

Hidden Risks in Sovereign Munitions Manufacturing

Applying AS IEC 62443 to Ensure Production Readiness from Competition to Conflict

Alfonso Sanzo – Principal Risk Engineer
GPA Engineering Pty Ltd

Consult
Engineer
Deliver

Ideas
Realised

GPA Engineering

Consult
Engineer
Deliver

Ideas
Realised

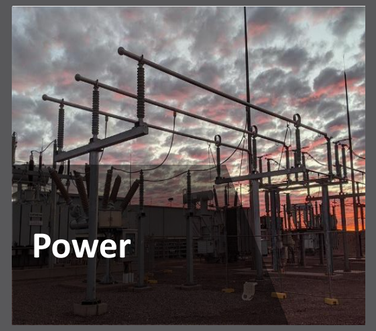
A highly experienced, multidisciplinary engineering and management firm, GPA has consulted and provided engineering, procurement and construction management (EPCM) services since 1987.

















410
employees

Head office
Adelaide

6
Australian
office
locations

100%
Australian owned

parari 2026 AUSTRALIAN EXPLOSIVE ORDNANCE SAFETY SYMPOSIUM
Proportional Safety – From Competition to Conflict
24-26 November 2026 National Convention Centre Canberra, Australia

GPA

Consult
Engineer
Deliver

Ideas
Realised

Strategic Question

Can Defence be confident that the automated manufacturing, storage and logistics systems it will rely upon during conflict have not already been compromised?

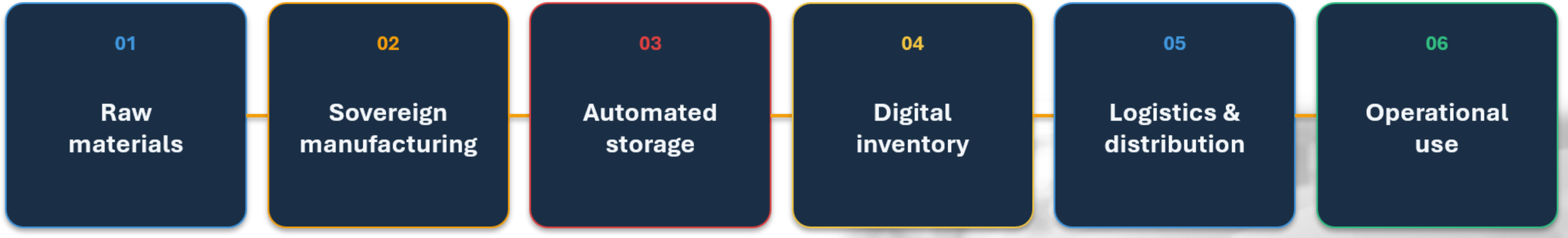
The risk may be embedded long before a facility enters operation.



The modern explosive ordnance lifecycle

Consult
Engineer
Deliver

Ideas
Realised



OT & IACS — potential attack surface at every stage

Global supply chains can introduce vulnerabilities before installation, commissioning or operational acceptance.

IT vs OT: a fundamental mismatch

Consult
Engineer
Deliver

Ideas
Realised

IT ENVIRONMENT

Protect data and digital services

Primary asset:	Data/ Information
High Priority:	Confidentiality
Consequence:	Data Loss/Information Leak / IT Services Disruption
Response Tolerance:	Minutes

OT ENVIRONMENT

Protect people, process and mission

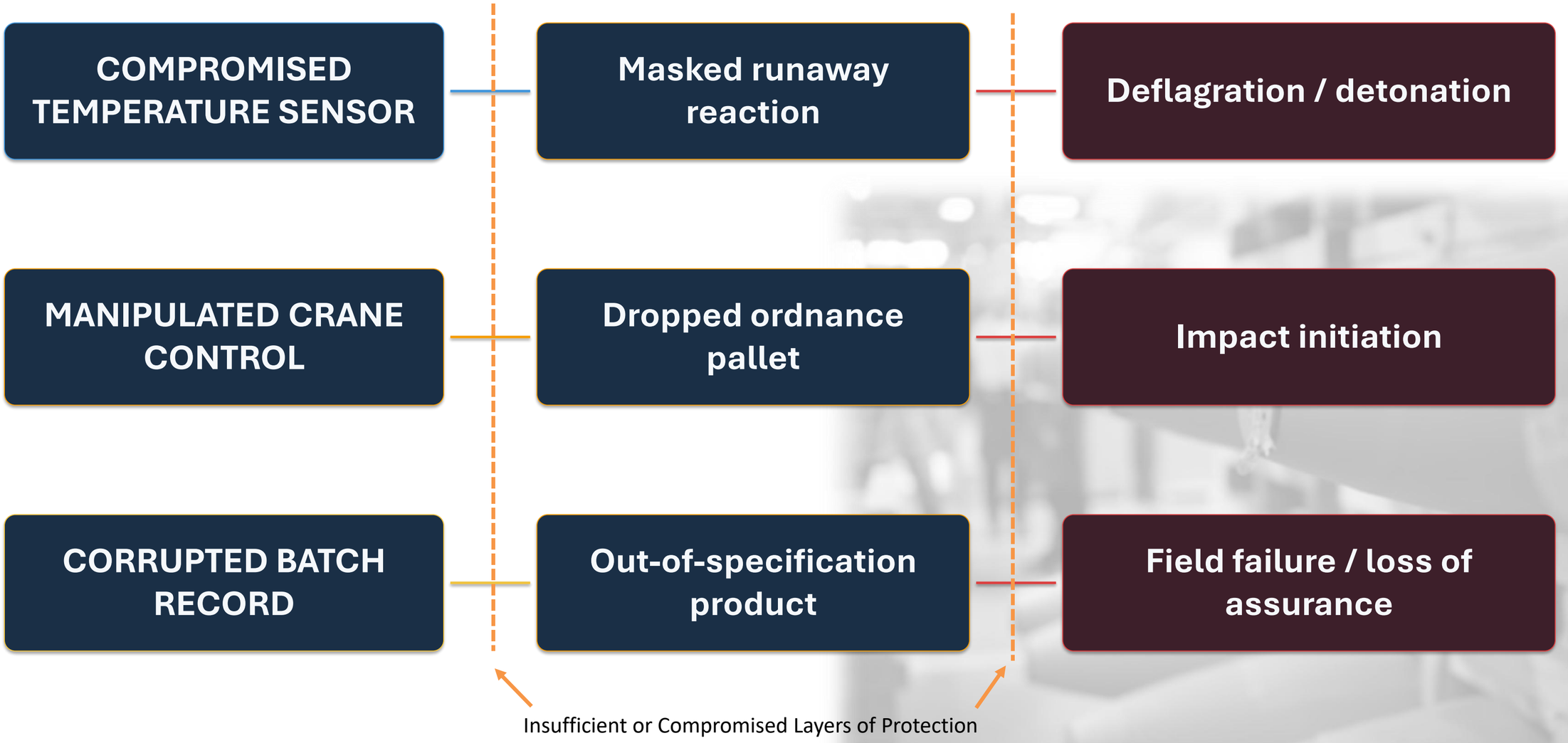
Primary asset:	Physical Process
High Priority:	Safety & Availability
Consequence:	Catastrophic event
Response Tolerance:	Seconds

parari 2026 AUSTRALIAN EXPLOSIVE ORDNANCE SAFETY SYMPOSIUM
Proportional Safety – From Competition to Conflict
24-28 November 2026 National Convention Centre Canberra, Australia

Cyber – physical risks in munitions

Consult
Engineer
Deliver

Ideas
Realised



Cyber – supply chain disruption risks

Consult
Engineer
Deliver

Ideas
Realised

01 SABOTAGE

Compromise causes a physical event

- Unsafe process conditions
- Loss of independent protection
- Potential injury, damage or destruction

02 DISRUPTION

Compromise undermines production confidence

- Production line stopped
- Inventory data corrupted
- Quality records cannot be trusted

During conflict, either outcome can severely impact combat effectiveness.

Introduction to AS/IEC 62443

The IEC 62443 series of standards is a comprehensive framework for securing Industrial Automation and Control Systems (IACS).

It addresses cybersecurity in industrial environments, providing guidelines for implementing security measures to protect against threats and vulnerabilities.

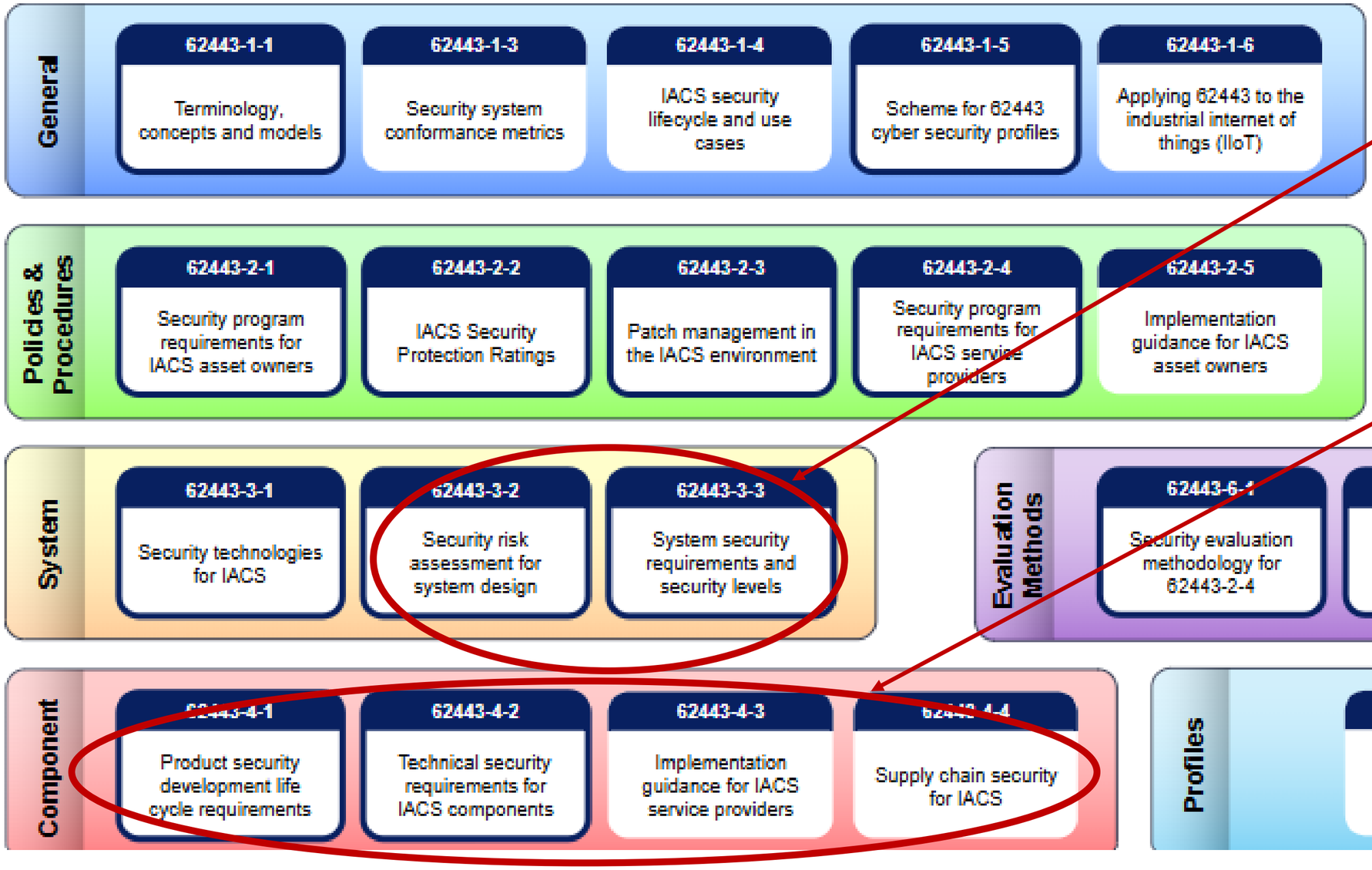
The standard is divided into several parts, each focusing on different aspects of industrial cybersecurity.



Introduction to AS/IEC 62443

Consult
Engineer
Deliver

Ideas
Realised



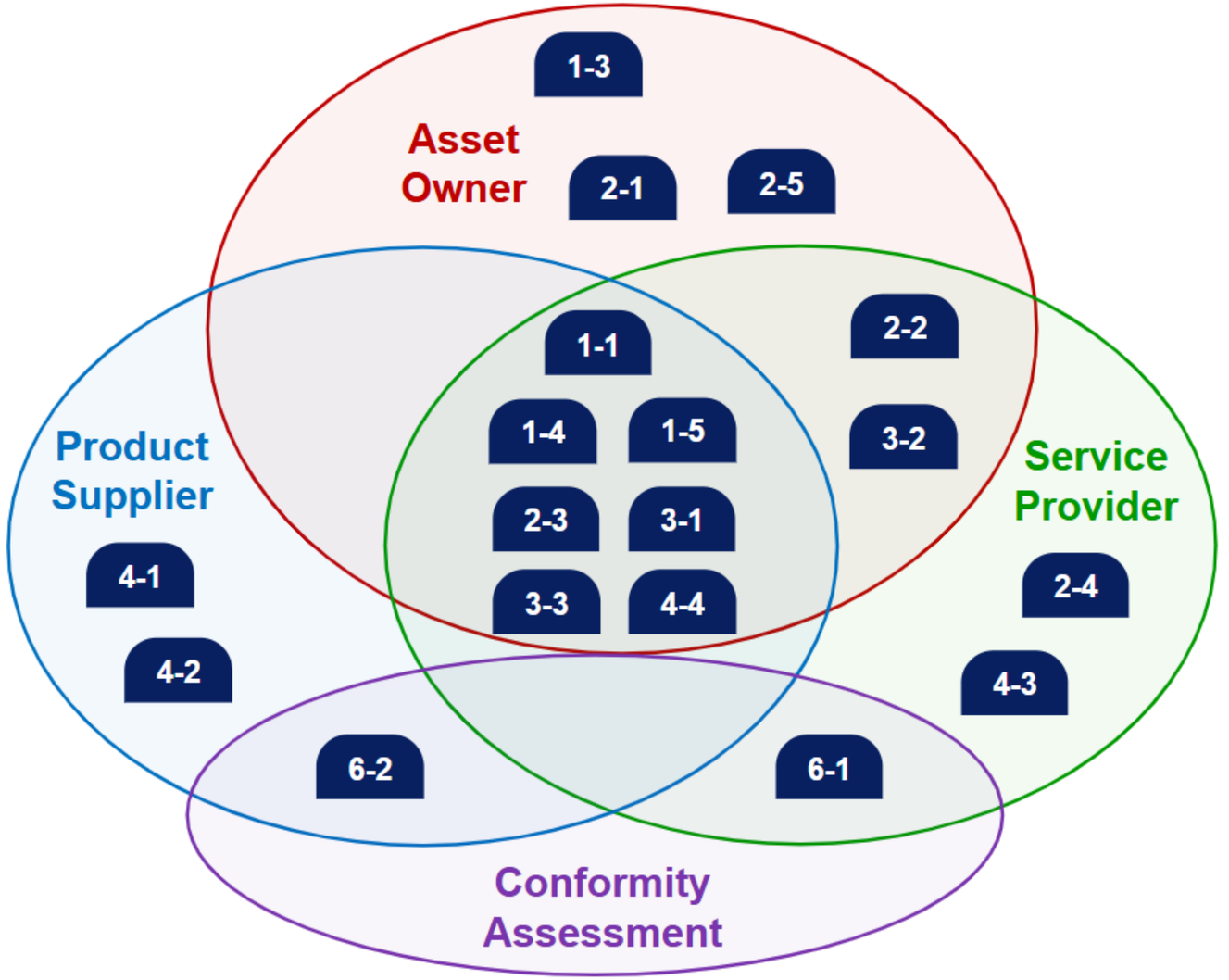
Concerned with Assessment of Risk & Assignment of SL-T – Impacts System Design & Specification

Requirements for Supply Chain – Impacts Procurement

AS/IEC 62443 – Application

The Cyber security risk assessment focuses on AS/IEC 62443 Part 3-2 as represented in the Systems Layer. IEC/ISA 62443 Part 3-3 then provides guidance on the Requirements to be applied based on the Security Level Target of the Zone or Conduit under consideration.

At the component level AS/IEC 62443 Part 4-1 and 4-2 provide guidance on the security requirements to be incorporated within actual IACS component designs and implementations. This allows component vendors to certify their products in terms of Security Level Capabilities.



AS/IEC 62443 Part 3-2 – Key Concepts & Terminology

IEC 62443-3-2 Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design. This part of the standard provides a framework to analyse IACS and OT networks for cyber security risks and provides the means to evaluate specific security risk levels. This standard introduces the concept of Zones and Conduits (ZC) for security risk assessment.

In assessing the design for residual risks IEC 62443 defines the following Security Level terms:

SL-T (Target Security Level)

- The desired level of security based on risk assessment and business needs.

SL-C (Capability Security Level)

- The maximum-security level that a component or system is capable of supporting.

SL-A (Achieved Security Level)

- The level that has been **actually implemented and validated** in the system or zone.



AS/IEC 62443 Part 3-2 – Key Concepts & Terminology

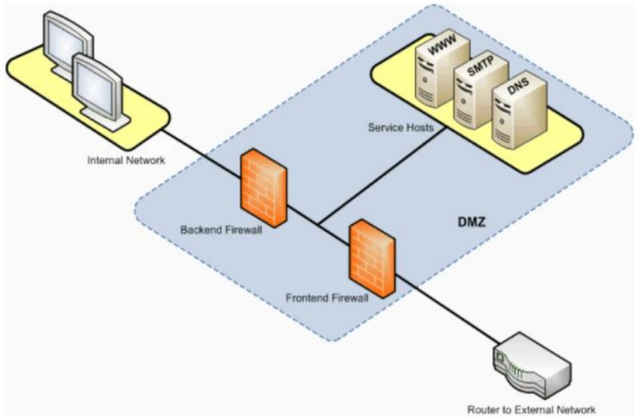
To undertake the review control system architectures, need to be divided into zones and conduits, defined as follows:

3.1.25 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 organization

3.1.3 conduit

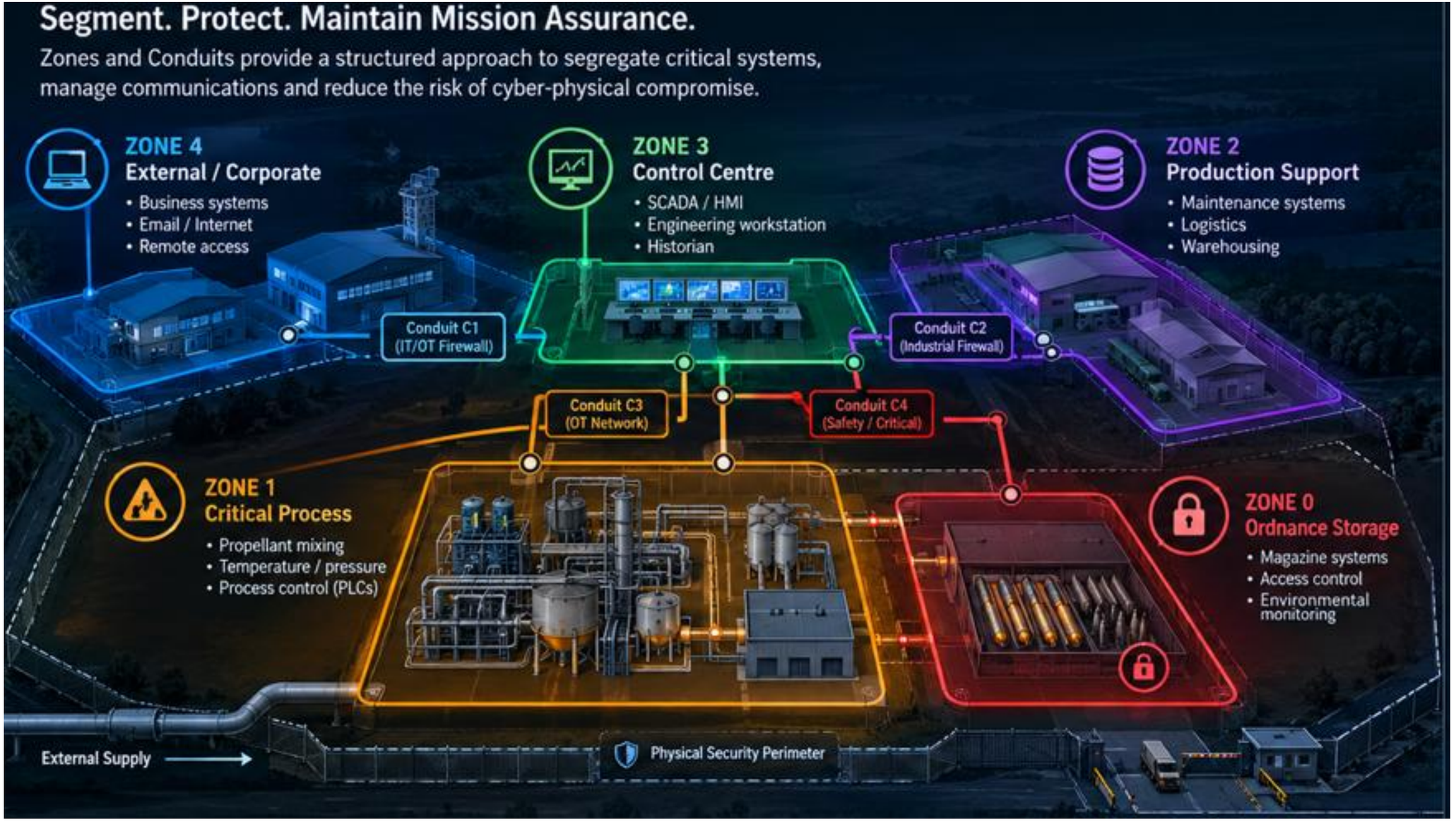
logical grouping of communication channels that share common security requirements connecting two or more zones



AS/IEC 62443 Zones & Conduits

Consult
Engineer
Deliver

Ideas
Realised



AS/IEC 62443 SL-T Definitions

The AS/IEC 62443 standard defines Security Levels (SLs) to describe the resilience of an Industrial Automation and Control System (IACS) against different types of threat actors.

These levels help organizations determine, through risk assessment as detailed in subsequent slides, the appropriate level of protection based on the capabilities and motivation of potential attackers **AND the consequences of a breach.**

Security Level	Definition by Requirement	Typical Threat Actor
SL 0	No specific security requirements or protection.	None (not secure)
SL 1	Protection against casual or coincidental violation.	Unintentional actors (e.g., accidents)
SL 2	Protection against intentional violation using simple means potentially with low resources, generic skills, and low motivation.	Basic hackers, curious insiders
SL 3	Protection against intentional violation using sophisticated means with moderate resources, ICS-specific knowledge, and moderate motivation.	Skilled insiders, organized crime
SL 4	Protection against intentional violation using sophisticated means with extensive resources, ICS-specific knowledge, and high motivation.	Nation-state actors, APTs

AS/IEC 62443 SL-T Defence Application Calibration

Consult
Engineer
Deliver

Ideas
Realised

Security Level	Definition by Consequence	Typical Threat Actor/Vector
SL 0	No specific safety implications. Non-significant disruption of "service" No loss of confidential Information.	None (not secure)
SL 1	No specific safety implications. Minor disruption of "service" able to be resumed in short duration. No loss of confidential Information.	Protection required against casual or coincidental violation.
SL 2	Potential safety implications but not of destructive nature. Disruption of "service" able to be resumed prior to impacting conflict response. Loss of confidential Information but consequence able to be contained.	Protection required against intentional violation using simple means potentially with low resources, generic skills, and low motivation.

Security Level	Definition by Consequence	Typical Threat Vector
SL 3	Safety implications potentially of a destructive nature. Disruption of "service" unable to be resumed prior to impacting mission. Loss of confidential Information that compromises effectiveness of conflict response.	Skilled insiders, organized crime
SL 4	Safety implications of a destructive nature. Disruption of "service" unable to be resumed prior to impacting mission and with long term impact. Loss of confidential Information that significantly compromises effectiveness or ability to execute mission.	Nation-state actors, APTs

The SL-T is determined based on the inherent risk a specific breach poses to the facility and/or mission. This requires an assessment of the consequences of a breach AND the inherent likelihood of the event if specific countermeasures are not applied.

AS/IEC 62443 SL-T Application Calibration

Consult
Engineer
Deliver

Ideas
Realised

Risk Assessment Matrix								
Consequence				Likelihood				
Safety Rating	People	Financial (EBIT)	Information Security	A Highly Likely (Multiple times in a year)	B Likely (Could occur within weeks to months)	C Possible (Could occur within months to years)	D Unlikely (could occur within the next few years)	E Highly Unlikely (could occur within decades)
Critical	1 – 3 fatalities or life threatening illness or total permanent disability to a small exposed group (<10 people).	>$50m to $200m	Loss of all/most confidential data. Unrecoverable data corruption. Loss of access to data or services for >3 days. Significant Intrusion.	25	20	15	10	5
Major	Serious injury or illness** to one or more persons, resulting in partial permanent disability.	>$20m to $50m	Significant loss of confidential data. Significant data corruption, but recoverable. Loss of access to data or services for 1 to 2 days. Significant Intrusion.	20	16	12	8	4
Serious	Serious injury or illness** to one or more persons not resulting in a permanent disability	>$5m to 20m	Loss of some confidential data. Some data corruption, but recoverable. Loss of access to data or services for < 24 hours. Intrusion, with some impact.	15	12	9	6	3
Moderate	Injury or illness to one or more persons resulting in medical treatment or outpatient treatment (i.e. not requiring admission as an inpatient) excluding treatment for a serious injury or illness	>$1m to $5m	Minimal to no loss of confidential data. No data corruption. Loss of access to data or services for < half business day. Intrusion, with no impact	10	8	6	4	2
Minor	A minor injury or illness resulting in first aid or no treatment	>$100k to $1m	No loss of confidential data. No data corruption. No loss of access to data or services. No intrusion.	5	4	3	2	1

The risk criteria and tolerable risk targets need to be agreed for each project application and are often embodied in the form of a risk matrix.

NON DEFENCE APPLICATION – EXAMPLE ONLY

Level	Description	Risk Acceptance Criteria
1	Very High	Not Acceptable
2	High Risk	Further Mitigation Required
3	Medium Risk	Acceptable
4	Low Risk	Acceptable

Inherenet Risk Score	SL-T Mapping
15 - 25	Very High
10-14	High Risk
3-9	Medium Risk
1-2	Low Risk

AS/IEC 62443 SL-T Defence Application Scalability

Particularly important to a defence application is that the required protection level (SL-T) can be considered as dynamic based on whether there is a normal competitive or peace-time context versus during a conflict.

In a competitive context a lower SL-T may be appropriate to a zone or conduit whereas this must shift to a higher or even SL-4 requirement during conflict.

During Peacetime Strategic Competition (Lower SL-T Posture):

- Zone 1 – Process Control: **SL-3** (even in peacetime, consequence of compromise is catastrophic; warrants elevated protection at all times)

During Transition to Conflict (Elevated SL-T Posture):

As strategic competition escalates toward conflict, we execute pre-planned escalation procedures:

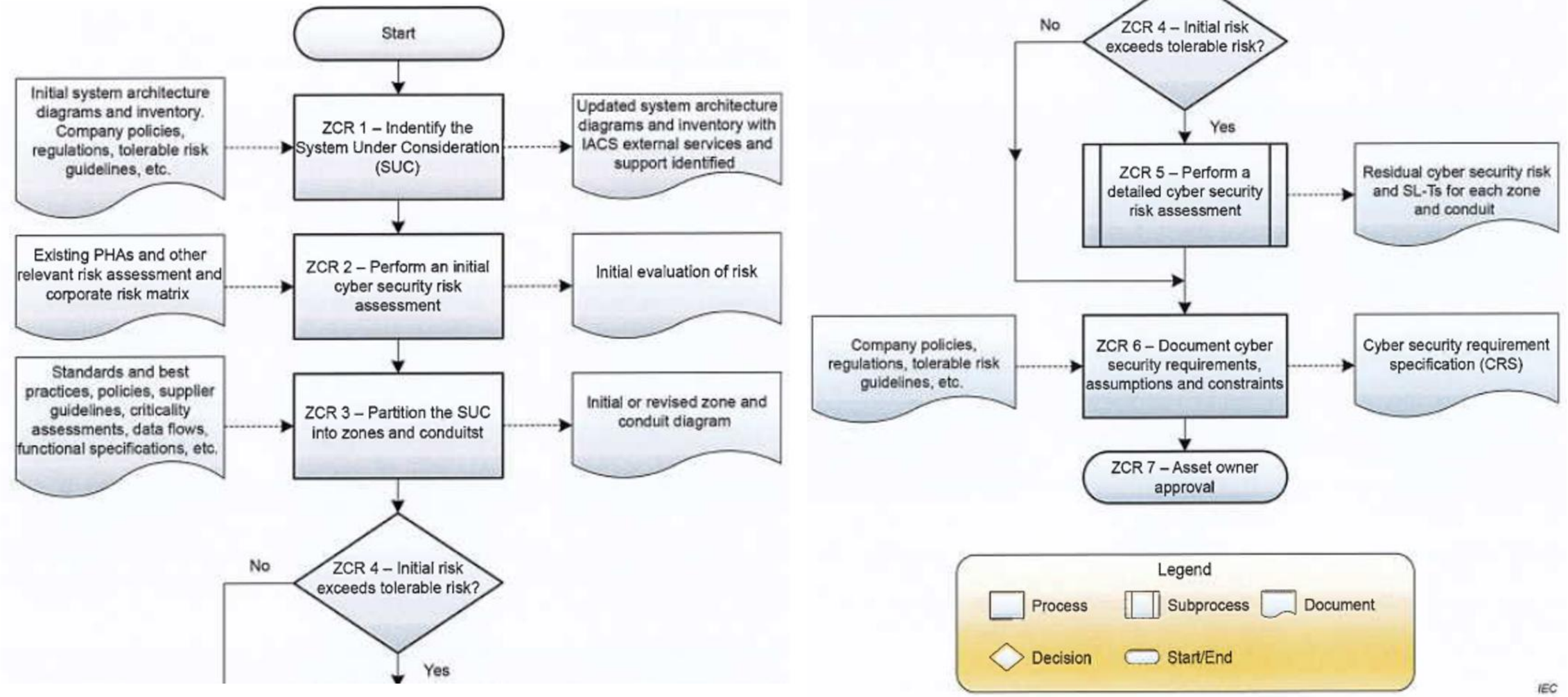
- Zone 1 – Process Control: **SL-4** — Air-gapping from all external networks; continuous monitoring activated; all remote access disabled; manual verification of safety-critical setpoints. The system design must allow the highest required SL-T to be achievable under a modified conflict operating posture.

AS/IEC 62443 SL-T Determination Workflow

Consult
Engineer
Deliver

Ideas
Realised

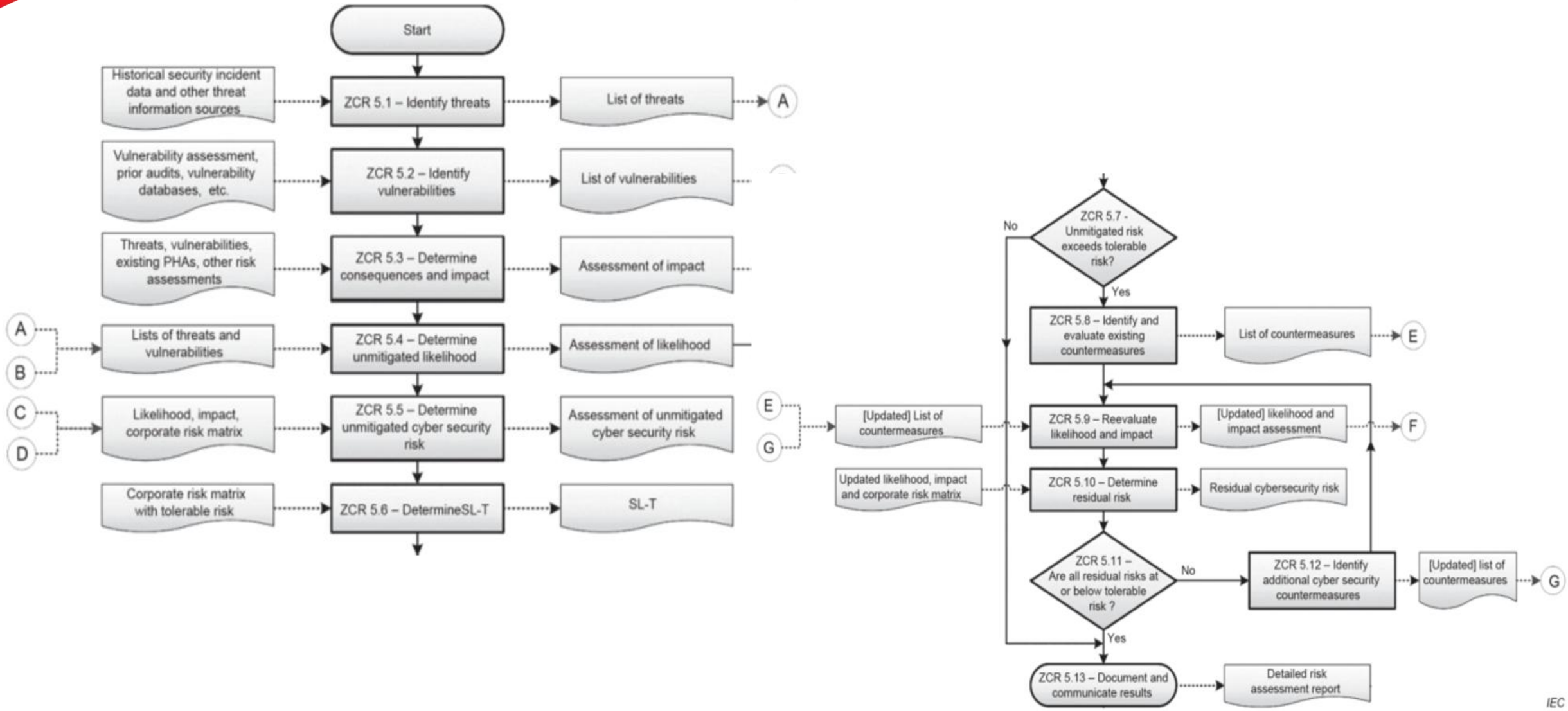
Figure 1 IEC62443-3-2 Workflow for conducting a cyber risk assessment



AS/IEC 62443 SL-T Risk Assessment Methodology

Consult
Engineer
Deliver

Ideas
Realised



AS/IEC 62443 Identifying the threats

How do we ensure we identify all threat sources and vulnerabilities?

- **Similar to all risk assessment processes in that the quality of the risk assessment will depend on the facilitation and competencies of the participants.**
- **Assembling the correct team.**
- **Skill of facilitator in developing a structured process for analysis.**
- **Use of a comprehensive set of prompts / guidewords to drive the discussions.**

Typical Threat Vectors

Threat Vector	Description	IEC 62443 Control
Unauthorized Access	Exploiting weak authentication or access control mechanisms.	SR 1.1 (Human user identification and authentication)
Malware Insertion	Via USB drives, infected software updates, or compromised third-party components.	SR 3.2 (Malicious code protection)
Network Intrusion	Attacks exploiting open ports, unsegmented networks, or weak perimeter defences.	SR 5.2 (Zone boundary protection)
Man-in-the-Middle (MitM) Attacks	Intercepting and altering communications between devices.	SR 3.1 (Communication integrity)
Denial of Service (DoS)	Overloading systems to disrupt operations.	SR 7.1 (Denial of service protection)
Insider Threats	Malicious or negligent actions by employees or contractors.	SR 1.3 (User account management), SR 2.1 RE (2) (Permission Mapping to roles)
Supply Chain Attacks	Compromised hardware or software from vendors.	SR 3.4 (Software and information integrity) SR 7.8 (Component Inventory)
Data Exfiltration or Manipulation	Stealing or altering sensitive operational data.	SR 4.1 (Confidentiality of information at rest or in transit
Exploitation of Software Vulnerabilities	Using known or zero-day vulnerabilities in ICS software.	SR 3.3 (Security function verification), SR 3.4 (Security function management)
Physical Attacks	Gaining physical access to devices or network infrastructure.	Physical access control – 62443-2-1 site security program.

Consult
Engineer
Deliver

Ideas
Realised

Threat Sources/Actors

Threat Source	Description
Human Actors	
External Actors	Individuals or groups outside the organization (e.g., hackers, cybercriminals).
Internal Actors	Employees, contractors, or partners with legitimate access.
Insiders (Malicious)	Authorized users who intentionally cause harm. Can be described as a Targeted Attack.
Insiders (Unintentional)	Users who accidentally cause security incidents (e.g., through negligence).
Competitors	Entities seeking industrial espionage or sabotage.
Nation-State Actors	Highly resourced and skilled attackers with political or strategic motives.
Hacktivists	Ideologically motivated attackers aiming to disrupt or defame.
Non-Human Sources	
Supply Chain	Vendors or third parties introducing vulnerabilities or malicious components.
Environmental Factors	Natural disasters, power failures, or other non-human threats.
System Failures	Hardware or software malfunctions that can compromise security.
Automated Threats	Malware, bots, or automated scripts targeting ICS environments.

AS/IEC 62443 SL-T Impact on Design

Once an SL-T is assigned to a subsystem, zone or conduit what is required in terms of the actual system design and implementation?

- **The SL-T will suggest the integrity and number of layers of protection required in the form of design features or countermeasures of a hardware, software or procedural nature required to meet the target integrity.**
- **Cyber security requirements are generally summarised as part of a cyber security specification that summarises the cyber related requirements**
- **Foundational Requirements (FR) are the basic security requirements that need to be considered for all security levels.**
- **The 7 Foundational Requirements (FR) are categorized as:**

Identification and Authentication Control (IAC)
Use Control (UC)
System Integrity (SI)
Data Confidentiality (DC)
Restricted Data Flow (RDF)
Timely Response to Events (TRE)
Resource Availability (RA)

AS/IEC 62443 SL-T Countermeasures

IEC 62443 System Requirements (SRs) and Requirement Enhancements (REs) mapped to Security Levels (SL1 to SL4) are summarised below.

Foundational Requirements (FR) are the basic security requirements that need to be considered for all security levels.

Foundational Requirement Name	Description
Identification and Authentication Control (IAC)	Ensures all users and devices are authenticated before access.
Use Control (UC)	Restricts access based on roles and responsibilities.
System Integrity (SI)	Protects against unauthorized changes and ensures system reliability.
Data Confidentiality (DC)	Safeguards sensitive information from unauthorized access.
Restricted Data Flow (RDF)	Controls communication paths to prevent data leakage.
Timely Response to Events (TRE)	Enables detection and response to security incidents.
Resource Availability (RA)	Ensures systems remain operational even under attack.

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)	✓	✓	✓	✓
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓
SR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for software process identity credentials			✓	✓
SR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
SR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users				✓
SR 1.8 – Public key infrastructure certificates		✓	✓	✓
SR 1.9 – Strength of public key authentication		✓	✓	✓
RE (1) Hardware security for public key authentication			✓	✓
SR 1.10 – Authenticator feedback	✓	✓	✓	✓
SR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
SR 1.12 – System use notification	✓	✓	✓	✓

AS/IEC 62443 SL-T Countermeasures

SRs and REs	SL1	SL2	SL3	SL4
FR 2 – Use control (UC)	✓	✓	✓	✓
SR 2.1 – Authorization enforcement	✓	✓	✓	✓
RE (1) Authorization enforcement for all users		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
SR 2.2 – Wireless use control	✓	✓	✓	✓
RE (1) Identify and report unauthorized wireless devices			✓	✓
SR 2.3 – Use control for portable and mobile devices	✓	✓	✓	✓
RE (1) Enforcement of security status of portable and mobile devices			✓	✓
SR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code integrity check			✓	✓
SR 2.5 – Session lock	✓	✓	✓	✓
SR 2.6 – Remote session termination		✓	✓	✓
SR 2.7 – Concurrent session control			✓	✓
SR 2.8 – Auditable events	✓	✓	✓	✓
RE (1) Centrally managed, system-wide audit trail			✓	✓
SR 2.9 – Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached			✓	✓
SR 2.10 – Response to audit processing failures	✓	✓	✓	✓
SR 2.11 – Timestamps		✓	✓	✓
RE (1) Internal time synchronization			✓	✓
RE (2) Protection of time source integrity				✓
SR 2.12 – Non-repudiation			✓	✓
RE (1) Non-repudiation for all users				✓

SRs and REs	SL1	SL2	SL3	SL4
FR 3 – System integrity (SI)	✓	✓	✓	✓
SR 3.1 – Communication integrity	✓	✓	✓	✓
RE (1) Cryptographic integrity protection			✓	✓
SR 3.2 – Malicious code protection	✓	✓	✓	✓
RE (1) Malicious code protection on entry and exit points		✓	✓	✓
RE (2) Central management and reporting for malicious code protection			✓	✓
SR 3.3 – Security functionality verification	✓	✓	✓	✓
RE (1) Automated mechanisms for security functionality verification			✓	✓
RE (2) Security functionality verification during normal operation				✓
SR 3.4 – Software and information integrity		✓	✓	✓
RE (1) Automated notification about integrity violations			✓	✓
SR 3.5 – Input validation	✓	✓	✓	✓
SR 3.6 – Deterministic output	✓	✓	✓	✓
SR 3.7 – Error handling		✓	✓	✓
SR 3.8 – Session integrity		✓	✓	✓
RE (1) Invalidation of session IDs after session termination			✓	✓
RE (2) Unique session ID generation			✓	✓
RE (3) Randomness of session IDs				✓
SR 3.9 – Protection of audit information		✓	✓	✓
RE (1) Audit records on write-once media				✓

AS/IEC 62443 SL-T Countermeasures

Consult
Engineer
Deliver

Ideas
Realised

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 4 – Data confidentiality (DC)	✓	✓	✓	✓
SR 4.1 – Information confidentiality	✓	✓	✓	✓
RE (1) Protection of confidentiality at rest or in transit via untrusted networks		✓	✓	✓
RE (2) Protection of confidentiality across zone boundaries				✓
SR 4.2 – Information persistence		✓	✓	✓
RE (1) Purging of shared memory resources			✓	✓
SR 4.3 – Use of cryptography	✓	✓	✓	✓



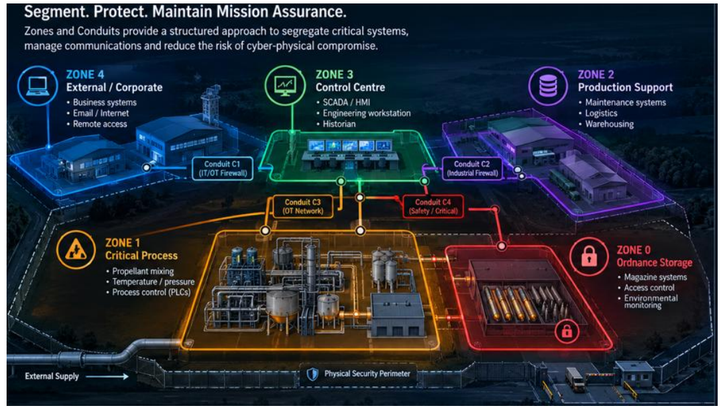
SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)	✓	✓	✓	✓
SR 5.1 – Network segmentation	✓	✓	✓	✓
RE (1) Physical network segmentation		✓	✓	✓
RE (2) Independence from non-control system networks			✓	✓
RE (3) Logical and physical isolation of critical networks				✓
SR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny by default, allow by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
SR 5.3 – General purpose person-to-person communication restrictions	✓	✓	✓	✓
RE (1) Prohibit all general-purpose person-to-person communications			✓	✓
SR 5.4 – Application partitioning	✓	✓	✓	✓
FR 6 – Timely response to events (TRE)	✓	✓	✓	✓
SR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
SR 6.2 – Continuous monitoring		✓	✓	✓

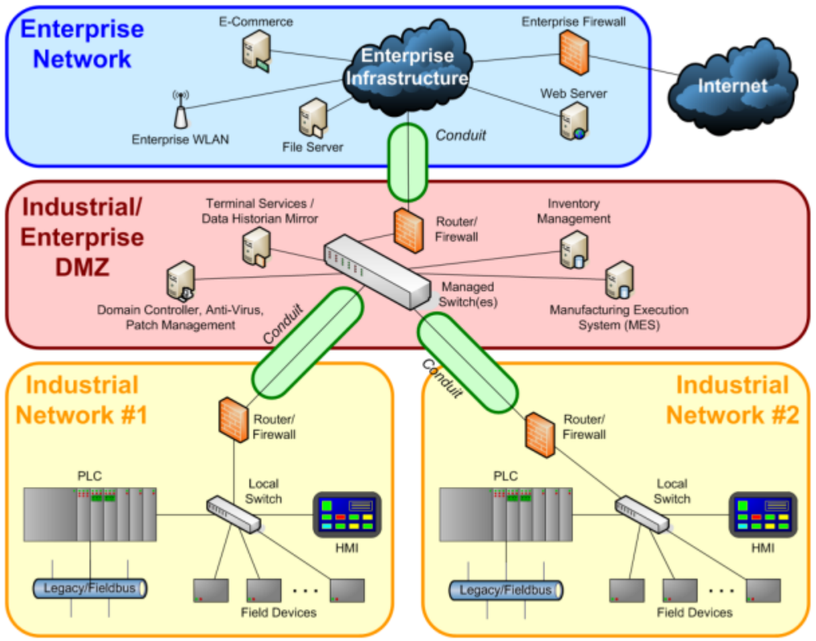
SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 7 – Resource availability (RA)	✓	✓	✓	✓
SR 7.1 – Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication loads		✓	✓	✓
RE (2) Limit DoS effects to other systems or networks			✓	✓
SR 7.2 – Resource management	✓	✓	✓	✓
SR 7.3 – Control system backup	✓	✓	✓	✓
RE (1) Backup verification		✓	✓	✓
RE (2) Backup automation			✓	✓
SR 7.4 – Control system recovery and reconstitution	✓	✓	✓	✓
SR 7.5 – Emergency power	✓	✓	✓	✓
SR 7.6 – Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings			✓	✓
SR 7.7 – Least functionality	✓	✓	✓	✓
SR 7.8 – Control system component inventory		✓	✓	✓

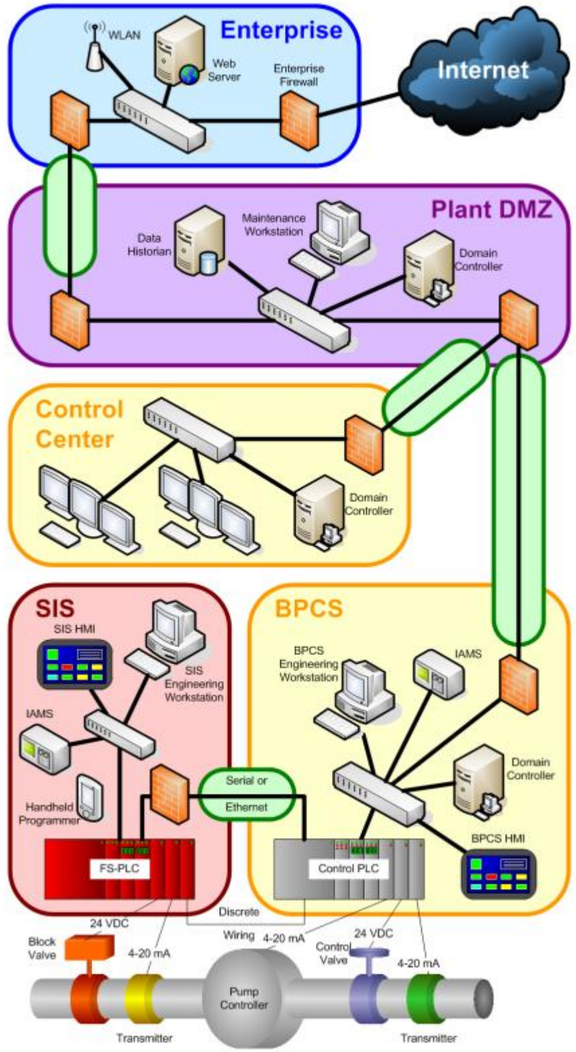
Industrial Application Example

Consult
Engineer
Deliver

Ideas
Realised





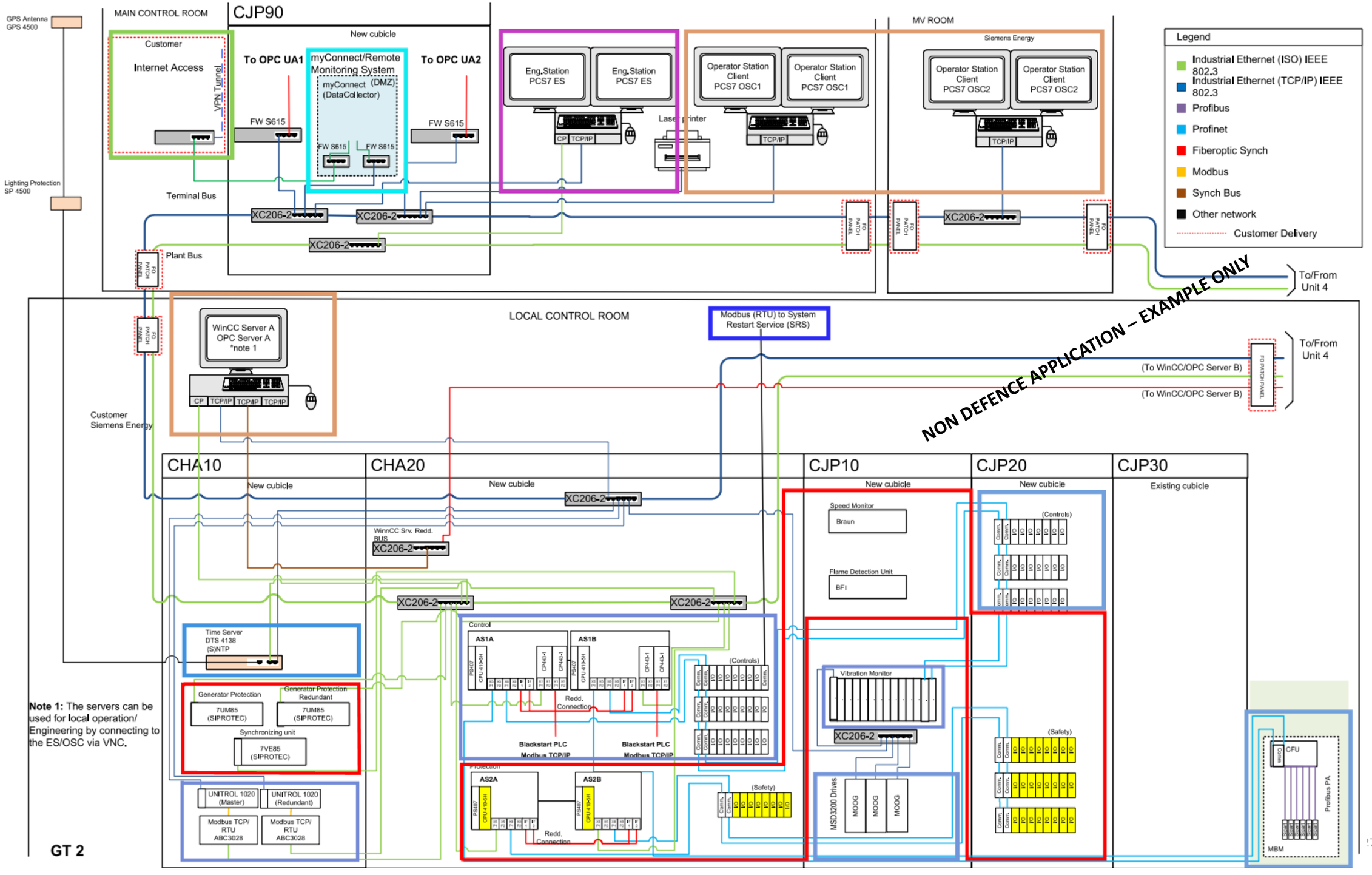


ZCR 1 Define the System Under Consideration (SUC)
In this case the design is mature and depicted on architecture drawing xyz-00-0001 Sht1 &2.

ZCR 2 Perform Initial Risk Assessment
An initial implicit risk assessment has been undertaken by Siemens to arrive at the architecture and configuration presented for review. Key equipment has been defined and partitioned into OT and IACS including Basic Process Control and safety Specific elements. Further OE has undertaken HAZOP, CHAZOP and LOPA studies that have identified credible consequences and impacts that are relevant to the IACS.

ZCR 3 Partition the SUC into zones and conduits
For the purpose of this risk assessment GPA has undertaken preliminary definitions of zones and conduits to enable the execution of a detailed cyber security risk assessment.

Worked Example – System Architecture



AS/IEC 62443 Assessment Template Example

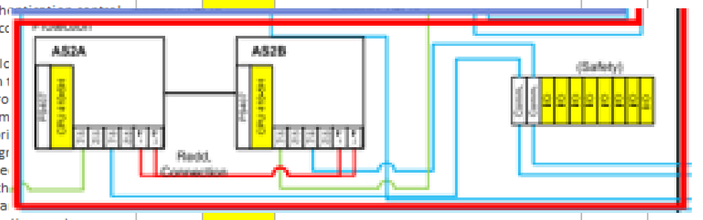
Consult
Engineer
Deliver

Ideas
Realised

Client Name	Client			Document Title	Document No.	Date	03/07/26	By	BAA
Client Project No.	-	GPA Project No.	260112	ICS Cyber Risk Assessment (Unit 2 and 4)	250112-LIS-001	Rev	A	Chkd	AS
Project Name	Upgrade Project							QA	LAH

SL-T=Security Level Target UTL=Unmitigated Threat Likelihood
MTL-Mitigated threat Likelihood ATL-Adjusted threat Likelihood

					Cyber Threat				Consequence / Impact														
Zone/ Conduit	Zone/ Conduit Desc.	Node/ Compon	Node/ Component Descriptio	Threat Vecto	Threat Source	Threat	Vulnerabilities	Consequence Descripti	Safe	Environ ment	Asse	Informatio n Secur	TAI	Ma	UTL	UTL rationale	Unmiti gat Ri	SL-T	Countermeasure(s)	MTL	Mitigated Risk	Recommendations/Comments/Actions	ATL	Adjested Risk
CR1	Z1 SIS1	GT Safety Instrumented System (SIS)	Controller	Unit SIS controller - AS2A and AS2B	Unauthorized Access, Data Exfiltration or Manipulation, Physical Attacks	Internal Actors, Insiders (Malicious)	Unauthorised change to the SIS logic by plugging in a laptop with OEMprogramming tools to the programming port on the SIS processor.	No specific vulnerability noted.	-Potential to compromise the SIS. -SIS is unable to bring	5-	3-	3-	2-			2-	Requires familiarity with OEMprogramming tools and the SIS logic used in the project. With tools available, online modification of the SIS controller is feasible. There is no maintenance/download inhibit d the programming port enabled. is compromised, the BPCS will remain active to ess variables within e limits.	10	SL-2	**Prevention -** SIS software authe (password) and cc management. SIS controller is lc enclosure within t Site access contro to the switchroom against unauthori A OEMsafety progr license is require provided under th software-based a (i.e., no USB drive licenses). **Response -** Video surviellance. SIS software are backed-up and recovery procedures readily available.					
CR2	Z1 SIS1	GT Safety Instrumented System (SIS)	Controller	Unit SIS controller - AS2A and AS2B	Malware Insertion, Exploitation of Software Vulnerabilities, Network Intrusion	Internal Actors	Unauthorised access to Plant Bus network used to make change to the SIS logic.	No specific vulnerability noted.									familiarity with amming tools and the SIS in the project. With ilable, online ion of the SIS controller is There is no nce/download inhibit is compromised, the BPCS will remain active to ess variables within e limits.	10	SL-2	**Prevention -** SIS software authentication control (password) and configuration management. Site access control measures apply to all locations from which the plant bus network can be accessed, protecting against unauthorized access. Spare ports on plant bus network switches are blocked. **Response -** SIS software are backed-up and recovery procedures readily available.	1-Highly Unlikely	5			
CR3	Z1 SIS1	GT OEMSafety Instrumented System (SIS)	Controller	Unit SIS controller - AS2A and AS2B	Supply Chain Attacks, Data Exfiltration or Manipulation	External Actors	Trojan software embedded within the safety application.	No specific vulnerability noted.										10	SL-2	**Prevention -** Reputable OEM and integrator; no third-party integrators involved. Procurement is conducted through verified Origin channels. SIS validation testing (FAT and SAT) will confirm the functionality of the safety system prior to return to service.	1-Highly Unlikely	5			
CR4	Z1 SIS1	GT OEMSafety Instrumented System (SIS)	Controller	Unit SIS controller - AS2A and AS2B	Malware Insertion	Insiders (Unintentional)	Accidental introduction of malware into the SIS controller.	No specific vulnerability noted.	Disruption in communication with other systems or internal detection by the SIS controller resulting in spurious trip of the turbine and productivity loss.	1-Minor	1-Minor	1-Minor	1-Minor	1	2	2-Unlikely		4	SL-1	**Prevention -** SIS software authentication control (password) and configuration management. Site access control measures apply to all locations from which the plant bus network can be accessed, protecting against unauthorized access. Spare ports on plant bus network switches are blocked. Refer engineering zone countermeasures listed under assessment CR21. **Response -** SIS configuration are backed-up and recovery procedures readily	1-Highly Unlikely	2	NOTE - Workshop considered the risk of unauthorized data manipulation via access to the Profinet communication between the SIS controller and I/O. However, this was deemed not credible, as the SIS I/O subnet is a dedicated, physically separated, proprietary connection.		



ZCR 4/5 **Initial & detailed cyber security risk assessment**

The scope of this workshop. Outcome shall be to determine and document the SL-T for each zone and conduit.

ZCR 6 **Document cyber security requirements**

Based on the SL-T for each zone and conduit, specific countermeasures shall be defined and documented as input to documentation that will fulfil the role of a Cyber security requirement specification, (CRS).

ZCR 7 **Approval Within Systems Engineering Framework**

NON DEFENCE APPLICATION – EXAMPLE ONLY

Supply Chain Integrity & Threats

"The final piece of the puzzle is supply chain integrity, and this is where Parts 4-1 & 4-2 of the standard become critical.

- **No specific countermeasure, either hardware, software or procedural will be effective if the component within our facility have been compromised in themselves.**
- **This becomes increasingly important as Australia establishes new sovereign manufacturing capability and introduces industrial equipment that may remain in service for decades.**
- **The drive for rapid deployment, cost effectiveness and efficiencies has led to increasing use of commercial off the shelf, COTS, equipment and services, supplied via a global supply chain implying a higher risk of vulnerabilities embedded within the system components.**

Aligning Cybersecurity with Explosive Safety Regulations

Attendees should take away actionable insights into three areas: ***conducting OT risk assessments for automated processes***, ***aligning industrial cybersecurity with explosive safety regulations***, and ***leveraging AS IEC 62443 to integrate and align with the facility's explosive safety case***.

- **The first step is to conduct OT-specific risk assessments. These are not IT risk assessments applied to OT — they must account for the physical consequences of cyber compromise, including explosive safety consequences.**
- **The second step is alignment. Your explosive safety case, under the Explosives Safety Regulatory Framework and DEOP 101 or state explosives and WHS regulations for industrial sites, should reference and incorporate OT cybersecurity as a contributing hazard. And conversely, your OT cybersecurity architecture should be informed by your explosive safety analysis — the zones with the highest consequence of compromise should receive the highest security levels.**
- **The third step is to embed this in your facility's operational readiness framework so that security posture can be escalated in step with the threat environment.**

Mission Assurance: Competition to Conflict

Consult
Engineer
Deliver

Ideas
Realised

DESIGN & BUILD

Assure at source

PEACETIME

Operate proportionately

ESCALATE

Activate rehearsed controls

CONFLICT

Protect safety & supply

ASSURANCE COST

Risk assessment and secure design

REMEDIATION COST

Retrofit after commissioning

COMPROMISE COST

Potentially immeasurable mission impact

Conclusions & Recommendations

I'll leave you with four recommendations:

Treat OT cybersecurity as an explosive safety discipline — integrate it into your safety cases, your hazard analyses, and your safety management systems.

Adopt AS IEC 62443 as the baseline standard for all new sovereign EO manufacturing, storage and logistics facilities — alongside the Defence security requirements, to fill the OT gap traditional IT frameworks weren’t designed for.

Mandate 62443-4 compliance in procurement — use contract specifications to require vendors to deliver components that meet defined security levels, and verify those claims through independent assessment.

Design for worst case SL-T, but operate at an appropriate SL-T during to achieve competitive benefits escalating during conflict — build the architecture and capability to o protect safety-critical zones at a high security from day one and implement scalable procedures to escalate posture as the strategic environment demands."

Thank You

Questions & discussion welcome!

GPA

Consult
Engineer
Deliver

Ideas
Realised

The intersection of explosive safety and cybersecurity — the conversation starts here.

Alfonso Sanzo | Principal Risk Engineer | GPA Engineering

GPA Engineering Pty Ltd.

Ph (08) 8299 8300
enquiries@gpaeng.com.au

gpaeng.com.au

Adelaide

Kaurna Country
121 Greenhill Road
Unley SA 5061

Ph (08) 8299 8300

Brisbane

Turrbal Country
Level 20
179 Turbot Street
Brisbane City QLD 4000

Ph (07) 3351 1300

Perth

Whadjuk Noongar Country
Level 3, Australia Place
15-17 William St
Perth WA 6000

Ph (08) 6370 5600

Darwin

Larrakia Country
Tenancy 404-2 Bldg. 4
631 Stuart Highway
Darwin NT 0800

Ph (08) 8299 8300

Melbourne

Boon Wurrung Country
Level 6
390 St Kilda Road
Melbourne VIC 3004

Ph (08) 8299 8300

Sydney

Gadigal Country
Level 1
418A Elizabeth Street
Surry Hills NSW 2010

Ph (08) 8299 8300