



A Practical Application of the ISA/IEC 62443 Standard Series

IOT SCADA HACKERS AUSTRALIA
DECEMBER 2023

Agenda

1. /whois @beLarge
2. Overview of the ISA/IEC 62443 Standard Series
3. Using Part 2-1 to Build a Cyber Security Management System
4. Applying Part 3-2 and Part 3-3 to Projects
5. Further Resources

/whois @beLarge

*A cyber security
architecture enthusiast,
infrastructure tourist and
“cyber hype guy”*

- o Operational Technology (OT) Security Team Leader at Powerlink
- o Worked in IT and OT in Network & System Engineering and Cyber Security roles for 15 years
- o Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- o Proud member of Professional's Australia (PA), incoming president of Qld Professional Engineers and a union delegate for PA at Powerlink
- o Vice Chair of the Queensland Branch of the Australian Information Security Association (AISA) and Chair of the AISA Security Architecture Special Interest Group (SecARCH SIG)
- o Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

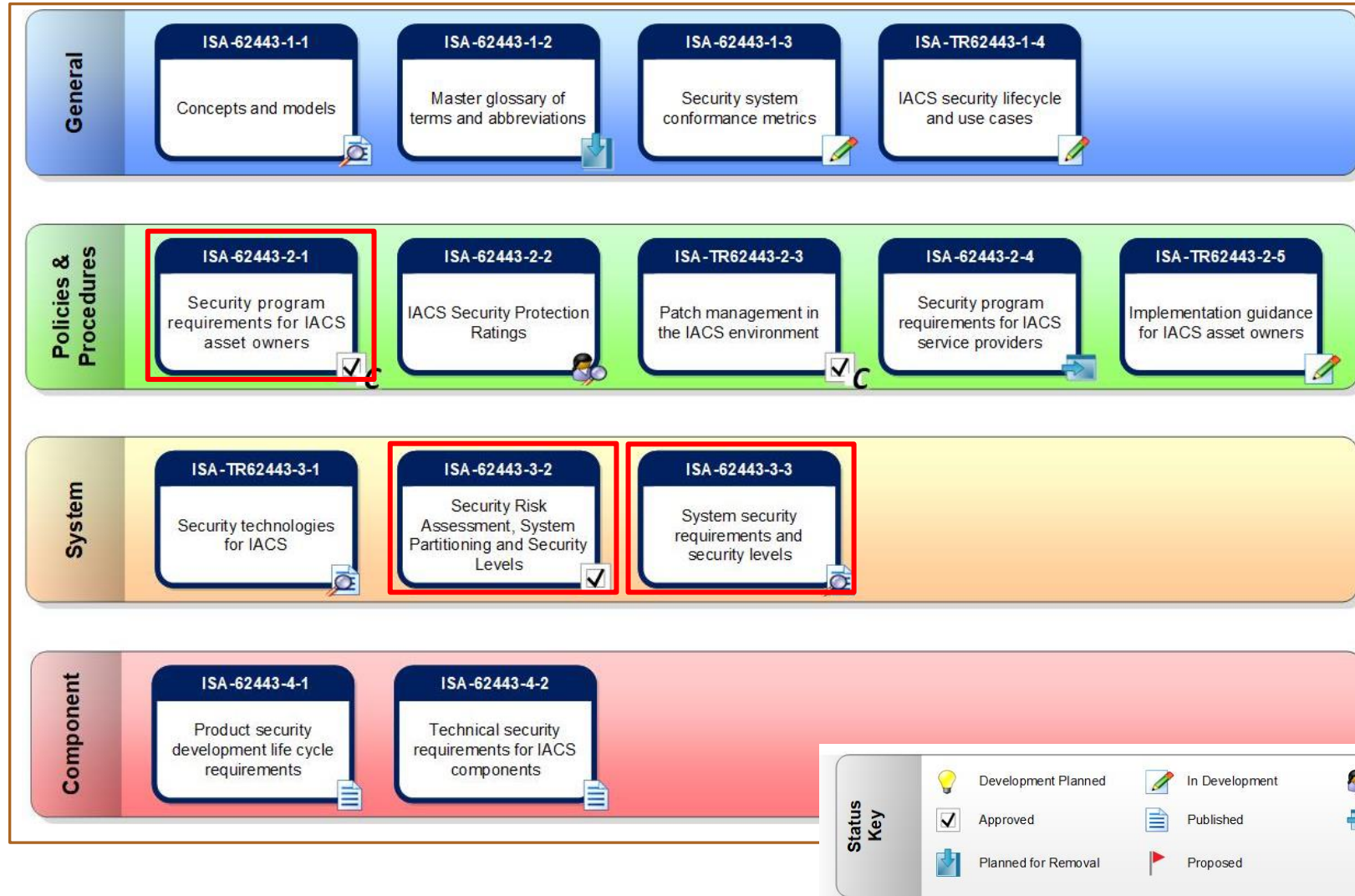


Overview of the ISA/IEC 62443 Standards Series

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



Hierarchy and Lifecycle View

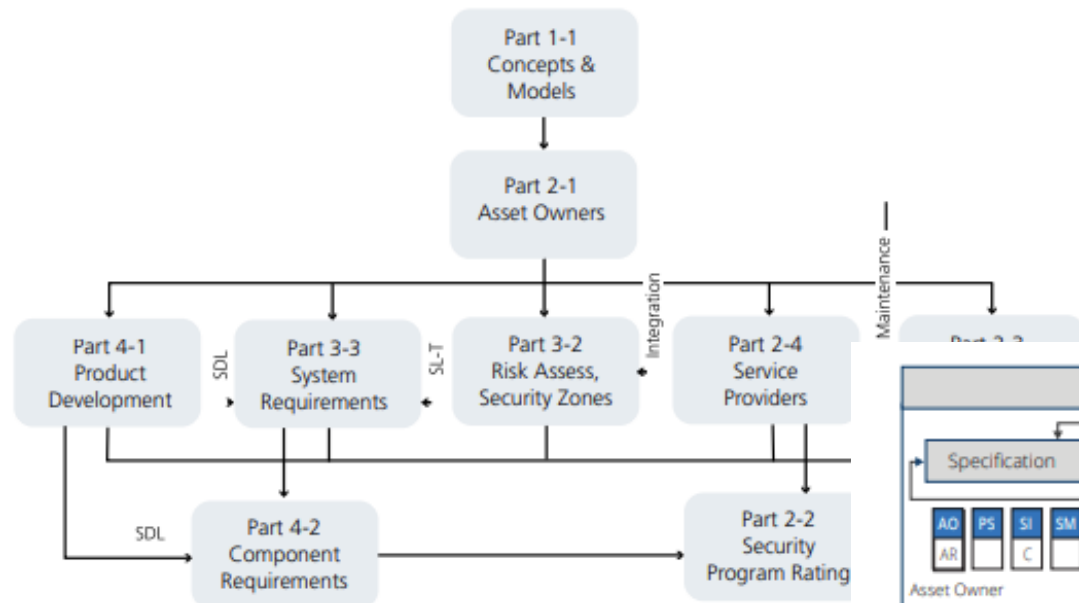
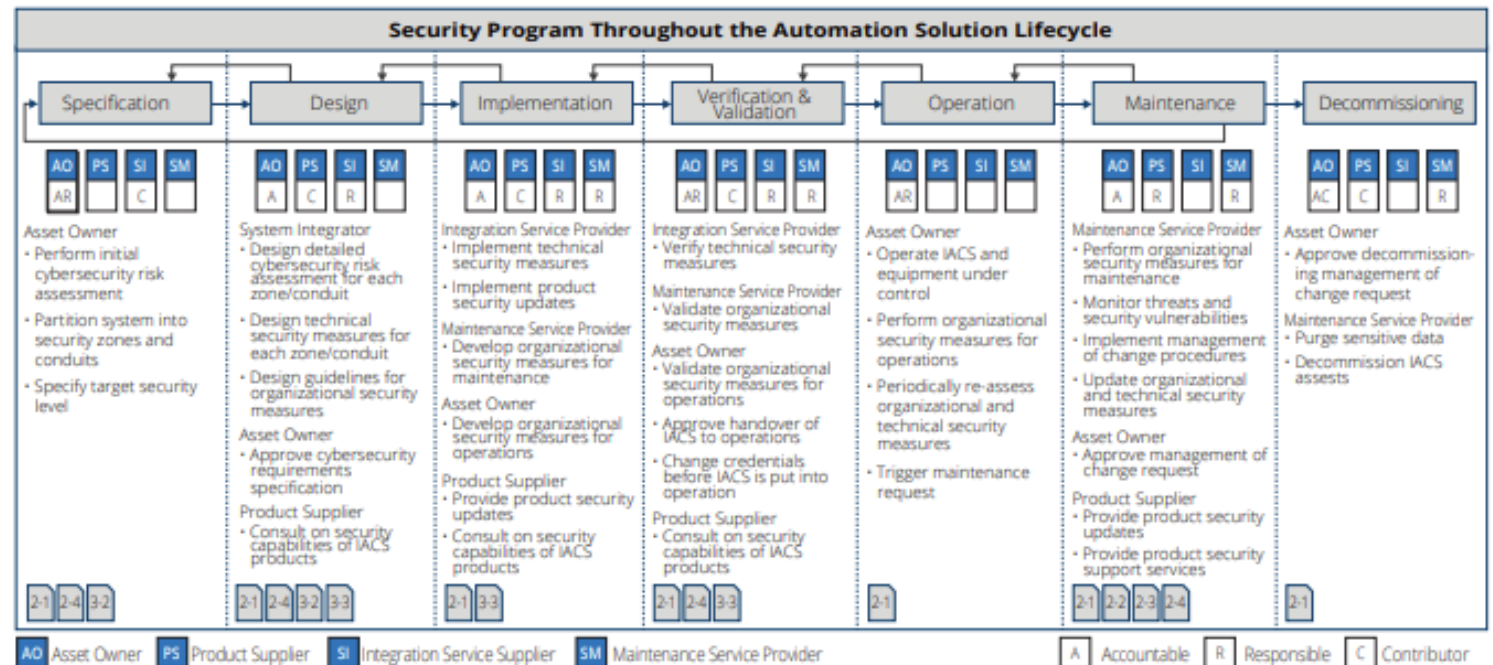


Figure 5: ISA/IEC 62443 Standards – Hierarchical



Build a Cyber Security Management System

USING PART 2 - 1

Definition of a CSMS

Cyber Security Management System

Program designed by an organization to maintain the cyber security of the entire organization's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the industrial automation and control systems side of the organization

Overview of CSMS Elements

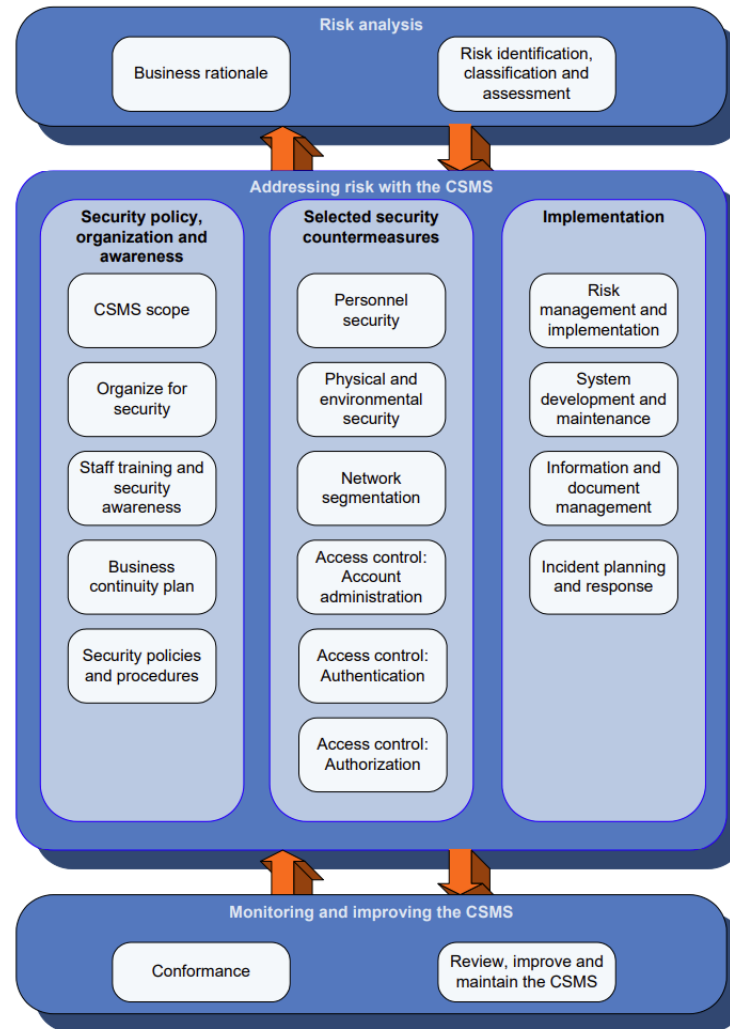
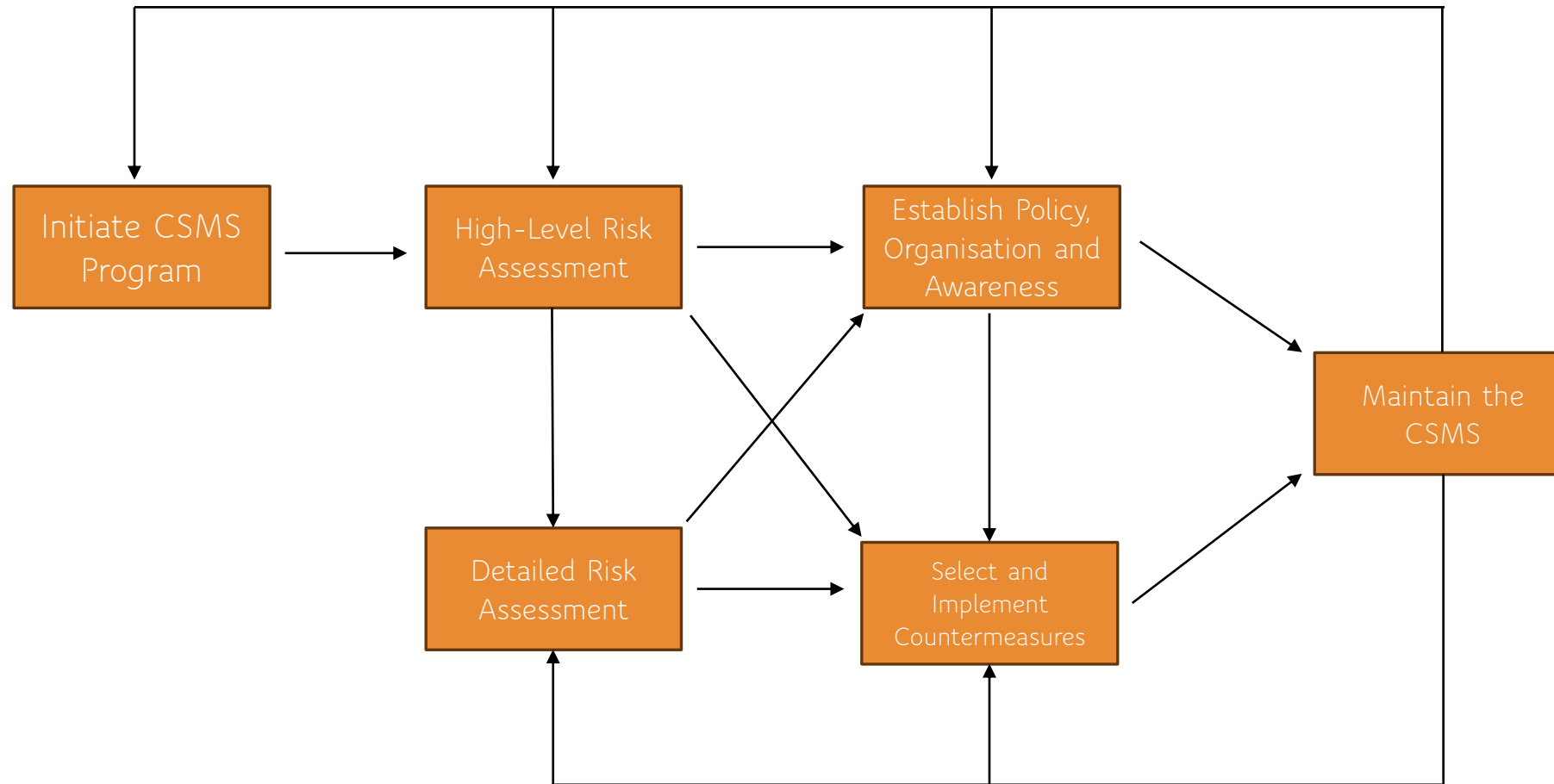


Figure 1 – Graphical view of elements of a cyber security management system

Process to Develop CSMS (Annex B)



Establish Policies and Procedures

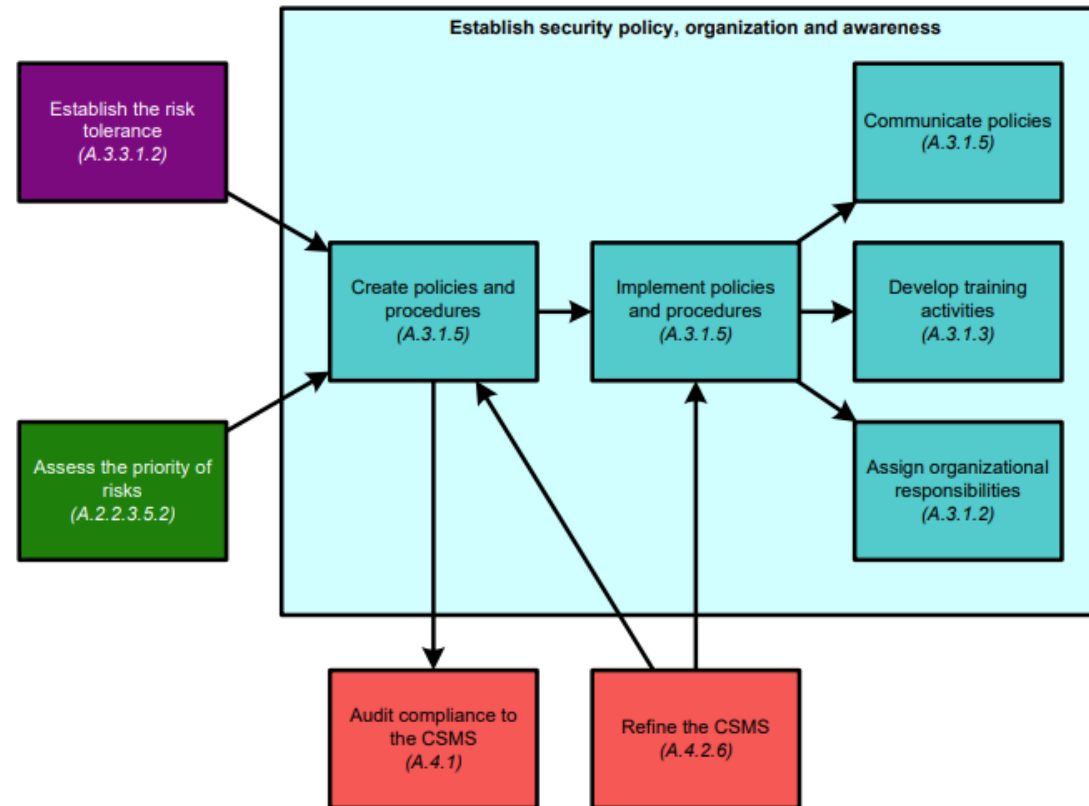


Figure B.5 – Activities and dependencies for activity: Establish policies and procedures

Application for a Project

USING PART 3-2 AND PART 3-3

Zone and Conduit Definitions

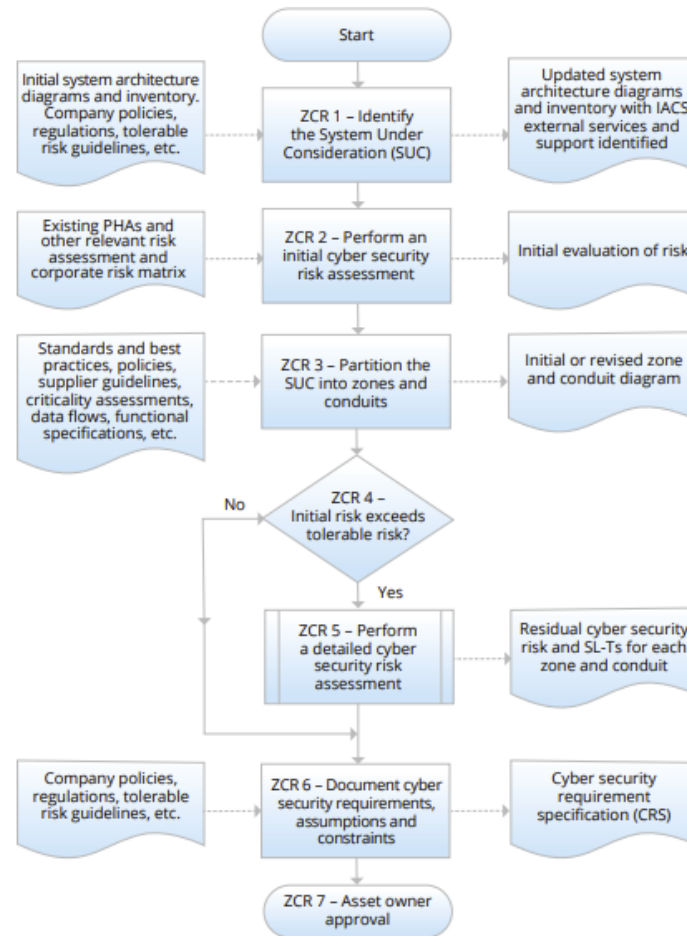
Zone

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

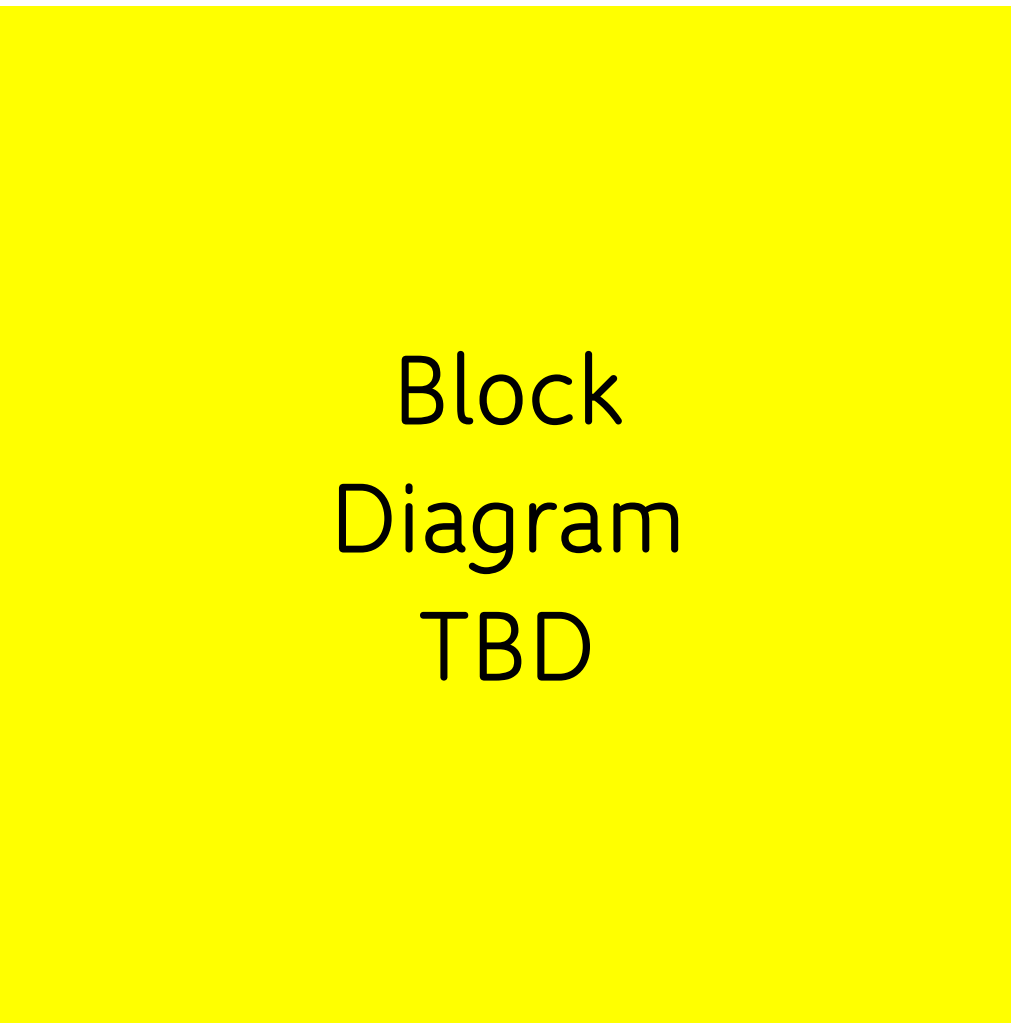
Logical grouping of communication channels that share a common security requirements connecting two or more zones

Overview of Part 3-2 - HLRA



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



Block
Diagram
TBD

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.

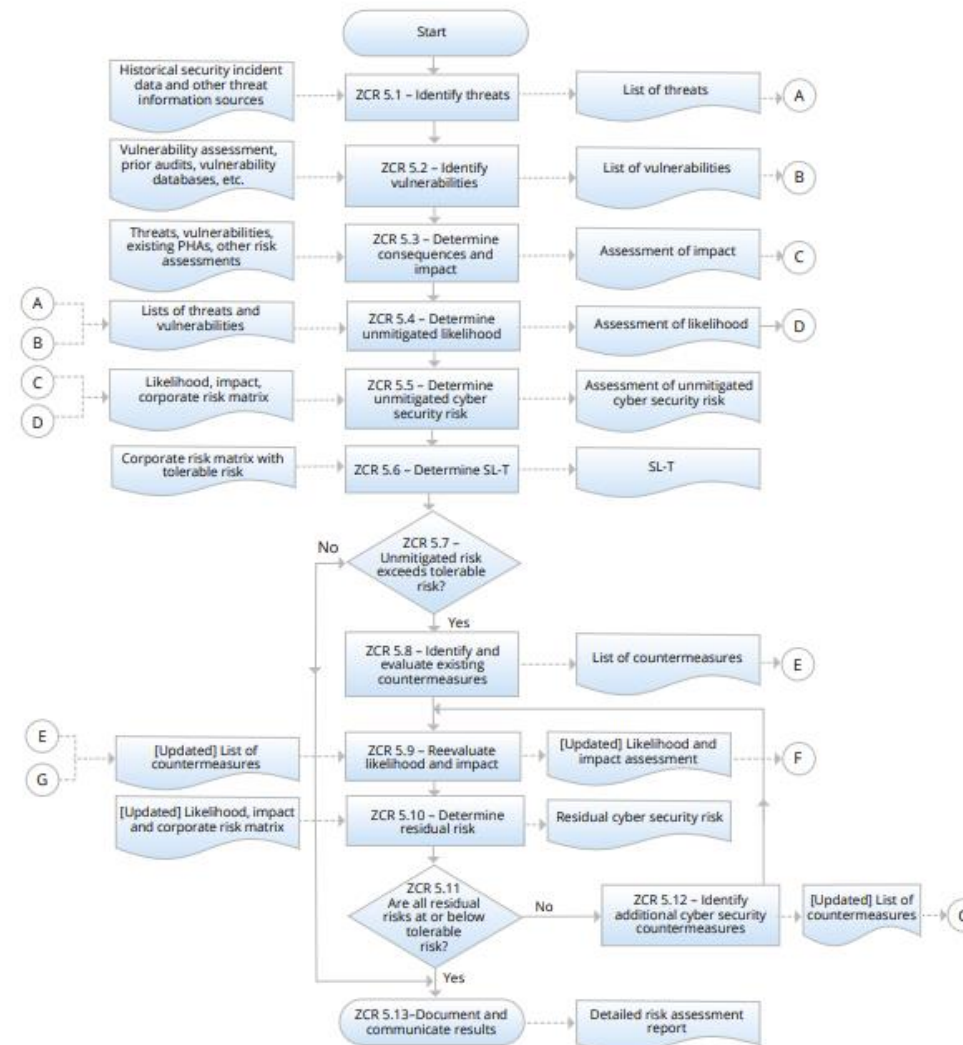
SL-1 Prevent the unauthorized disclosure of information **via eavesdropping or casual exposure**

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**

Overview of Part 3-2 – Detailed Risk Assessment



Example 62443 Risk Workbook

		Threat Scenario		Consequence																
	Threat Source	Threat Action	Vulnerabilities	Consequence Description	Impact					UTL	Risk	SL-T	Countermeasures	MTL	Risk	Recommendations	ATL	Ris		
Zone					S	E	F	R	Max											
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 default 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

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)

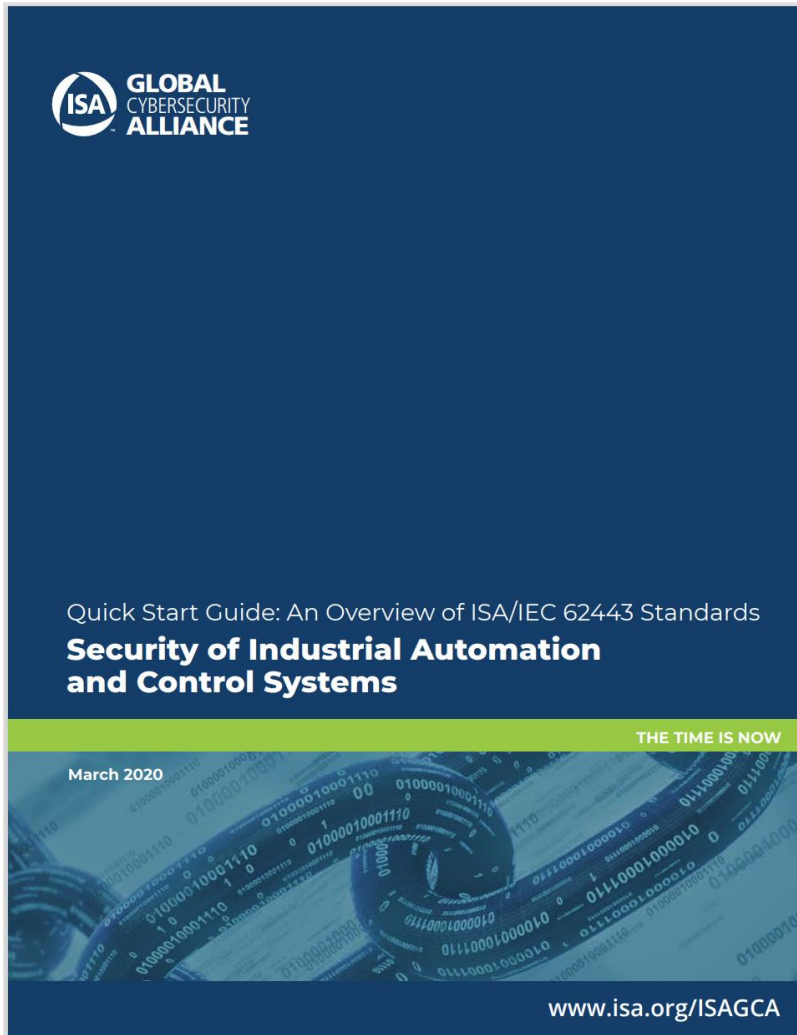
FR 7 – Resource Availability (RA)

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 (RDE)					
SR 5.1 – Network segmentation		9.3 SR 5.1 – Network segmentation 9.3.1 Requirement <p>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.</p>			
RE (1) Physical network segmentation					
RE (2) Independence from non-control system networks		9.3.2 Rationale and supplemental guidance <p>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.</p>			
RE (3) Logical and physical isolation of critical networks					
SR 5.2 – Zone boundary protection					
RE (1) Deny by default, allow by exception		<p>Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.</p>			
RE (2) Island mode		9.3.3 Requirement enhancements <p>(1) Physical network segmentation</p> <p>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.</p>			
RE (3) Fail close		<p>(2) Independence from non-control system networks</p> <p>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.</p>			
		<p>(3) Logical and physical isolation of critical networks</p> <p>The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.</p>			

Further Resources



<https://www.isa.org/membership>

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

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/>

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-39990 [Registration required.]

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



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>



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