[1] we looked at the structure and purpose of IEC 62443 and how Fortinet products can assist in implementing the security requirements stated within the Standard. In this paper, we examine how to use the Standard to strategically reduce your ICS cybersecurity risk.

[1] SANS Institute, Effective ICS Cybersecurity Using the IEC 62443 Standard," November 2019, www.sans.org/reading-room/whitepapers/analyst/effective-ics-cybersecurity-iec-62443-standard-39960 [Registration required.]

Analyst Program

©2020 SANS™ Institute

https://www.sans.org/white-papers/39990/



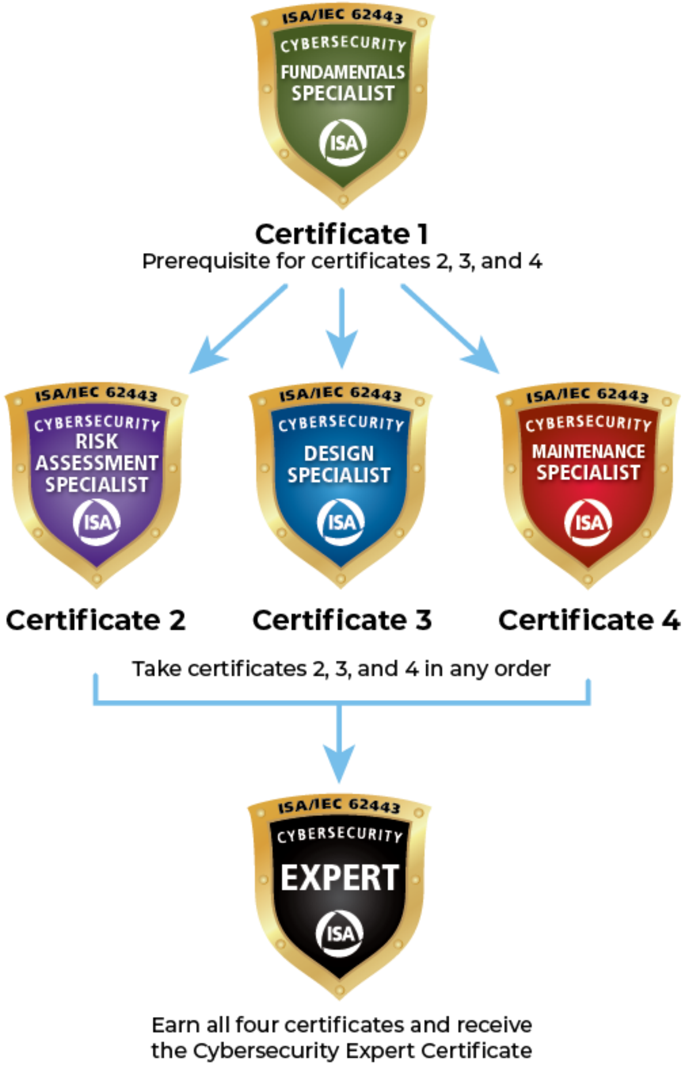
exida

IMPLEMENTING IEC 62443

A Pragmatic Approach to Cybersecurity

David G. Gunter
Michael D. Medoff
Patrick C. O'Brien

https://www.amazon.com.au/Implementing-IEC-62443-Pragmatic-Cybersecurity/dp/1934977179



ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST ISA
Certificate 1
Prerequisite for certificates 2, 3, and 4
ISA/IEC 62443 CYBERSECURITY RISK ASSESSMENT SPECIALIST ISA
ISA/IEC 62443 CYBERSECURITY DESIGN SPECIALIST ISA
ISA/IEC 62443 CYBERSECURITY MAINTENANCE SPECIALIST ISA
Certificate 2
Certificate 3
Certificate 4
Take certificates 2, 3, and 4 in any order
ISA/IEC 62443 CYBERSECURITY EXPERT ISA
Earn all four certificates and receive the Cybersecurity Expert Certificate

https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

THANK YOU!

https://linkedin.com/in/blargeau

bruce@blarge.io

https://blarge.io

https://www.blarge.io/04-contact

https://github.com/beLarge