Cyber Security in Industry

An Overview of IEC 62443 (ISA99)

ProSalus
SAFETY CONSULTANTS

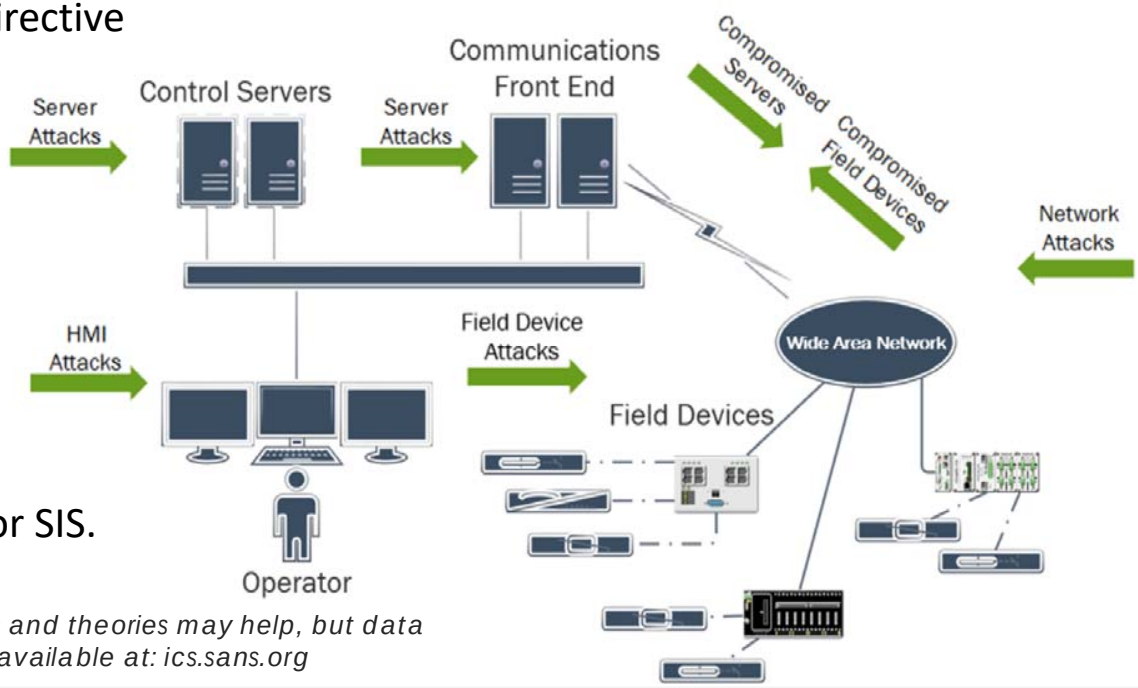
IACS Cyber security

- IACS operate industrial plant equipment and critical processes .
- The number of recorded incidents related to IACS have increased.
- Tampering with IACS can lead to:
  - Death, Injury, or Sickness;
  - Environmental releases;
  - Equipment damage;
  - Production loss / service interruption;
  - Off-spec / dangerous product;
  - Loss of trade secrets.

- IACS security is about preventing intentional or unintentional Interference with the proper operation of plant.

How Big is the Problem for IACS?

- Data from the Repository of Industrial Security Incidents (www.risidata.com) suggests their have been injuries and deaths as a result of IACS security incidents, but not all companies are publishing data, this will change with the introduction of the EU Directive on Network & Information Security (NIS).
- Not all threats originate from the internet – maintenance activities, software upgrades / patches, remote access, wireless, physical security and unauthorised access are just as big an issue for SIS.



Taken from "Pictures and theories may help, but data will set us free" Blog available at: ics.sans.org

SRA – IEC 61511-1 Clause 8.2.4

- Clause 8.2.4 states that a Security Risk Assessment (SRA) must be carried out to identify vulnerabilities in the SIS.
- The SRA output needs to include:
  - A description of the devices covered by the SRA;
  - A description of the identified threats;
  - The potential consequences and the likelihood;
  - Consideration of vulnerabilities and threats at all of the lifecycle phases;
  - The determination of requirements for additional risk reduction;
  - A description of, or references to information, on the security and compensating measures to be taken to reduce or remove the threats.

Legal Requirements

- Network and Information Systems (NIS) directive, 2016/1148. Concerns digital service providers and critical infrastructure. Guidance available from NCSC. (EU)
- Computer Misuse Act 1990. Concerns un access to modify information, including sniffing software. (UK)
- *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (US)*
- Numerous legal requirements in other legislation in both criminal and non-criminal law.

Achieving Security

- Ideally security will be achieved through the design of the process being inherently secure.
- When this is not possible security is achieved by introducing sufficient security countermeasures to reduce the risk from security incidents to an acceptable level.
- To ensure that the security countermeasures are sufficient the risk must be understood and determined.
- These security countermeasures can either be preventative, mitigative or detective in nature.
- This is achieved by performing a Security Risk Assessment (SRA).
- To achieve this adequate level of security there a number of guidance documents, including standards and frameworks.

Security Objectives

- A useful basis for security objectives is the C.I.A. triad.
  - **Confidentiality**
  - **Integrity**
  - **Availability**
- In the ICS environment, parts of this triade will be more critical and a balance for the facility must be found.

- Company-specific security objectives must be considered and documented.
- This includes the intended function of the facility

System Security UK

- OG-0086 – Cyber Security for IACS identifies IEC 61511-1 as Recognised Good Practice (RGP).
- Compliance with OG-0086 will contribute towards a suitable demonstration of compliance with UK legislation and COMAH ECI Operational Delivery Guide requirements for ALARP demonstration for the facility.
- The reference is related to IEC 61511-1 2nd Edition Clause 8.2.4, 11.2.12, and 11.7.3.2 requirements for a Security Risk Assessment (SRA).
- Both OG-0086 & IEC 61511 reference IEC 62443 as the applicable international standard as well as ISA-TR84.00.09-2013 – Security Countermeasures Related to SIS as the relevant standards for IACS SRA and implementation.

Cyber Security for Industrial Automation and Control Systems (IACS)

Open Government status
Open

Target audience

Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors

Contents

1

Framework for Cyber Security

- The OG-0086 approach is similar to the US NIST 800 Cyber security Framework of:

- The UK HSE guiding principles are:
- Protect, detect and respond - It is important to be able to detect possible attacks and respond in an appropriate and timely manner in order to minimise the impacts.
- Defence in depth - No single security countermeasure provides absolute protection as new threats and vulnerabilities can be identified at any time. To reduce these risks, implementing multiple protection measures in series avoids single point failures.
- Technical, procedural and managerial protection measures. Technology is insufficient on its own to provide robust levels of protection

NIST CSF Functions

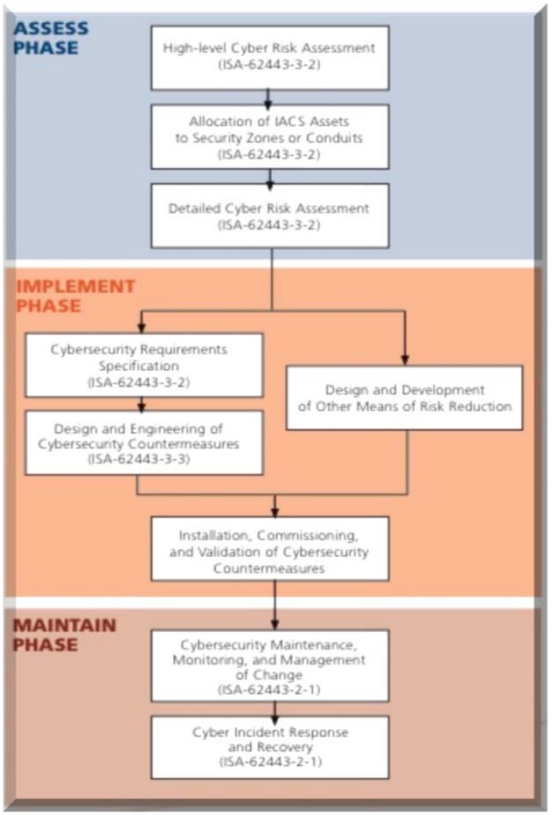
The NIST CSF is a popular framework as it is free to use unlike other frameworks, such as IEC 62443.

Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Asset Management ID.AM	Identity Management, Authentication and Access Control PR.AC	Anomalies and Events DE.AE	Response Planning RS.RP	Recovery Planning RC.RP
Business Environment ID.BE	Awareness and Training PR.AT	Security Continuous Monitoring DE.CM	Communications RS.CO	Improvements RC.IM
Governance ID.GV	Data Security PR.DS	Detection Processes DE.DP	Analysis RS.AN	Communications RC.CO
Risk Assessment ID.RA	Information Protection Processes and Procedures PR.IP		Mitigation RS.MI	
Risk Management Strategy ID.RM	Maintenance PR.MA		Improvements RS.IM	
Supply Chain Risk Management ID.SC	Protective Technology PR.PT			

IEC 62443 – Security for IACS

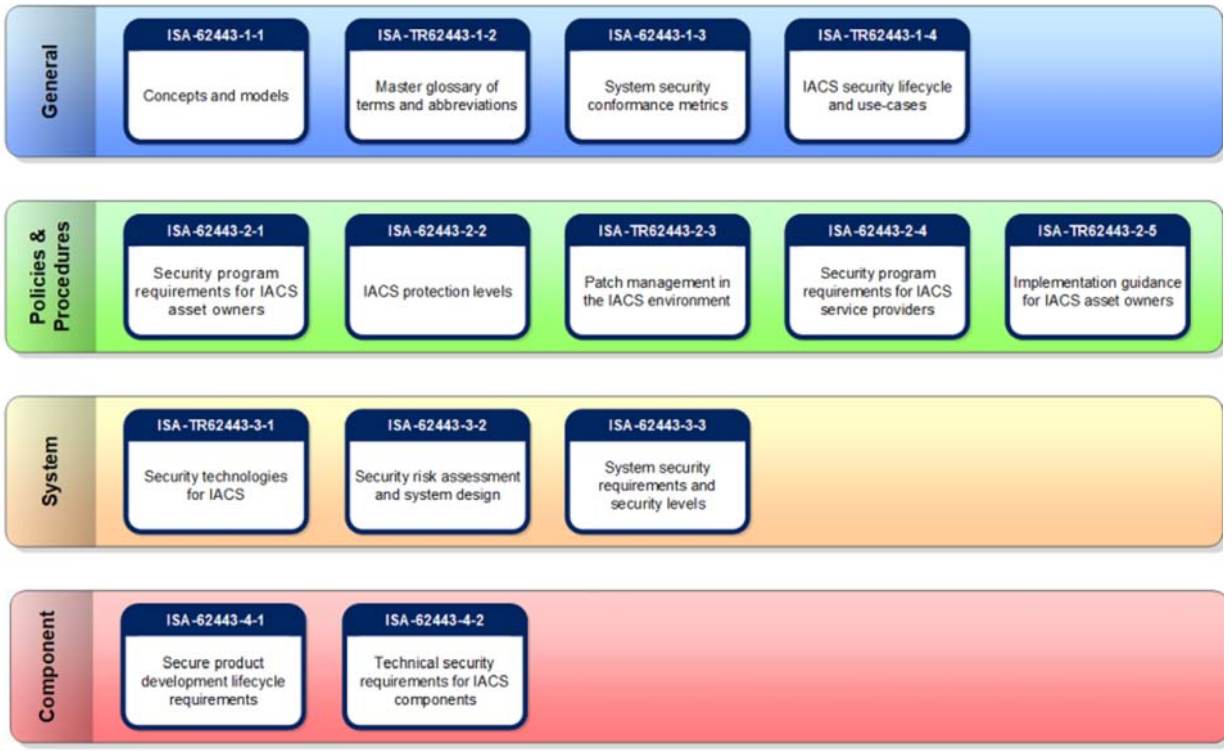
IACS & SIS must be secure from both physical or cyber damage as a result of malicious acts or accidental events that would impact on the ability to maintain functional and safety integrity on demand.

To prevent both physical and cyber damage the Security Risk Assessment (SRA) and risk control measures must be based on a mix of technical, procedural and managerial protection measures taken from the guidance in IEC 62443 and in ISA TR84.00.09.



IEC 62443 – Security for IACS

The Hierarchy of the IEC 62443 – Security for IACS Standards, several are still under development at this time

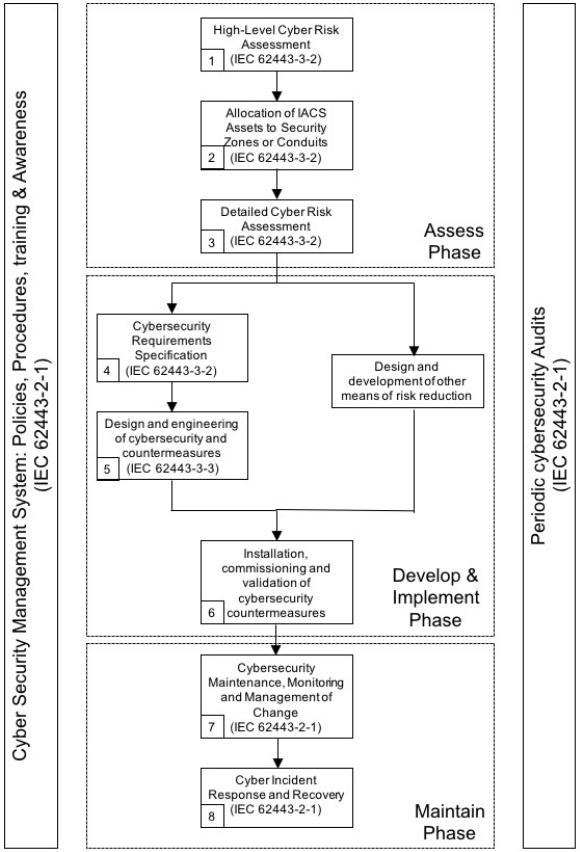


Security Management System

- As a fundamental part of any effective Security Management System (SMS), the results from the Security Risk Assessment (SRA) can be used to develop, improve or maintain the current SMS.
- In order to maintain the reduced level of the treated risk, a SMS should be in place. Without an effective SMS the risk will not be effectively treated, as such an incident is more likely and there is a possibility of regulatory consequences.
- There are a number of standards and guidelines which will aid in the creation of this management. This includes:
  - IEC 62443-2-1 – The ICS standard for the creation and maintenance of the Security Management System (CSMS).
  - ISO/IEC 27001 – A general IT standard detailing the requirements for the creation of a Information Security Management System (ISMS).
  - NIST Cybersecurity Framework (CSF)
  - IEC 61508 – A general standard revolving around functional safety, but details the creation and maintenance of a management system.
  - IEC 61511 – A process specific standard revolving around functional safety, but details the creation and maintenance of a management system.

IEC 62443 Security Lifecycle

- Once the SRA has been completed the later activities can be carried out:
  - Management of Change of the facility - ensuring no changes are implemented where the impact is either unknown or will have a detrimental impact to the facility.
  - Ensure some form of Incident response and monitoring is in place on the facility.
    - Information gathered during this stage can be used for later SRAs, as it represents the threats and vulnerabilities that are present on the site and will aid in the deciding the likelihood.



ProSalus SAFETY CONSULTANTS

Cybersecurity Frameworks

- An advantage of following a cybersecurity framework is that it is likely that all required steps will be completed. However, unless audited by conducted effectively there is no guarantee of its effectiveness.
- The three most common frameworks are:
  - IEC 62443
  - ISO/IEC 27001
  - NIST Cybersecurity Framework (CSF)
- There is a framework released by CPNI and CESG “Security for Industrial Controls Systems (SICS)” available from NCSC.
- Further to this IEC 61511 should be considered, for any implemented management systems.

What is an Asset Inventory?

- An asset inventory is a register of all assets on the site.
- All in scope assets are considered an asset and should be recorded in the asset inventory.
- The facility owner should maintain the register and ensure that it is kept up to date and that it covers all IACS hardware and software.
- Asset Inventory is a requirement of a number of standards including IEC 61511 with respect to devices used for Safety Instrumented Systems (SIS).
- To ensure that the register is kept up to date the register should be included in the facility Management of Change (MOC) system.
- As such any changes in either hardware or software configuration must be subjected to MOC, strictly controlled and documented, including logs, to avoid compromising ongoing risk management.

What is the purpose of an Asset Inventory?

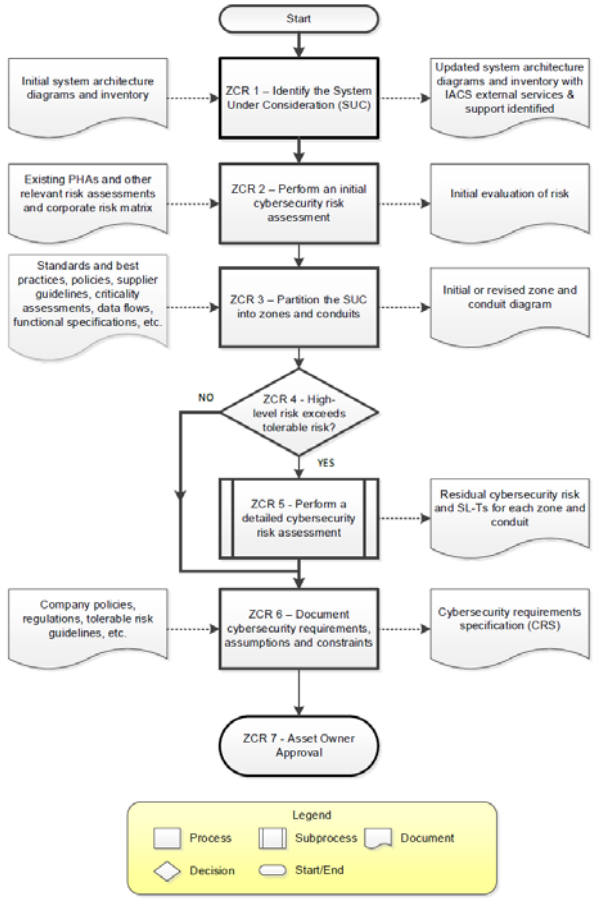
- It is vital that all assets present on the site are known, and that all records, including diagrams, are **kept up to date and accurate.**
- Assets pose both a **benefit and a vulnerability**, and may even introduce hazards themselves.
- The asset inventory is commonly part of the “Defining the IACS” activities. This activity is a requirement of IEC 61511 and in the UK HSE OG-0086, a benchmark standard in the COMAH Inspection of Electrical, Control and Instrumentation Systems at COMAH Establishments (EC&I).
- There are a number of Nation-specific legislative requirements which must be considered by organisations e.g. the German IT Security Law, requiring a Cyber Security Management System (CSMS) requiring all assets on site to be recorded.

How does the Asset Inventory relate to SRA?

- The Process Hazard Analysis (PHA) identifies the hazardous scenarios that plant operations present when a failure of equipment occurs.
- To identify cyber risk we need to identify the assets that present an exploitable risk.
- The asset inventory is a key tool in this process.
- Effective risk assessment is dependent upon a complete, accurate asset inventory.
- For the purposes of Cyber Risk Assessment it is necessary to ensure that the following information is available to ensure its usefulness in the High-Level SRA and the Detailed SRA.

Security Risk Assessment (SRA) Process from EN 62443-3-2

- The first major step in the SRA process involves the High-Level SRA. This process entails the scoping of the System under Consideration (SuC) and the actual performing of the High-Level SRA.
- These two steps are connected, as the SuC is the assets, systems and processes which will be assessed during the course of the SRA.



ProSalus SAFETY CONSULTANTS

High Level SRA:
Connection between SRA and PHA

- Risks are identified by reviewing the HAZOP and examining completed Functional Safety Assessments.
- Identified risks will be examined for assets that may be exploited leading to a security event or incident that could have a detrimental impact on the facility.
- This process is performed by collecting all hazardous scenarios that contain exploitable assets and inputting these scenarios into the High-Level SRA form.
- A number of PHA tools now contain the ability to indicate whether a scenario involves an exploitable asset or not. (If this was not addressed in the PHA it should be completed prior to the SRA).

Causes and consequences

High-Level Security Risk Assessment (SRA)

IEC 62443-2-1 Clauses 4.2.3.1-14 Requirement

- The organisation shall perform a high-level and detailed cybersecurity risk assessment of the System under Consideration (SuC), for example the control and safety instrumented system for a processing unit.
- The SuC will be presented as a System or Network diagram for the purposes of the SRA, but, it will also be necessary to provide the plant P&ID's so that the PHA can be correctly interpreted.
- This assists in identifying the worst-case unmitigated risk that the SuC presents to the facility.

Determining the Cyber Risk

- The cyber risk is determined by considering the Threat, the Vulnerability and the Consequence.

$$\boldsymbol{Risk = Threat\ x\ Vulnerability\ x\ Severity}$$

- This formula is conceptual and has no mathematical basis.
- The most effective way to ensure security is to design the cyber risk out, giving the facility inherent security.
- However, to do this the risk must be determined and analysed.

High-Level Security Risk Assessment (SRA) Flow Diagram

This is a basic diagram showing a typical process in completing a High-Level SRA and completing the High-Level SRA form show earlier.

Example of a High-Level SRA form

Hazardous Scenario	Asset	Asset Description	Threat Source	Threat Vector	Vulnerability	Countermeasure	Consequence	Severity	Likelihood	Risk / SL	Comments

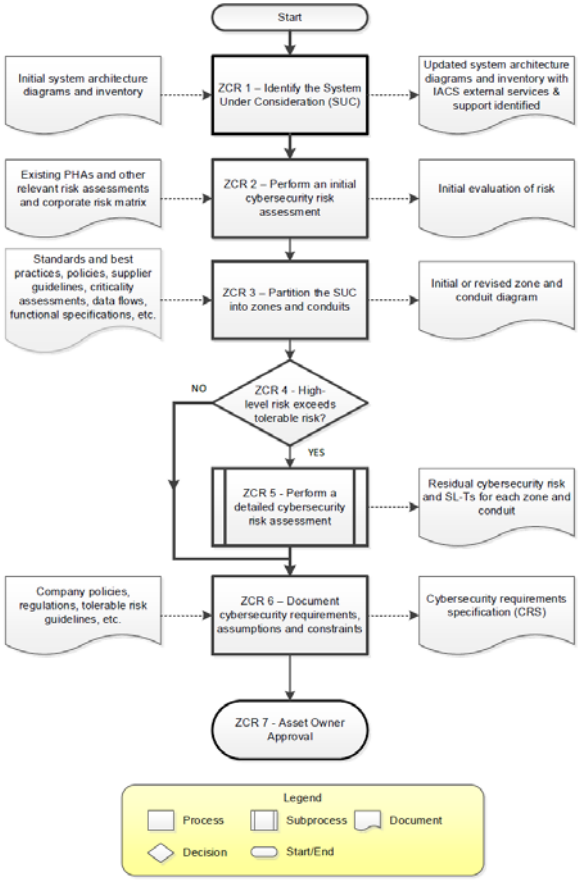
Example of a Security Risk Matrix

Likelihood		Consequence				
		Minor Problem easily handled by normal day to day processes	Some Disruption Possible (e.g., damage between $500K and $1 Million)	Significant Time & Resources Required (e.g., damage between $1 Million and $10 Million)	Operations Severely Damaged (e.g., between $10 Million and $25 Million)	Business Survival is at Risk (e.g., damage > $25 Million
Likelihood	**Almost Certain** (e.g., Greater than 90%)	High	High	Extreme	Extreme	Extreme
	Likely (e.g., Between 50% and 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (e.g., Between 10% and 50%	Low	Moderate	High	Extreme	Extreme
	Unlikely (e.g., From 3% to 10%)	Low	Low	Moderate	High	Extreme
	Rare (e.g., < 3% Chance)	Low	Low	Moderate	High	High

Example of a 5 x 5 Risk Matrix taken from IEC 62443-3-2

Security Risk Assessment (SRA) Process from EN 62443-3-2

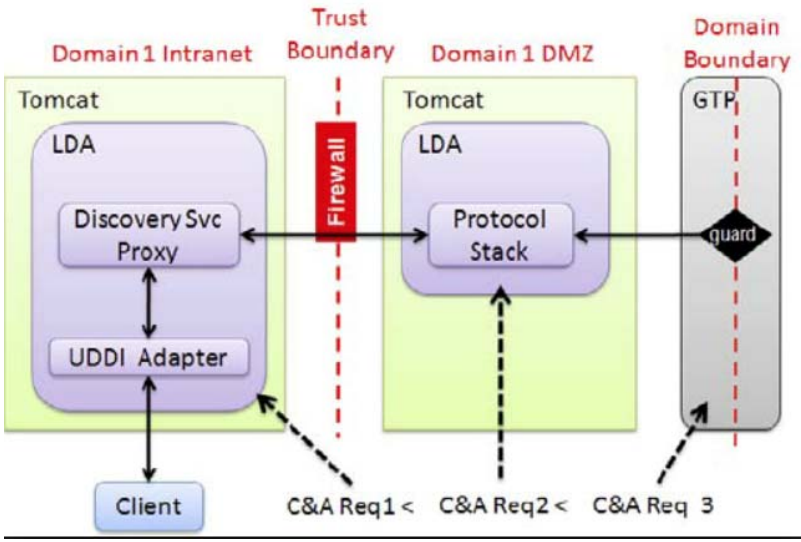
- The next major step in the SRA process involves the partitioning of the SuC into zones and conduiting. This process entails the putting the assets within the System under Consideration (SuC) different zones which have similar requirements.
- At this stage it is expected that a complete and accurate network diagram is expected, as it will have been used in the High-Level SRA.
- This process revolves around the Zone and Conduit Model incorporated in IEC 62443.



ProSalus SAFETY CONSULTANTS

Trust Boundaries

- A important consideration for the chosen zones is the level of trust that may be applied to the zone.
- This will impact on what connections or communication should be allowed between this zone and any others, especially if the other zone is considered trusted.
- By closely monitoring and controlling what connections or communications are allowed, entry points to the zones can be controlled.
- This ensures the security of the facility and in subsequent maintenance activities, such as Intrusion Detection.
- Information detailing entry points and possible attack paths will also be required during the detailed risk assessment, to give an indication of how an attack could progress and escalate.



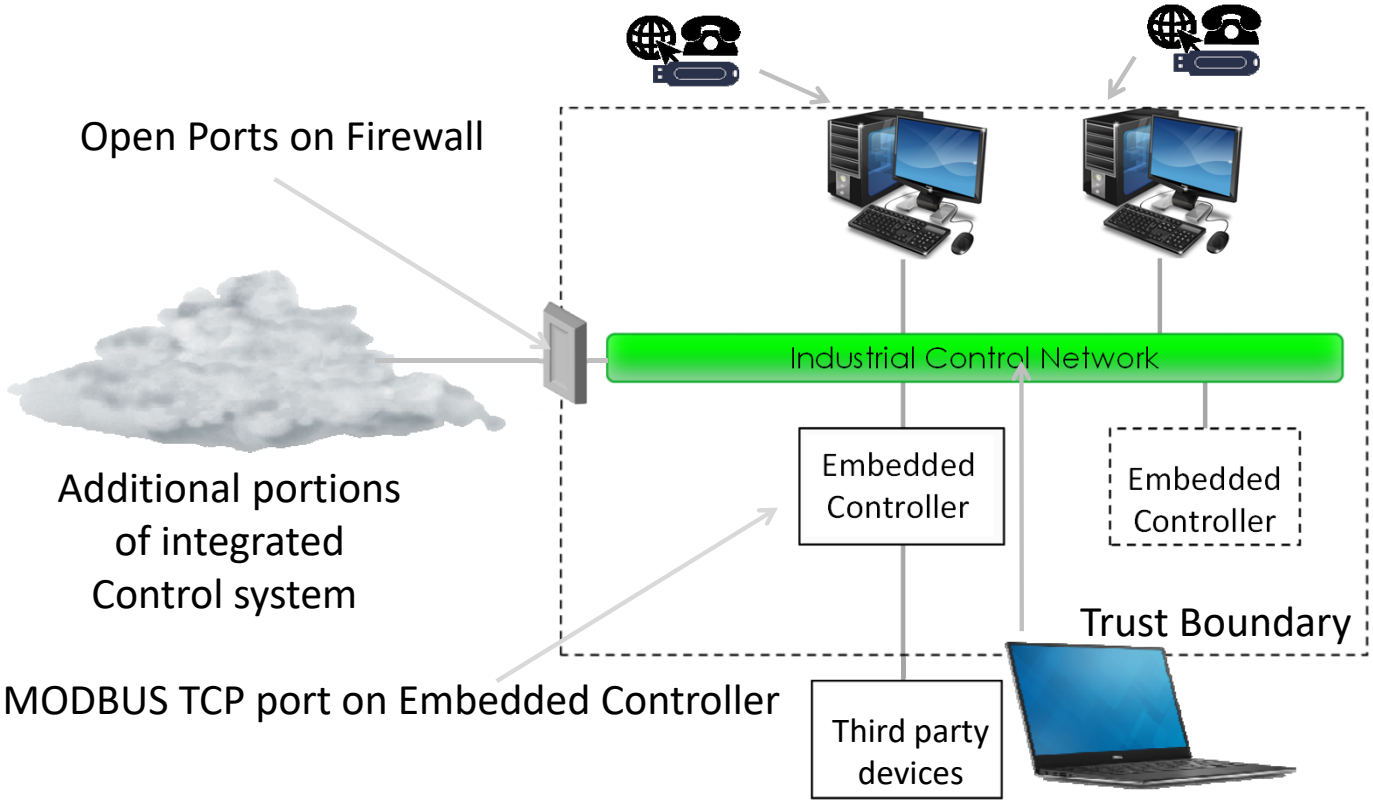
Purdue Model

- The Zone and Conduit model originates from the Purdue model which splits the network across the facility into a number of layers.
- It is useful to structure the network diagrams and system architecture using this model, as the level of trust required for each zone will differ, with the Enterprise Zone having a lower level of trust.
- This model is a benchmark for zone separation, with further zones and conduits based upon the requirements of each asset.
- This model also takes into account the DMZ zone which will be positioned between the enterprise and the operations zone.

Benefits of Applying The Zone and Conduit Model

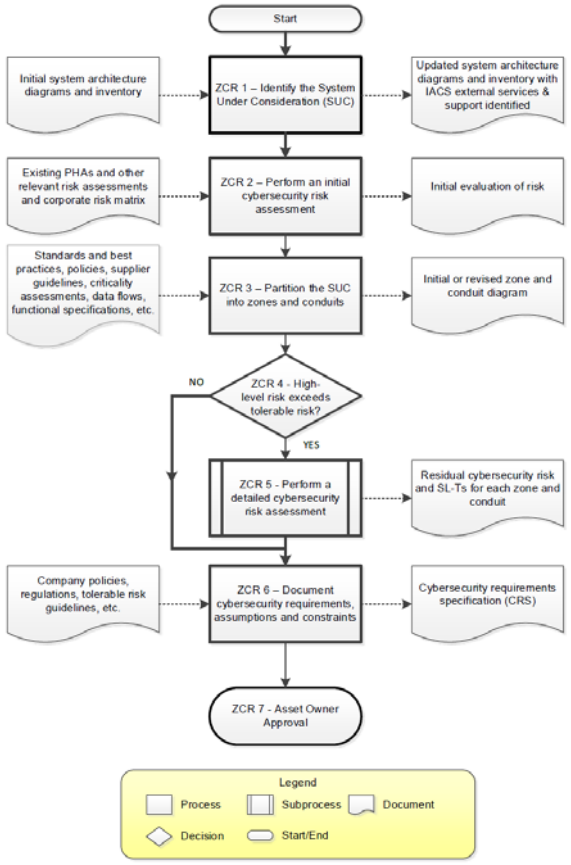
- While useful for determining the security level of the zone and conduits, this exercise also has a number of additional benefits.
  - Digital communications will be limited, making the facility more inherently secure.
- The model also incorporates the concepts of the Principle of Least Privilege and the Principle of Least Route.
  - **Principle of Least Privilege** – where users can only access assets and systems which they have authorisation to.
  - **Principle of Least Route** – where a network node is only given the connectivity necessary to perform its designed function.

Entry Points & Trust Boundary



Security Risk Assessment (SRA) Process from 62443-3-2

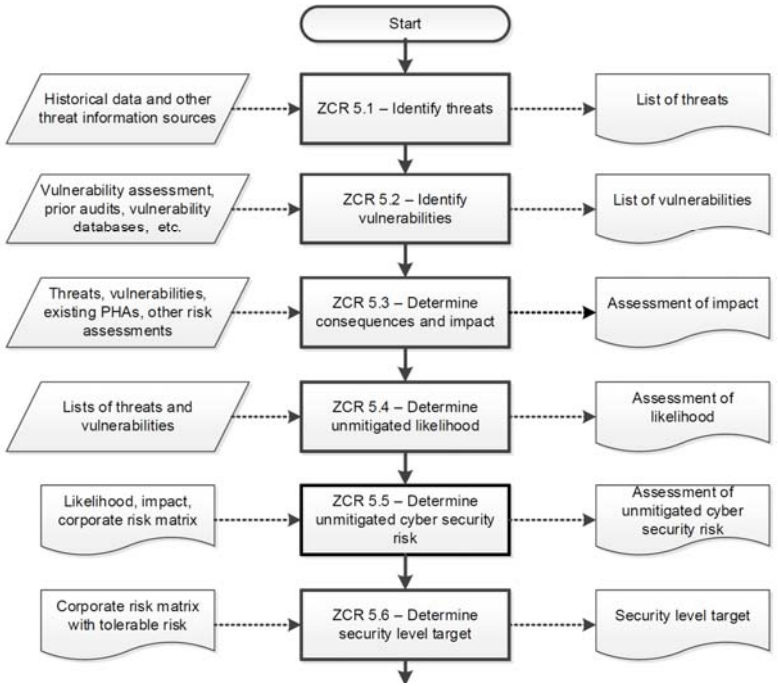
- Analysing the output of the High-Level SRA. Ensures that the High-Level risks that have been identified are considered and treated until either an acceptable or tolerable level of risk is achieved. This entails ensuring any counter measures that have earned credit are in place and provide the risk reduction claimed.
- If it is found that the risk has been treated sufficiently then for these risks the Detailed-Level SRA may be skipped and the documentation step, including the CSRS, may be started.
- However, if the risks have not been treated sufficiently or the safeguards claimed are not implemented, then the risks must be considered using a Detailed-Level SRA.



ProSalus SAFETY CONSULTANTS

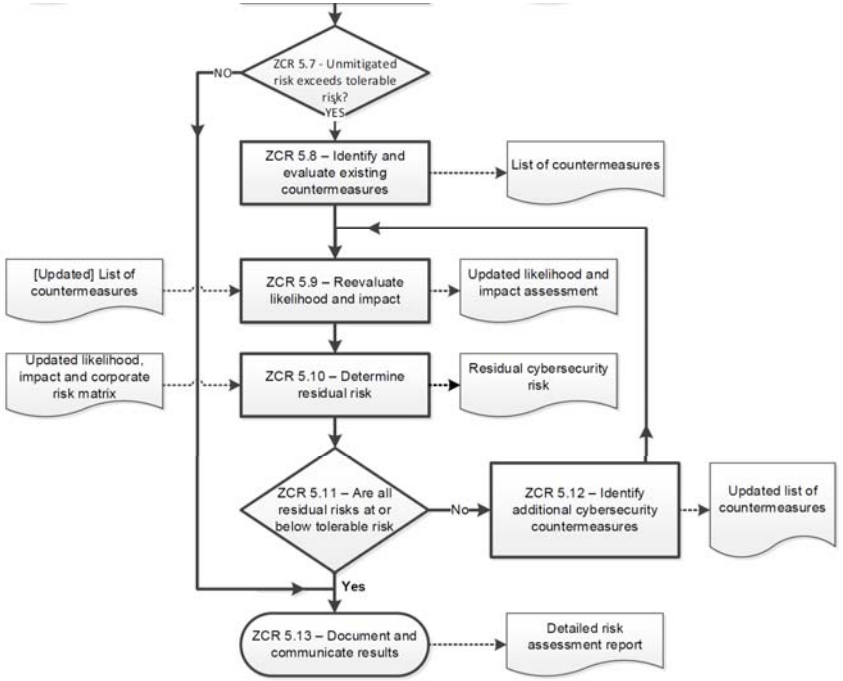
Detailed-Level SRA Process Diagram – SRA Process

Flow diagram for Detailed-Level SRA, specifically the actual risk analysis activity.



Detailed-Level SRA Process Diagram – Gap Analysis

Flow diagram for Detailed-Level SRA, specifically the gap analysis activity.

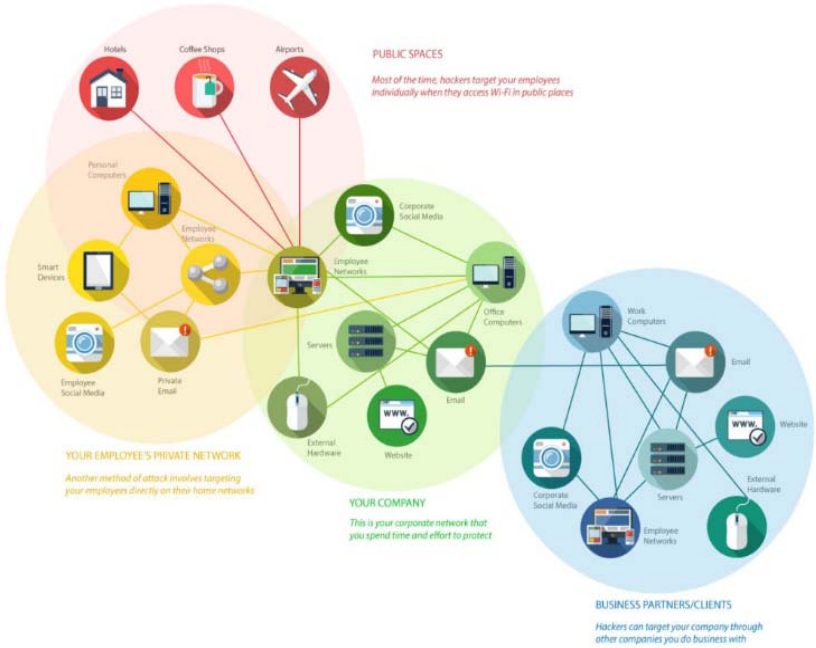


Attack Surface

- When considering the risks during the Detailed-Level SRA, it is important to have an idea of a possible attack path, so that the risks can be fully considered.

- During the Detailed-Level SRA it is important that not only the identified assets from the High-Level SRA are considered but also the risks faced from the zone.

- The best way to do this is to have a consideration towards what the attack surface of the zone would be.



Attack Surface Diagram

- The following diagram shows a conceptual method of viewing a site.

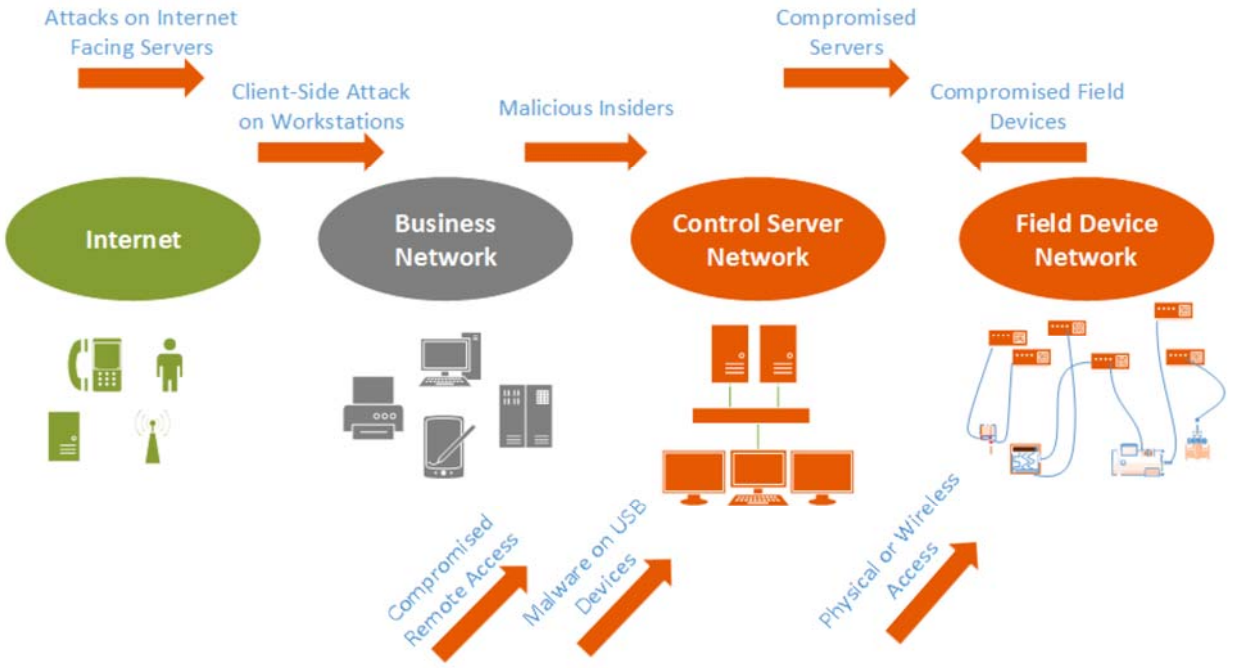


Diagram taken from: Sans summit archive.

Control Attack Surface Diagram

- The following diagram shows a control network specific attack surface diagram

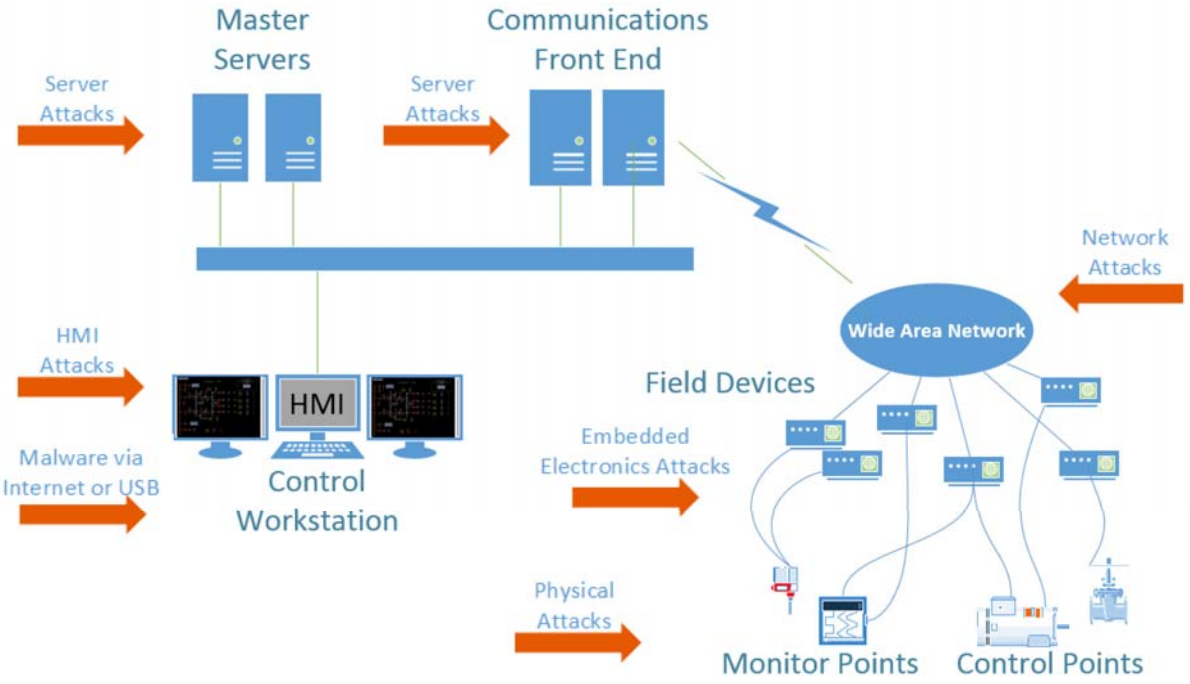
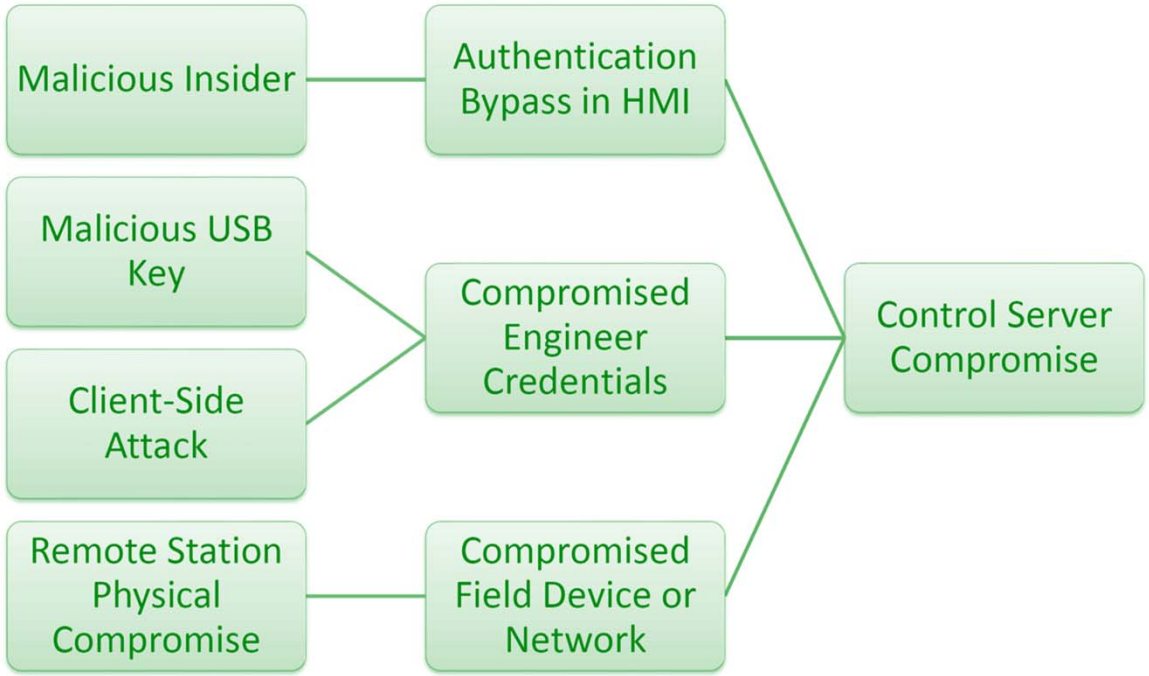


Diagram taken from: Sans summit archive.

Example of a Basic ICS Attack Tree

- The diagram shows a very basic IACS attack tree, with no attack costs calculated.
- Diagram taken from: Sans summit archive.



Types of Security Levels (SLs) from EN 62443-3-3

- SLs are broken down into three different types: target, achieved and capability. These types, while they are all related, have to do with different aspects of the security lifecycle.
- **Target SLs (SL-T)** are the desired level of security for a particular IACS, zone or conduit. It is established to communicate this to those responsible for designing, maintaining or operating the facility. This usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

- **Achieved SLs (SL-A)** are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target SLs.
- **Capability SLs (SL-C)** are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated.

Types of Security Levels (SLs) from EN 62443-3-3

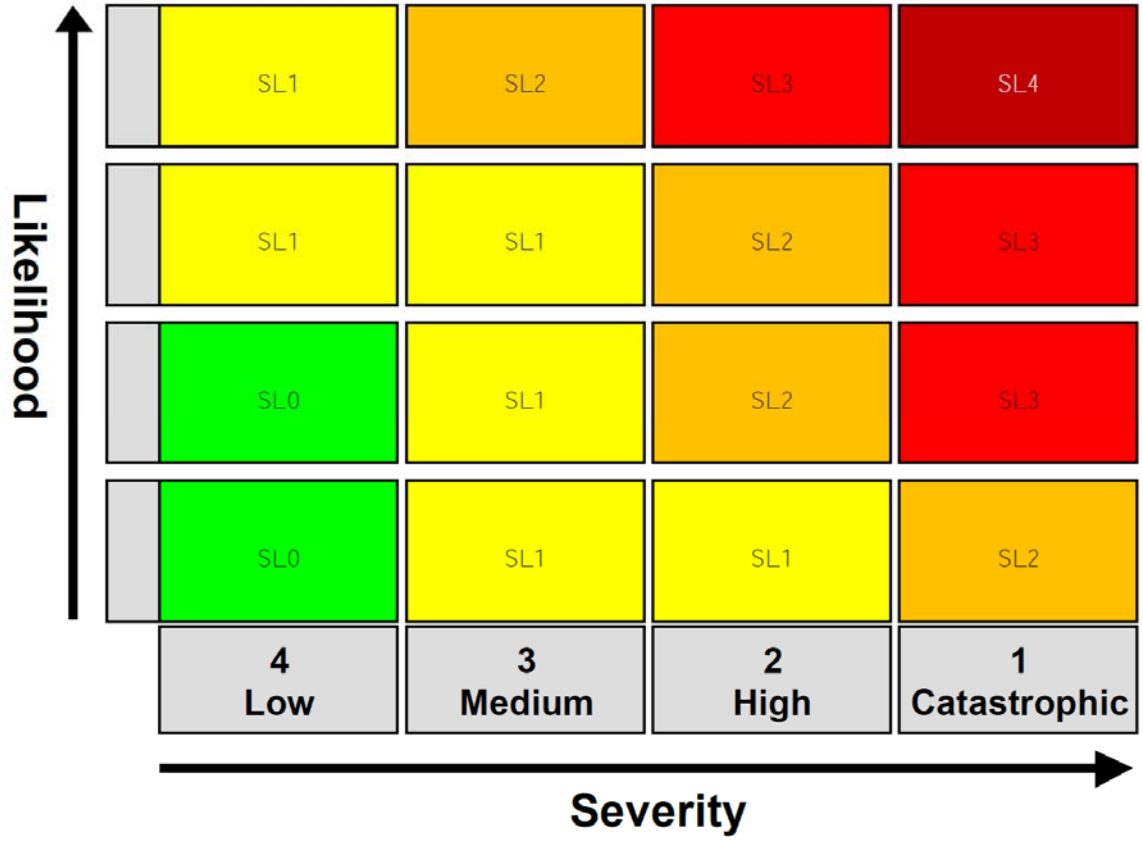
SLs are broken down into three different types: target, achieved and capability. These types, while they are all related, have to do with different aspects of the security lifecycle.

- **Target SLs (SL-T)** are the desired level of security for a particular IACS, zone or conduit. It is established to communicate this to those responsible for designing, maintaining or operating the facility. This usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.
- **Achieved SLs (SL-A)** are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target SLs.
- **Capability SLs (SL-C)** are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated.

Security Level Definitions

- ISA 62443-3-3 defines SLs in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security
- **SL 0**: No specific requirements or security protection necessary
- **SL 1:** Protection against casual or coincidental violation
- **SL 2:** Protection against intentional violation using simple means with low resources, generic skills and low motivation
- **SL 3:** Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
- **SL 4:** Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Example of Determining the Security Level Using a Risk Matrix



Example of Using a SL-T to Discover the Foundational Requirements.

Example section of table from IEC 62443-3-3 showing the mapping of a SL value to the FR

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)					
SR 3.1 – Communication integrity	7.3	✓	✓	✓	✓
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1			✓	✓
SR 3.2 – Malicious code protection	7.4	✓	✓	✓	✓
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1		✓	✓	✓
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2			✓	✓
SR 3.3 – Security functionality verification	7.5	✓	✓	✓	✓
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1			✓	✓
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2				✓
SR 3.4 – Software and information integrity	7.6		✓	✓	✓
SR 3.4 RE 1 – Automated notification about integrity violations	7.6.3.1			✓	✓
SR 3.5 – Input validation	7.7	✓	✓	✓	✓
SR 3.6 – Deterministic output	7.8	✓	✓	✓	✓
SR 3.7 – Error handling	7.9		✓	✓	✓
SR 3.8 – Session integrity	7.10		✓	✓	✓
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1			✓	✓
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2			✓	✓
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3				✓
SR 3.9 – Protection of audit information	7.11		✓	✓	✓
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1				✓

Document cybersecurity requirements, assumptions and constraints

Requirement:

- Following the Security Risk Assessment (SRA) there is a requirement to document the cybersecurity requirements, assumptions and constraints with the SuC as needed to achieve the Security Level – Target (SL-T).
- IEC 62443 requires the following documentation:
  - Cybersecurity Requirements Specification (CSRS)
  - SuC Description
  - Zone and Conduit Diagrams
  - Zone and Conduit Characteristics
  - Operating Environment Assumptions
  - Threat Environment
  - Organisational Security Policies
  - Regulatory Requirements

Cybersecurity Requirements Specifications

To ensure that the cybersecurity requirements specifications fulfills it's purpose, the following requirements should be included as a minimum:

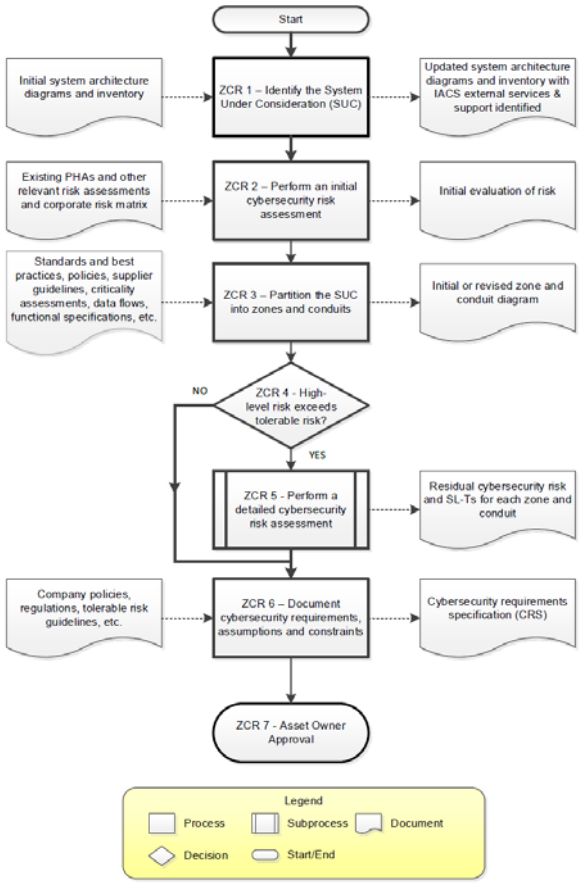
- System architecture diagram
- A description of the System under Consideration (SuC)
- Zone and Conduit characteristics and diagram
- Network segmentation requirements
- Operating environment assumptions
- Threat environment
- Organisational security policies
- Tolerable Risk
- Regulatory Requirements
- Access control requirements
- Physical security requirements
- Detection and monitoring requirements
- Response time requirements
- OS hardening requirements
- Device hardening requirements
- Applicable policies and procedures
- Security level-Target (SL-T)

ProSalus
SAFETY CONSULTANTS

Asset Owner Approval

Requirement:

- The asset owner management who are accountable for the safety, integrity and reliability of the process controlled by the SuC shall review and approve the results of the risk assessment.
- While those involved in the risk assessment may have the required knowledge and training, it is possible that they do not have authority to accept the risk for the organisation.
- This is especially important where the risk assessment has been facilitated by a third-party.



ProSalus SAFETY CONSULTANTS

ProSalus
SAFETY CONSULTANTS