DNV·GL

RECOMMENDED PRACTICE

DNVGL-RP-G108 Edition September 2017

Cyber security in the oil and gas industry based on IEC 62443

DNV GL AS

FOREWORD

DNV GL recommended practices contain sound engineering practice and guidance.

Any comments may be sent by e-mail to *rules@dnvgl.com*

This service document has been prepared based on available knowledge, technology and/or information at the time of issuance of this document. The use of this document by others than DNV GL is at the user's sole risk. DNV GL does not accept any liability or responsibility for loss or damages resulting from any use of this document.

CHANGES – CURRENT

This is a new document.

Acknowledgements

Industrial automation and control systems (IACS) in oil and gas installations are vulnerable to cyber security incidents. As a result, countermeasures must be in place, and the facility operator must be confident that these countermeasures are sufficient and correctly performed. The risk must be acceptable for all systems including existing and possibly obsolete systems. Due to the high number of packages and systems in the packages, a standard based approach is required.

Such standards for industrial automation and control systems are evolving, and the IEC 62443 standard is emerging as the preferred approach for many. The challenges are that this is a generic standard for all industrial components and that it is not finalized yet. Verifying conformance to the entire set of the IEC 62443 series of standards is very costly, and some parts may be irrelevant to certain industries. The standard also refers to security levels (SL), but it may be difficult to define the correct target for the different systems. Currently the standard defines what to do, but does not fully detail how to do it.

To overcome these challenges, this recommended practice for implementing IEC 62443 (3-2, 3-3 and 2-4) in the oil and gas sector was produced based on a joint industry project (JIP) with participation from ABB, DNV GL, Emerson, Honeywell, Kongsberg Maritime, Lundin Norway, Petroleum Safety Authority (PSA) Norway, Shell Norway, Siemens, Statoil and Woodside Energy. The purpose of this JIP was to define a common and practical approach on how to secure industrial automation and control systems (IACS) in the oil and gas sector.

The recommended practice intends to follow the regulatory requirements defined by PSA for the Norwegian continental shelf and by Health and Safety Executive (HSE) for the UK oil Sector.

CONTENTS

SECTION 1 GENERAL

1.1 Introduction

This recommended practice provides a guideline for how to apply the IEC 62443 series of standards in the oil and gas industry. Although the standard describes cyber security requirements for all industries, this recommended practice is tailored to oil and gas. While the standard focuses on what to do, this recommended practice focuses on how to do it.

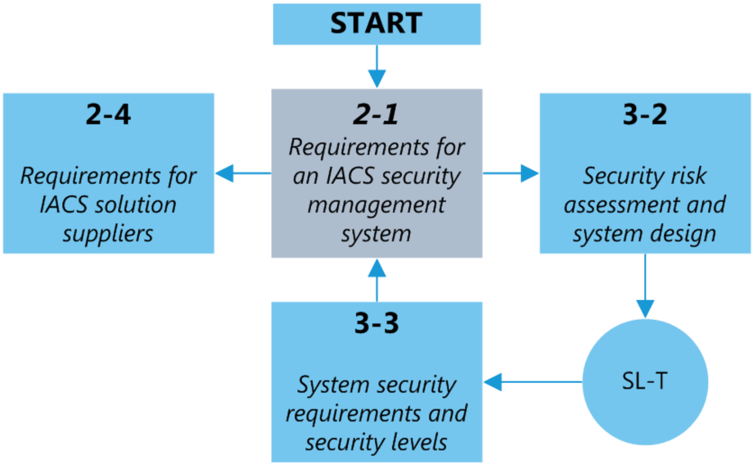
The IEC 62443 standards currently consist of a number of finalized and draft documents. This guideline focuses on four of them. Figure 1-1 indicates how the four IEC 62443 standards interrelate.

Organisations operating an industrial automation and control system (IACS) should have a cyber security management system (CSMS) in place, according to IEC-62443-2-1 /1/. This standard describes the implementation, management and operation of an IACS management system based on ISO/IEC 27001 and ISO/IEC 27002.

IEC 62443-3-2 sets the requirements for risk assessment leading to the identification of zones and conduits for the IACS. Based on the detailed risk assessment for each zone and conduit, the sufficient security level target (SL-T) for each could be determined.

The SL-T guides which requirements and enhancements in IEC 62443-3-3 that should be evaluated to ensure sufficient countermeasures.

A supplier of IACS must provide an organisation that are able to handle the technical requirements as well as organisational and operational requirements given in IEC 62443-2-4. Combined with the specified requirements in IEC 62443-3-3, the correct IACS with sufficient security can be delivered to a customer that is able to maintain the security level.


START
2-4
Requirements for IACS solution suppliers
2-1
Requirements for an IACS security management system
3-2
Security risk assessment and system design
3-3
System security requirements and security levels
SL-T

*Note that 3-3 and 2-4 partly overlap. Therefore, both 3-3 and 2-4 are used to define system security requirements in the project and operations phases.

Figure 1-1 Using the IEC 62443 standards overview

The recommended practice is relevant for the whole oil and gas industry, but focuses on the front end engineering design (FEED), production and operation phase of greenfield and brownfield projects in the upstream sector. Figure 1-2 indicates the steps described in this recommended practice that are related to the concept, FEED, project and operations phases. In Sec.5 and Sec.6, important requirements and practical "how to" guidance are provided for the project and operations phases. It should be noted that these are recommendations and not a complete list of measures.

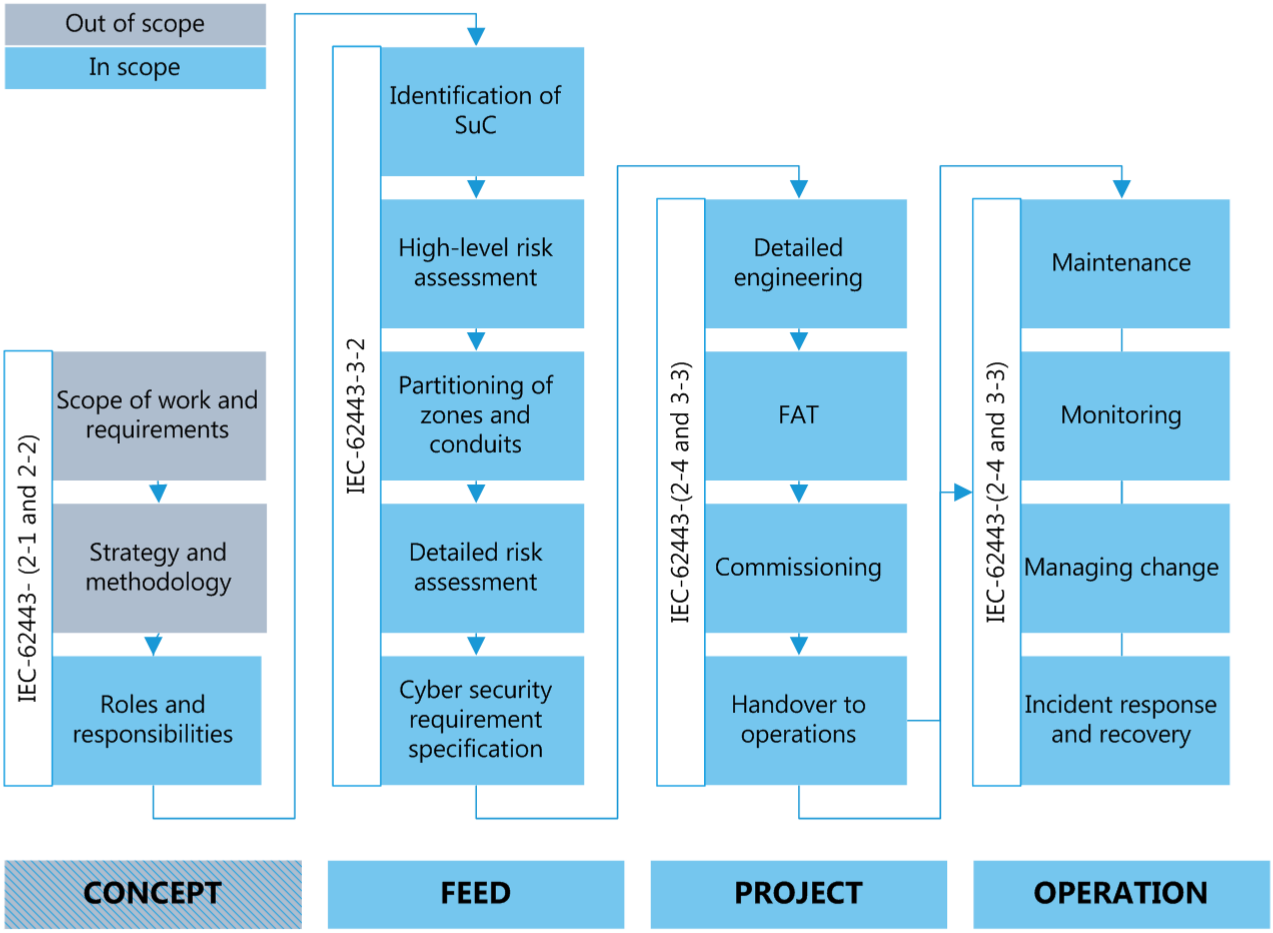


Figure 1-2 IEC 62443 in FEED production and operation

The target audience of this recommended practice is intended to include all the elements (people, process and technology) that are involved in ensuring cyber security is taken care of in the IACS (asset owner, system integrator, product supplier, service provider, compliance authority). This recommended practice clarifies the responsibilities shared between these parties, and describes who performs the activities, who should be involved, and the expected inputs and outputs.

The asset owner (operator) should have a cyber security management system in place before initiating an oilfield project. The requirements for a CSMS are defined in IEC 62443-2-1 /1/ and ISO 27001 /8/, and are not further discussed in this recommended practice.

Cyber security is implemented as a combination of technology, processes and people as illustrated in Figure 1-3. This recommended practice focuses on technology and processes. The security level concept to group technical requirements is used throughout the document. The maturity level concept, described in IEC-62443-2-4, groups processes and organizational requirements. This concept is not included in this recommended pactice, but is described in /2/.

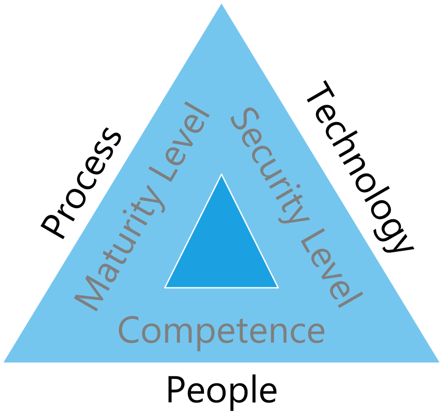


Figure 1-3 Cyber security involving process, technology and people

The IEC62443 committees plan to issue a new standard for protection levels (PLs). The aim is to define security control classes (SCC), and do a mapping compared to the requirements in IEC62443-2-1, IEC62443-2-4 and IEC62443-3-3.

The technical implementation and configuration in the IACS and how the IACS solution is operated, maintained and deployed will be reflected in the protection level (PL). Protection level is a methodology to evaluate the protection of plants in operation. The methodology includes the evaluation of technical capabilities and the related processes in a combined evaluation.

PLs combine the evaluation of technical and organizational measures.

The intention is to update this recommended practice once the IEC standards' definitions of PL are released.

SECTION 2 DEFINITIONS AND ABBREVIATIONS

Glossary of technical terms.

2.1 Definitions

Table 2-1 Terms and definitions

Term	*Definition*
authentication	process of validating identity
authorization	right or permission that is granted to a system entity to access a system resource Authorization is dependent on authentication.
availability	ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided
asset owner	in this context, the asset owner is the oilfield operator
brownfield project	a project following a prior project or work
conduit	logical grouping of communication channels, connecting two or more zones, that share common security requirements
cyber security	actions required to preclude unauthorized use of, denial service to, modifications to, disclosure of, loss of revenue from or destruction of critical systems or informational assets
cyber threat	a circumstance or event that has, or indicates, the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society
firewall	inter-network connection device that restricts data communication traffic between two connected networks
greenfield project	a new project not following a prior project or work
insider	trusted person, employee, contractor, or supplier who has information that is not generally known to the public
operation organisation	personnel (asset owner/vendors) with work tasks related to the operation phase
outsider	person or group not trusted with inside access, who may or may not be known to the targeted organization
penetration	successful unauthorized access to a protected system resource
remote access	use of systems that are inside the perimeter of the security zone being addressed from a different geographical location with the same rights as when physically present at the location
risk	the product of the likelihood and the consequence of a threat being realized
service provider	vendor of services related to industrial automation and control systems In larger oilfield projects, the term engineering, procurement and construction contractor is used.

Term	*Definition*
system owner	official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system
threat agent	causative agent of a threat action
threat vector	path or means by which a threat source can gain access to an organizational asset
vendor	in this context: vendor of safety and automation systems
vulnerability	flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s integrity or security policy

2.2 Abbreviations

Table 2-2 Abbreviations

Abbreviation	*Description*
AAA	authentication, authorization and accounting
ACL	access control list
AD	active directory
ALARP	as low as reasonably practicable
BPCS	basic process control system
CAP	critical action panel
CCTV	closed circuit television
CSRS	cyber security requirement specification
CSMS	cyber security management system
DMZ	demilitarized zone
DNS	domain name system
EAP-TLS	extensible authentication protocol transport level security
EPC	engineering, procurement and construction
ESD	emergency shutdown
EWS	engineering workstation
F&G	fire and gas
FAT	factory acceptance test
FEED	front end engineering design
FW	firewall
GPO	group policy object
HAZID	hazard identification
HAZOP	hazard and operability study

Abbreviation	*Description*
HMI	human-machine interface
HSE	Health and Safety Executive
IACS	industrial automation and control systems
ICS	industrial control system
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IPL	independent protection layers
IPSec	internet protocol security
JIP	joint industry project
LCR	local control room
MAC	media access control
MSCM	Microsoft security compliance manager
MC	mechanical completion
MOC	management of change
OSI	open system interconnection
OU	organizational unit
PL	protection level
RAS	remote access server
RBAC	role-based access control
RCR	remote control room
RP	recommended practice
RTO	recovery time objective
RPO	recovery point objective
SAS	safety and automation system
SAT	system acceptance test
SIEM	security information and event management
SIL	safety integrity level
SIS	safety instrumented system
SCADA	supervisory control and data acquisition system
SCW	security configuration wizard
SL	security level
SL-T	security level target
SSH	secure shell

Abbreviation	*Description*
SuC	system under consideration
TCD	thermal conductivity detector
TLS	transport layer security
TRA	threat and risk assessment
VLAN	virtual local area network
VTP	VLAN trunking protocol
WLAN	wireless local area network
WPA	wi-fi protected access
WSUS	Windows server update services

SECTION 3 CONCEPT PHASE

3.1 General

This recommended practice focuses on the FEED, project and operation phases, but also includes best practice for roles and responsibilities that should be defined in the concept phase. Definitions of roles and responsibilities are applicable to all phases, but a special focus should be given in the concept phase.

3.2 Roles and responsibilities

In oil and gas projects, multiple vendors, contractors and the asset owner are involved in different phases from early concept studies, through FEED, detail engineering, fabrication, testing, packaging, transport, storage, installation and commissioning. To ensure effective cyber security, it is important to have a clear understanding of roles and responsibilities.

Historically, cyber security has not been a priority in the projects phase - often because the responsibilities and design requirements are not fully understood.

The following table gives a sample on who is responsible for performing the activities described in IEC 62443-3-2 /3/, and in which phase in the project the activities should be included. The table applies to greenfield projects – or large brownfield projects involving an EPC contractor.

Table 3-1 Example of greenfield responsibilities

Activity	*Phase*	*Main responsible*	*Performed by*	*Input provided by*
Identification of the System under Consideration (SuC)	FEED	Asset Owner	EPC contractor	Asset Owner
High-level risk assessment	FEED	Asset Owner	EPC contractor	Asset Owner
Partition the SuC into zones and conduits	FEED	Asset Owner	EPC contractor	Asset Owner Package vendors
Detailed cyber security risk assessment of zones and conduits	FEED	Asset Owner	EPC contractor	Asset Owner Package vendors
Establish the cyber security requirements specification	FEED	Asset Owner	EPC contractor	Asset Owner
Installation, commissioning and validation	Detailed engineering	Asset Owner	EPC contractor	Asset Owner Package vendors

SECTION 4 FEED PHASE

4.1 General

This section is based on IEC 62443-3-2 /3/, and describes good practice on how to perform security risk assessment and system design during the FEED phase. The recommended steps, detailed in [4.2] to [4.5], are indicated in Figure 4-1. Performing the steps will result in the cyber security requirement specification (CSRS) being documented. The CSRS will then be used to communicate the cyber security requirements to stakeholders, and by the development/implementation teams that will perform the detailed design, installation, FAT, commissioning and verification.

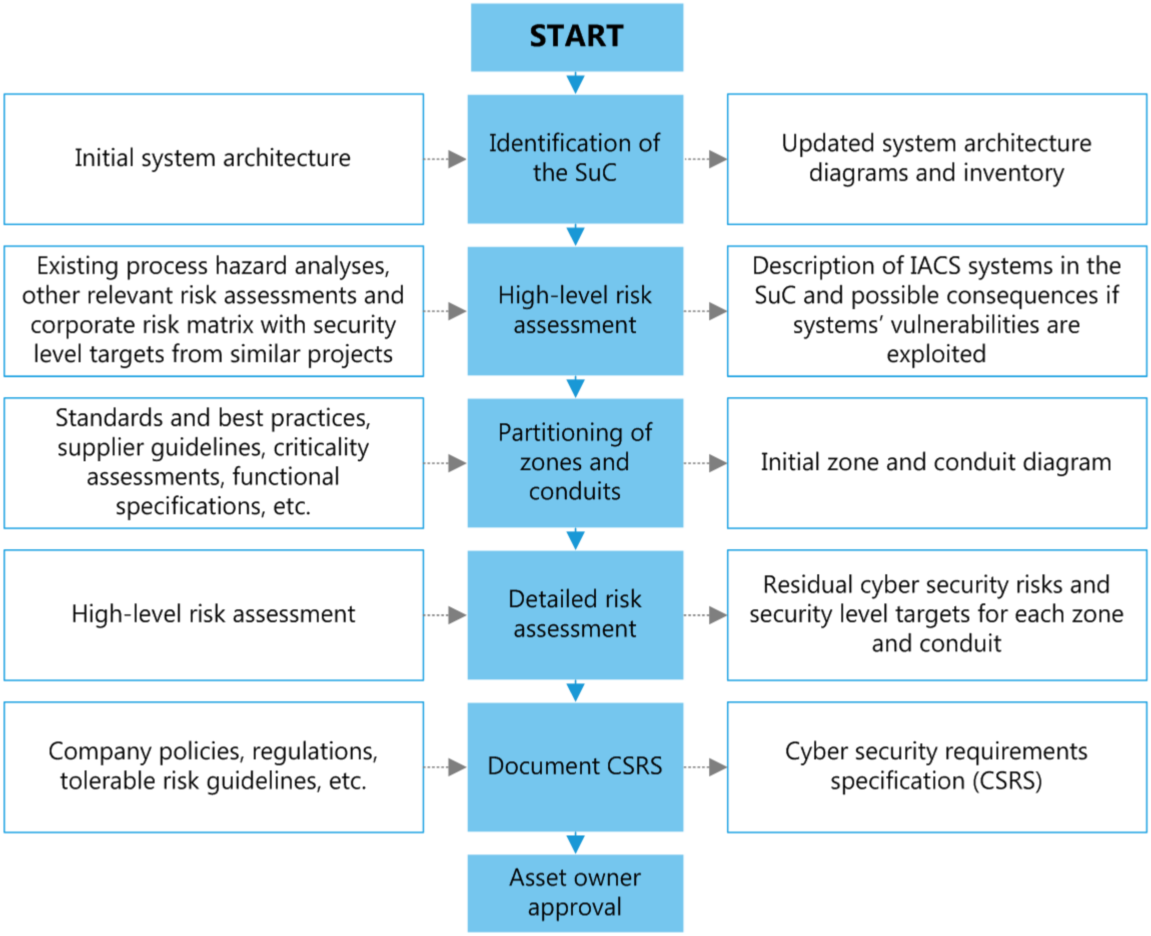

START
Initial system architecture
Identification of the SuC
Updated system architecture diagrams and inventory
Existing process hazard analyses, other relevant risk assessments and corporate risk matrix with security level targets from similar projects
High-level risk assessment
Description of IACS systems in the SuC and possible consequences if systems' vulnerabilities are exploited
Standards and best practices, supplier guidelines, criticality assessments, functional specifications, etc.
Partitioning of zones and conduits
Initial zone and conduit diagram
High-level risk assessment
Detailed risk assessment
Residual cyber security risks and security level targets for each zone and conduit
Company policies, regulations, tolerable risk guidelines, etc.
Document CSRS
Cyber security requirements specification (CSRS)
Asset owner approval

Figure 4-1 Steps in FEED phase

For greenfield projects, an initial CSRS may be prepared before the risk assessment is completed, as procurement of equipment packages often is completed early in the FEED phase. It is recognized that, at that time, all the information used as input to the CSRS might not be available. However, it is of vital importance to set some initial cyber security requirements during the procurement process to ensure that the equipment needed has the necessary cyber security capabilities to meet the expected level of security controls/requirements.

4.2 Identification of the system under consideration

Input:

1) Initial system architecture diagrams and inventory.
2) Initial network topology diagrams for all packages that will be included in the IACS.

What should input look like:

1) High-level network topology diagrams.
2) Example diagram.
3) Systems communication within and external to the system under consideration (SuC).

Best practice for identification of the SuC:

1) Include an overview of all system assets needed to provide the IACS solution.
2) Describe the security perimeters:
   - include firewalls used to implement perimeters.
3) Define which external access/entry points will exist to the SuC after it is handed over to production:
   - remote access to IACS
   - online file transfer requirements
   - offline file transfer requirements (USB …) to offline systems
   - data flows to/from external systems.

Output: Description of intended operational environment, updated system architecture diagrams and asset list describing the SuC, perimeters and entry points.

4.3 High-level cyber security risk assessment

The high-level risk assessment is used to determine the business and HSE impact in the event of system compromise or failure. The purpose of the high-level risk assessment is to identify the worst-case unmitigated risk to the SuC /3/. The output of a high-level risk assessment will be input to the grouping of assets into zones and conduits and the detailed risk assessments. The steps involved in the high-level cyber security risk assessment are shown in Figure 4-2.

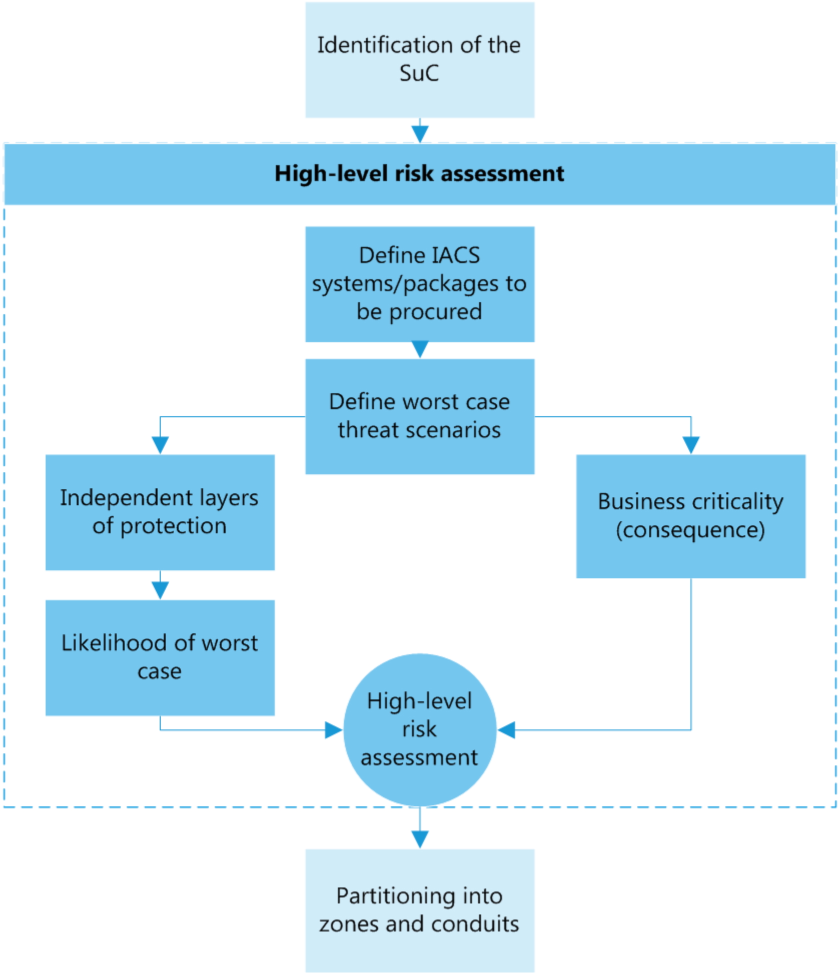

Identification of the SuC
High-level risk assessment
Define IACS systems/packages to be procured
Define worst case threat scenarios
Independent layers of protection
Business criticality (consequence)
Likelihood of worst case
High-level risk assessment
Partitioning into zones and conduits

Figure 4-2 High-level cyber security risk assessment

The target group for the high-level risk assessment includes stakeholders who may have limited in-depth knowledge of cyber security risks. The high-level risk assessment should be documented in a manner that allows all stakeholders to get a clear overview of the high-level cyber risk picture.

The high-level risk assessment is usually based on a review workshop. The output should be presented to appropriate local/regional asset owners and stakeholders.

Input:

- Corporate risk matrix, business impact assessments, disaster recovery plans, incident response plan, functional specifications, etc.
- Relevant safety assessments (such as a safety requirements specification).
- Description of asset owner performance standards for safety systems and barriers.

Best practice for performing the high-level risk assessment:

1) Collect information about which IACS systems/packages in the SuC that are to be procured and installed.
2) Define on a holistic level the worst-case cyber threat scenarios based on inputs such as the corporate risk matrix, business impact assessments, etc.

3) Define the business criticality/consequence of the worst-case scenarios (safety, environmental, financial, brand). Consider using input from the safety discipline work related to HAZID and HAZOP activities.
4) Describe which of the IACS systems/packages that will have critical functionality needed to implement the safety systems and barriers and define the generic independent layers of protection. Consider using a bow-tie-based approach.
5) Define the likelihood of the worst-case scenarios (e.g. high, medium, low). The likelihood can for example be based on the threat agent ’s capability, motivation and opportunity, as described in /18/ to exploit a threat vector. The opportunity is based on the vulnerabilities in the respective systems/ packages.
6) Based on previous steps, conduct a relative risk ranking of unmitigated risks relating to the SuC's systems/packages.

Output: A description of IACS systems in the SuC and possible consequences if the systems' vulnerabilities are exploited, causing the systems to be unavailable or a loss of integrity or confidentiality. Evaluation of what represents the worst-case unmitigated risk.

4.4 Partition the system under consideration into zones and conduits

Input:

1) Outputs of the high-level cyber security risk assessment.
2) Reference model defined in this document.

What should input look like:

1) High-level cyber security risk assessments. Consider the reuse of risk assessments for similar IACS solutions.
2) Reuse of zone and conduit drawings for similar projects.
3) Reuse of package vendor best practice.

4.4.1 Overall strategy for partitioning the system under consideration into zones and conduits

The data networks connecting components in the SuC should be separated into zones based on systems functionality, location, responsible organization or the risk assessment.

It is recommended to start with a functional segmentation which divides the network into several layers, with the enterprise zone on the top, progressing through the DMZ, to the control zones, and finally to the IACS and safety instrumented system (SIS) (/20/). Figure 4-3 represents a simplified traditional functional segmentation of the network. This figure shows generic devices, and their location may vary between SAS vendors.

Partitioning the SuC into zones and conduits will require a good understanding of:

— how different systems interact
— where information flows between systems:
    — which devices communicate
    — how fast/often those devices communicate
— what form the information takes
— the security differences between system components
— the criticality of systems (based on a high-level risk assessment as described in [4.3]).

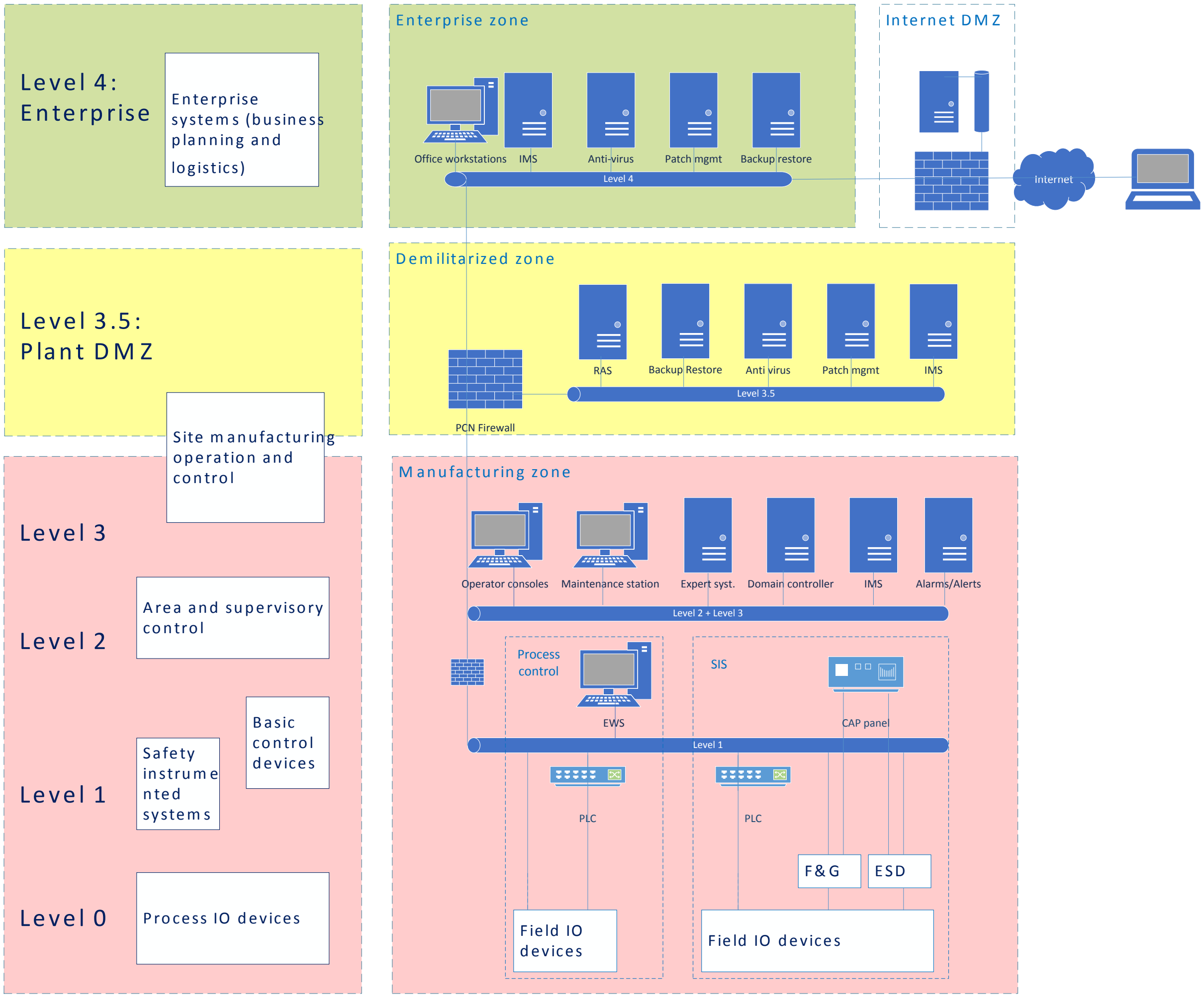


Figure 4-3 Traditional functional separation of IACS

With the basic primary zones in place, the focus can turn to the specific groupings, or subzones, within each primary zone, and how these subzones interact with other subzones. In this step, the nature of the network traffic sent and received by each subzone component, along with the specific network services offered, or required within them are considered. Security requirements and functionality already defined in the previous steps are refined and clarified.

Some considerations:

- Systems that do not have functional or operational dependencies requiring them to be in the same zone should be segmented into different zones by firewalls (even if they are on the same criticality level) as:
  - This will reduce the likelihood of viruses and worms spreading to other systems.
  - It can provide better access control to specific computers in a specific zone (prevent pivoting).
  - This will limit the exposure of systems to other/external systems.
- Systems (or parts of systems) with different criticality should not be mixed in the same zone. They may require different security levels and different countermeasures.

- If there are systems in the SuC that are not able to implement effective risk mitigating countermeasures, then network segmentation can be a countermeasure in itself. Such systems can be placed in a separate zone and have very limited connections to external systems. These may, for example, be systems that have reached end-of-support – and cannot be updated with security patches or have updated antimalware software installed.
- Communications between zones should be controlled and logged by firewalls. Firewalls should only allow traffic that has been explicitly allowed. All other traffic should be dropped. Firewalls should be logged and monitored. Consider enabling firewall controls, where available, on the systems themselves.
- A high number of zones require many separation devices and administrative procedures. Such complexity may influence the security and availability. A balanced approach is needed.

Partitioning the SuC into zones and conduits will facilitate the detailed risk assessment and make it easier to identify effective security countermeasures to mitigate risk to an acceptable level.

4.4.2 Separation of safety instrumented system zones

SIS zone(s) can be separated from the control zone(s) in different ways. ISA-TR84 /21/, describes four options: air-gapped, interfaced, integrated 2 zone and integrated 1 zone. The example generic zone model in Figure 4-3 shows an integrated 1 zone. In this section, the integrated 2 zone model is shown as a sample in Figure 4-4, but other separation mechanisms are relevant. The figure shows traffic from the SIS zone communicating to the basic process control system (BPCS) and higher-level systems for monitoring purposes. This information should be read-only flowing from the SIS zone out to other systems.

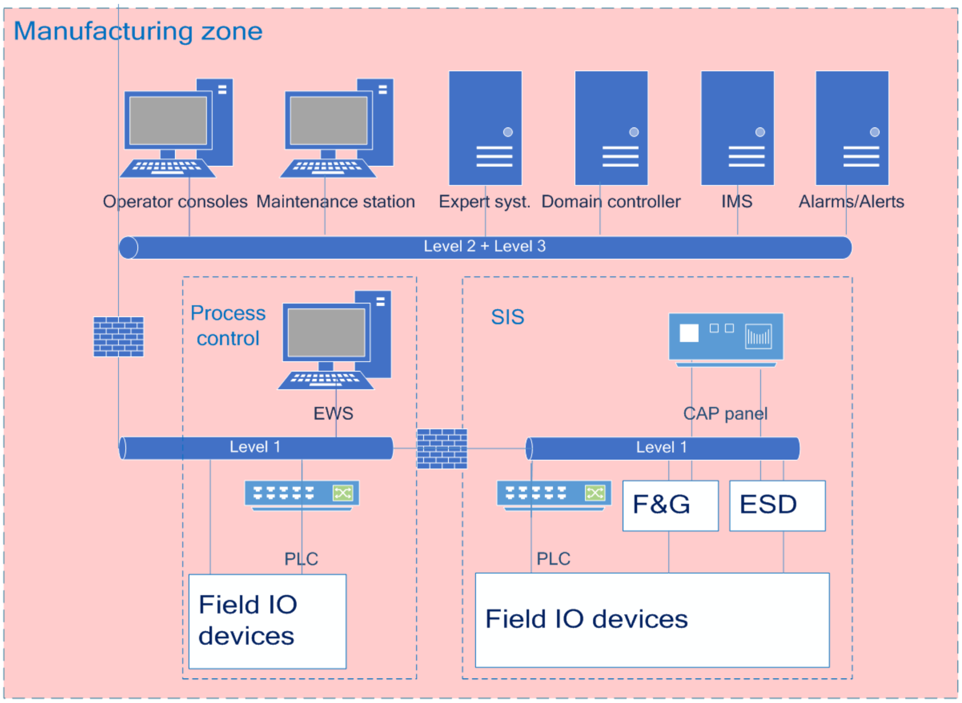


Figure 4-4 Integrated 2 zone

The separation of SIS zones should be based on a risk assessment.

SIS communications and process control communications should be physically or logically separated. Failures and cyber security incidents should not prevent the SIS from performing its safety functions.

Additionally, it should not be possible to establish connections to SIS from other zones (including remote access applications) at level 3 or above. (See IEC 62443-2-4 /2/ Req. ID SP 05.01 to SP 05.09)

The SIS controller should be protected from unauthorized and unintended download of changes e.g. with unique passwords for each SIS. The password should only be known to authorized personnel defined as users of the SIS systems.

Hardwired signals between SIS controllers can be used as an alternative for safety-critical communication on the common process network.

A local security device (e.g. local key switch) can be used to provide extra protection to the SIS controllers.

In a network where the SIS and process control are physically connected, (integrated 1 zone) logical separation must be used to ensure the fulfilment of these requirements.

For HSE compliance follow /22/ appendix 5: *Additional SIS Considerations*.

4.4.3 Separation of temporary connected devices

The SuC consists of systems of different size, complexity and criticality. Engineering tools, configuration tools and diagnostic tools are necessary to operate and maintain these systems. For highly critical systems, these tools should be included as permanent equipment (example SIS, SAS, electro control. etc.).

For systems with low criticality, these tools may be connected using remote access solutions or by use of temporary devices (e.g. portable computer). This greatlydepends on the party that will operate and support the systems in the operations phase. For example, – if the asset owner operates and support the system, permanent equipment can be a good solution.

For systems with an extensive use of external suppliers bringing temporary devices, a separate zone for temporary connected devices should be established. In this zone, procedures and technical solutions should be established to verify the patch status, hardening status and antivirus status. After this verification process, the device may be given access to IACS zones through the remote access solution or a solution tailored for this temporary access zone. The verification of the device may also be used as part of the approval process to allow the device to be physically connected to other zones.

The best practice for connecting temporary service PCs is to:

— Use dedicated equipment for the purpose.
— Obtain formal approval of the connection by the asset owner.
— Verify that the device has an updated patch level.
— Verify that antivirus and endpoint protection are installed and signatures are updated. Solutions detecting heuristic behavior are preferred.
— Verify that antivirus scanning is performed prior to connection.

Connecting a temporary device directly to an IACS zone should be handled as a deviation.

In addition to procedures and technical equipment for the verification of portable computers, equipment to verify removable storage devices should be established. It is a good practice to use two independent antivirus solutions on such equipment. The antivirus signature files should be kept updated.

4.4.4 Separation of wireless communications

Wireless communication can be split into different categories, such as wireless communication for the office network, wireless communication for the entertainment devices and wireless communication for the industrial networks (e.g on the control network level).

Requirements for wireless communication can be found in IEC-62443-2-4 SP04 and IEC62443-3-3 FR1 SR1.6 and FR2 SR2.2.

Traditionally, IACS equipment is cabled on new-builds, but changes and new equipment tend to be connected to a wireless network due to cabling cost. Therefore, wireless security should be included in the network design and procedures.

The following best practice applies regarding zones for wireless communication:

- Wireless communication should be in one or more zones separated from wired communication.
- Wireless networks should apply strong authentication and encryption schemes (example WPA2 or EAP-TLS).
- “Mobile workers” and devices (except planned barrier devices) shall not simultaneously be connected to both wireless office networks and wireless industrial networks.
- Access to wireless networks shall be restricted to authorized devices.

More information:

For more information on securing wireless networks, see /19/, and the wireless recommendations (currently chapter 6.3.2.5) of NIST SP 800-82 /10/.

4.4.5 Separation of devices connected via untrusted networks

Devices that are permitted to make connections to the SuC via an untrusted network should only be allowed to do so through the remote access solution. This includes devices in the enterprise network, devices connected to the temporary connected device zone (see [4.4.3]), and vendor devices used for remote maintenance.

Permanent devices placed in a physically secured area may be connected to process control segments as described in [4.4.6].

A sample zone and conduit model for the remote access solution is given in Figure 4-5. The figure shows an external user (e.g. control system vendor) setting up a secure connection to the organizations' VPN gateway in the Internet DMZ. If the authentication is successful, the user will be authorized to access the RAS server in the process control DMZ. The user will then be authenticated again and will, based on a defined work order, be given a connection into the requested process control system.

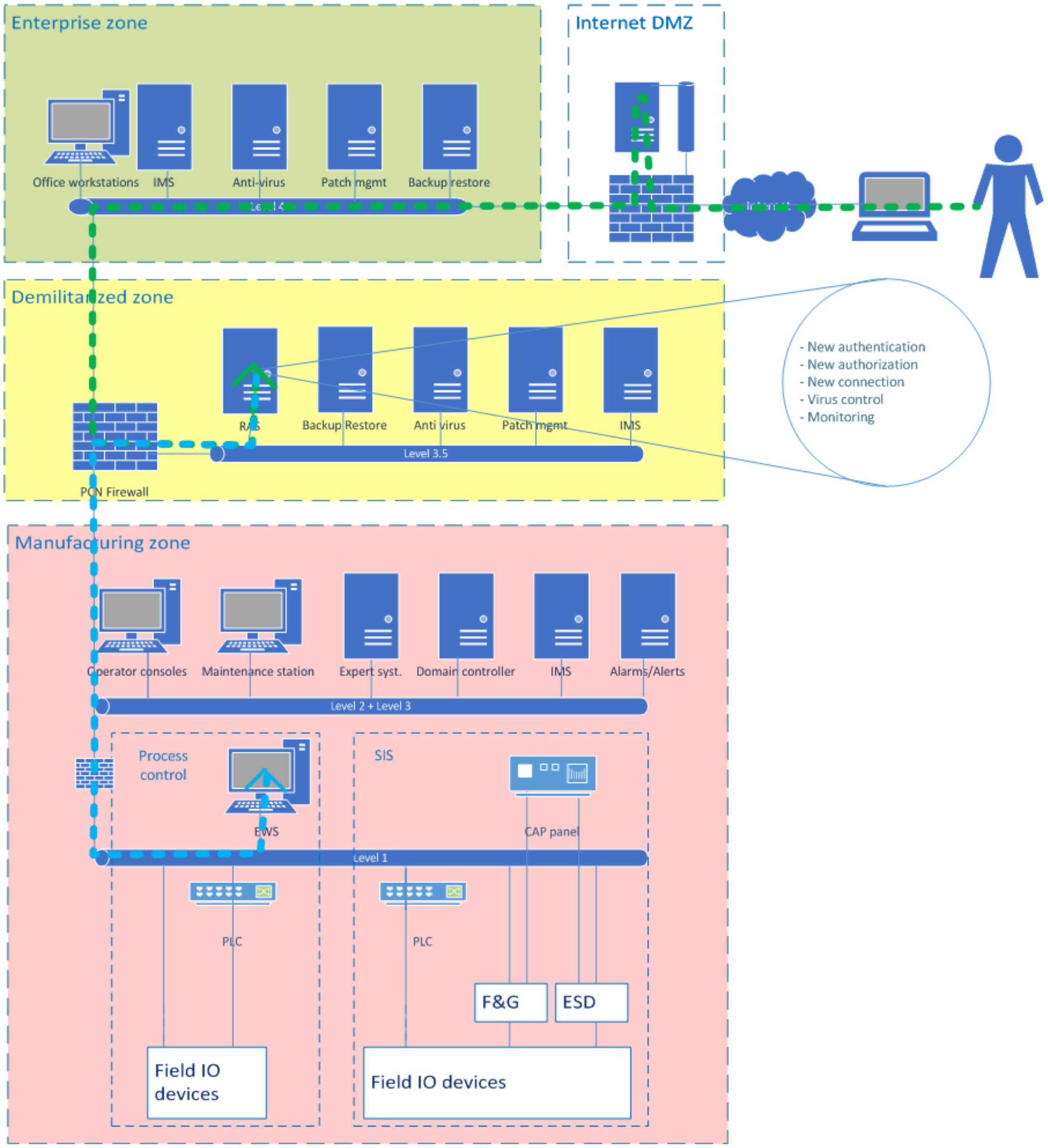


Figure 4-5 Zones and conduits for remote access solution

The best practice for building the remote access solution is described in [5.2.6].

4.4.6 Zones and conduits for remote control rooms

The figure below illustrates a typical remote control room scenario. In practice, there will be several applications/computers in different zones at the plant that need channels to communicate with the remote control room. Each of these zones will require a corresponding zone at the remote control room, preferably with the same security level.

Examples of zones in local plant may be zones for HMI, CAP, ESD, CCTV, PA etc. Based on criticality and consequence, these zones may require different security levels (SL).

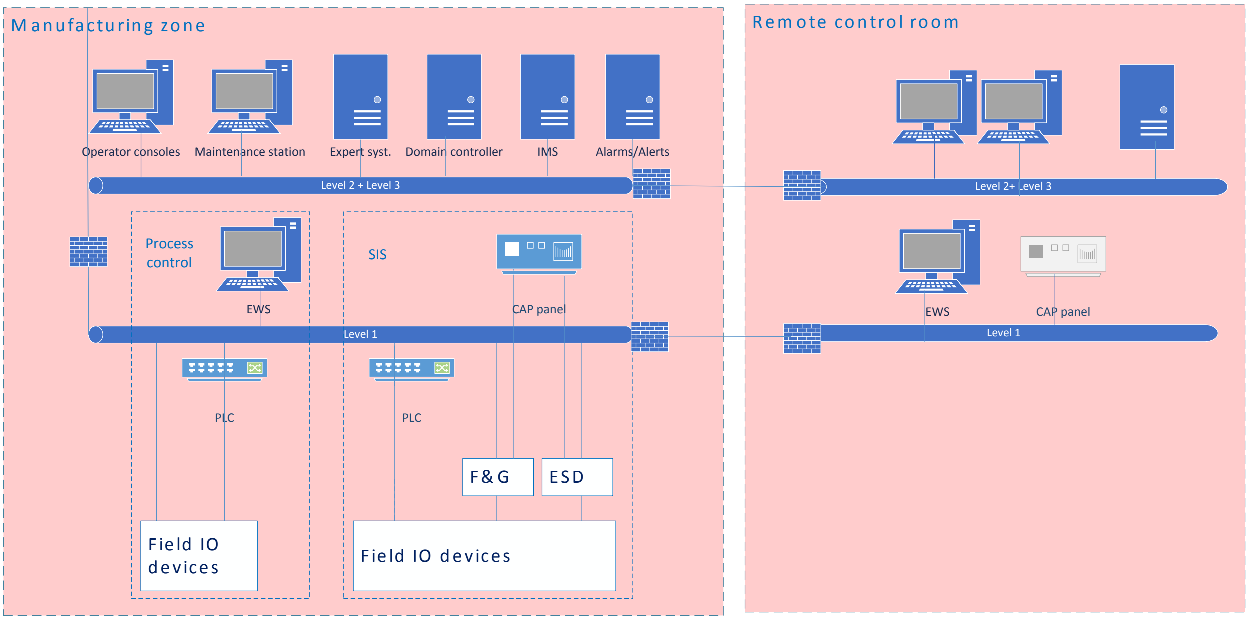


Figure 4-6 Zones for remote control rooms

Conduits are used to connect the zones. To ensure good cyber security, it is considered good practice to use the following design criteria when implementing the conduits:

— Conduits connecting zones with high criticality should be designed with two separate network routes between LCR and RCR. This to ensure high availability.

— Conduits connecting zones with high criticality should have functionality for mutual authentication, verification of packet integrity and encryption of packets. This to avoid un-authorized access, man-in-the-middle attack scenarios and/or eavesdropping.

It is considered good practice to implement conduits between high criticality zones using secure tunnels between the zones. The endpoint of the conduit should be within the different zones. Solutions should be based on well accepted network security standards (see /11/).

— For L3 communications (that can be routed using IP routing), IPSec in tunnel mode can be used. Mutual authentication, packet integrity, encryption and anti-replay mechanisms are included in this standard, and should be configured. Avoid splitting the tunnel and allow it to terminate on the equipment at the border of (or within) the zone.

— For L2 communications (zones A1 and A2 need to communicate on L2 because they belong to the same IP subnet – or because non-IP traffic is used) IEEE 802.11AE (MacSEC) can be used. Mutual authentication, packet integrity, encryption and anti-replay mechanisms are included in this standard, and should be configured.

Protect the management interface of the solution used to implement the conduits in the same way as you protect the hardware/software and information within the zones.

Establish procedures and responsibilities for encryption key management. Such keys are normally handled in digital certificates which have an expiry date (typically three years). After the key has expired, the devices stop communicating. A common overview of certificates and periodic reviews should be established or this service may be delivered by an external certificate authority.

4.4.7 Documentation of zone and conduit characteristics

Input:

- Initial topology drawings (high network topology diagrams, control system topology drawings).
- Results of the high-level risk assessment.

What input should look like:

- This document provides a generic zone and conduit drawing. The different SAS vendors may have different preferences.

Output: Updated system architecture diagrams and an inventory describing the SuC, perimeter and entry points

What should output (delivery) look like (content and formats):

High-level IACS network topology from typical vendors in the oil and gas industry.

Figure 4-7 shows a simplified drawing of zones. In this figure, only two process zones (P and Pn) and two safety zones (S and Sn) are shown. P and S could e.g. be for a critical turbine system with a high security level, while Pn and Sn could be for a less critical sand-monitoring system with a low security level. The figure also shows examplesof conduits connecting the different zones.

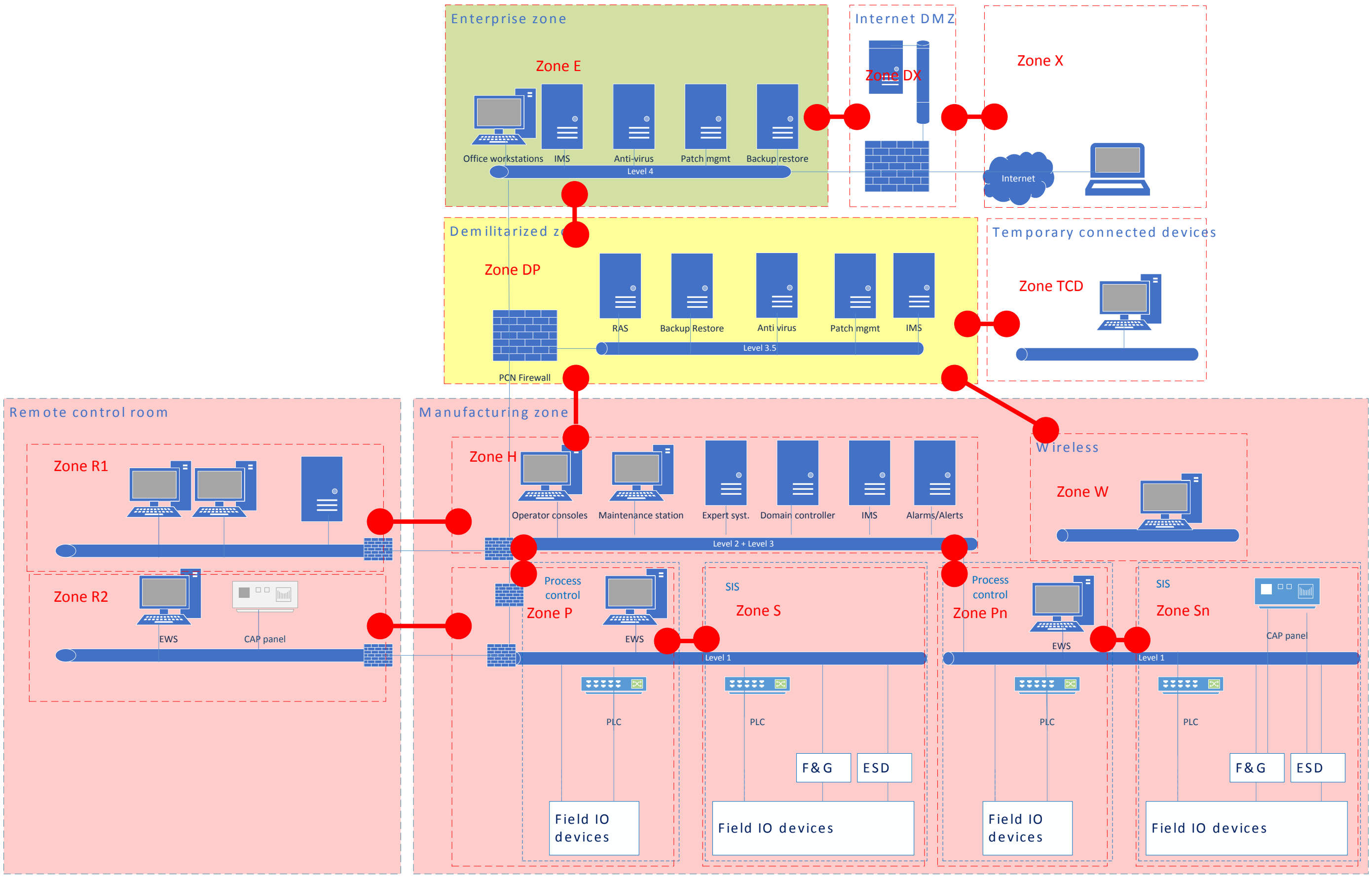


Figure 4-7 Example zone and conduit drawing

The following characteristics should be documented for zones and conduits:

- name and/or unique identifier
- physical and/or logical boundary
- entry points (integrations, wireless, remote access …)
- list of external data flows (and internal data flows within a zone)
- assets (equipment and software)
- connected zones
- security requirements
- SL-T
- security policies
- assumptions and dependencies.

The conduits and their numbering should be reflected in network filtering rules for routers and firewalls.

4.5 Detailed cyber security risk assessment of zones and conduits

This sub-section provides a brief description of the detailed risk assessment. Further information can be found in App.B. The detailed risk assessment is initially conducted in the FEED phase, butis continuously updated, according to similar principles, in the project and operations phase.

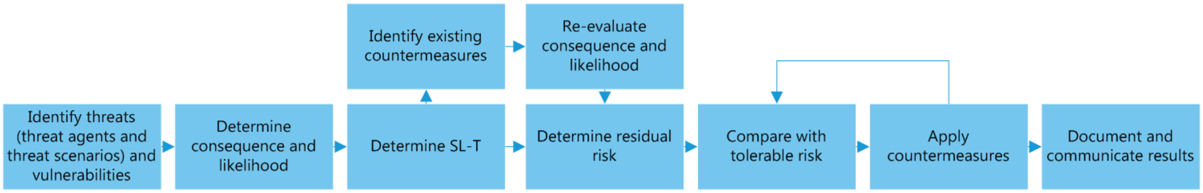

Identify existing countermeasures
Re-evaluate consequence and likelihood
Identify threats (threat agents and threat scenarios) and vulnerabilities
Determine consequence and likelihood
Determine SL-T
Determine residual risk
Compare with tolerable risk
Apply countermeasures
Document and communicate results

Figure 4-8 Overview of the detailed risk assessment workflow (described in App.B)

The following recommendations apply to the detailed risk assessment:

- Use a scenario-based approach.
- Do qualitative risk assessments, since these are less complex and will help to compare risks across different projects and systems.
- Do the risk assessment on groups of systems when that is expedient. For example – if a vendor delivers a SAS system that consists of several zones, it can be reasonable to do a risk assessment of the complete SAS system.
- The EPC contractor should facilitate risk assessments, with relevant system/package vendors' risks aligned with the chosen risk methodology.
- Describe some assumptions that will be needed during the risk assessment:
    - External interfaces should be identified and described by the project.
    - Asset owner should provide description of policies and procedures. For example, existing work processes for operation and maintenance.
    - Asset owner should describe mechanisms used for management of barriers.
    - Internal interfaces and flows in the zones should be considered as these can be exploited by a threat agent.
- Reuse risk assessments for similar systems where applicable.
- Use a common scale calibration. This will make it easier to compare inputs and analysis across projects and systems.

— Choose the highest risk associated with the worst-case scenario when aggregating risks.

The output from the high-level risk assessment and the separation into zones and conduits gives a good overview of the software-based systems that are critical for the operation of the given installation. A detailed risk assessment should be carried out for each zone and conduit. However, it is important to prioritize systems with high consequences where threats are relevant.

The detailed risk assessment is usually based on workshops covering all zones and conduits. The output should be presented to local/regional top management and mitigating actions should be incorporated accordingly.

4.5.1 Asset owner approval

The asset owner or appropriate authority will be required to accept SUC's residual risk. If the residual risk deviates from the tolerable risk (ALARP), then the appropriate management system to close gaps should apply (e.g. project punchlist, MOC, deviation).

4.5.2 HSE requirements for risk assessment

The UK HSE guidance /22/ includes specific guidance for the risk assessment of SIS zones. To follow this guideline, it is recommended to include the guidance in Note 6 of the document. This will give an updated risk assessment for countermeasures considered for SIS.

4.5.3 IEC 61511 (edition 2) requirements for risk assessment

The IEC 61511 standard for functional safety /7/ has in edition 2, 2016 included requirements for a cyber security risk assessment in chapter 8.2.4. To follow these requirements, it is recommended to assess all project phases (from design to operation) in the risk assessment.

The standard also refers to ISA TR 84.00.09 /21/. To follow the risk assessment requirement in this standard, the hazards and threat agents significant for a SIS as described in chapter 5 should be included in the risk assessment.

SECTION 5 PROJECT PHASE

5.1 General

In the project phase, systems are built and tested. After testing, the systems are handed over to operation organisation.

5.2 Detailed engineering

The deliverables from a project's detailed engineering phase include procurement specifications, construction drawings, and evidence of design verification. Specific security controls should be considered to identify, prevent, detect, respond and recover from a cyber security incident /23/.

During the detailed engineering, it must be assured that the delivered solutions' security level achieved (SL-A) corresponds to the required SL-T. The risk due to any lack of compliance should be mitigated.

Microsoft Windows is the most commonly used operating system in IACS. It is used in this section to provide an example of how to apply security controls in computer operating systems.

5.2.1 Hardening

All computers should be hardened. One of the most important hardening steps is to keep the installed software and enabled hardware features to a minimum on the computers and network devices. The attack surface will as a general rule increase with the number of applications and services installed. This is also true for the server roles and network device features that can be added, as adding a new role or feature will increase the attack surface.

Requirements:

The hardening requirements are given in IEC 62443-2-4 /2/ SP.02.03, SP.03.05 and IEC 62443-3-3 /4/ FR2, FR7.

The security of the control system is based on the security mechanisms of the operating system and directory service used. The operating system default settings are not sufficiently secure, and several hardening steps should be implemented to increase the security.

All unnecessary features in network devices that are enabled by default should be disabled.

How to implement:

The hardening of Windows-based systems should be centrally controlled in the active directory through group policy objects (GPO). The main principle is that one GPO should be created for each defined group of computers and users. Organizational units (OU) can be created to enable the special treatment of computers and users by linking group policies to these units. Group policies can be used to apply specific settings, rights, and behaviour to all servers within an OU. When group policy is used instead of manual steps, it is simple to update multiple computers at the same time with any changes that might be required.

A redundant configuration should be used, with a primary and secondary domain controller that will control the Windows security of the control system.

Request hardening documentation from vendors and follow the guidance given in the documentation. If no vendor guidelines for system hardening exist, hardening should be implemented based on commonly recognized practices and tested during system implementation. The Microsoft security compliance manager (MSCM) is a Microsoft security accelerator that can be used to create hardening GPOs that target specific computer roles. The Microsoft security configuration wizard (SCW) can create server-specific hardening GPOs, analyse the servers' software and services and find required firewall configurations, etc. The SCW can create a GPO for centrally managing the settings.

Only secure access methods like HTTPS and SSH (SSH 2 or OpenSSH 2.3.0 or higher is required) should be used. These should be enabled on required device ports only. HTTP access and other unused management protocols shall be disabled in network devices. Unused network ports should be disabled and assigned to an unused VLAN where possible.

The local administration of network devices like firewalls and switches should be prevented after the initial configuration. The network devices should then be controlled by remote administration with centralized account management only. The encryption of passwords stored in the configuration files must be activated since there will still be a local account for fall-back situations where the centralized access control mechanism cannot be reached.

If no configuration is done, VLAN 1 is by default used to manage switches, which implies that VLAN 1 may end up spanning the entire network across zones. To prevent VLAN 1 from becoming a backdoor, it should be disabled. The proprietary VLAN Trunking Protocol (VTP) automatically configures VLANs across several switches, but it introduces a risk that an administrator unintentionally may create an error that propagates the entire network. Hence, the VTP should be disabled and VLANs should be manually configured.

5.2.2 Account management

Differentiated access to applications and services must be implemented on all computers and systems, in order to make access for less privileged users possible. This chapter describes how to set up account management in the detailed engineering phase. Information about how accounts are managed in the operation phase is described in [6.2.1].

Requirements:

The requirements for account management are given in IEC 62443-3-3 FR1, FR2 and IEC 62443-2-4 /2/ SP 09.01 -SP 09.09.

The account management system should ensure that personal and unique user accounts to be used. The only common accounts allowed in the system should be the one used by the operators in the control-room. In addition, there may be a need for service accounts, however these should have stricter password complexity requirements. It is recommended that one service account should only be used for one specific service or well-defined group of services.

Password policies should be implemented in a domain enforcing strong passwords and requiring password changes at given intervals for interactive users. Asset owner rules for password policies should be followed, including password length, periodic change of passwords, lockout of users, etc.

All computers should be automatically locked after a period of inactivity. Computers in the control-room are excluded from this requirement when the common operator account is logged on.

The built-in administrator and guest account should be disabled. These two accounts should never be used. A new local administrator account must be created to replace the built-in account.

The secure storage of account information and passwords and documentation of these procedures is a vital step in the handover to operation (see [5.6]).

How to implement:

For control systems based on Microsoft Windows, active directory should be used as the catalogue service since it is already an integrated part of the operating system. This makes it possible to centrally control user permissions, logon requirements and password requirements. Password change management for domain accounts should be controlled by GPO. All service accounts and common accounts should have passwords changed manually.

Access to resources should be controlled by a method called role-based access control (RBAC). This simplifies user and resource management and tracking of permissions. The principle of RBAC is to assign permissions to a role rather than to a user directly. The role represents the sum of permissions needed for a person to perform a defined job in context of the role.

- Roles are defined based on a defined job.
- Permissions are defined based on job responsibilities.

The benefit of using RBAC is strict control of users and permissions spanning the whole environment. The RBAC model enforces the least privilege principle. RBAC also facilitates an easy method to add or revoke permissions individually or to a group of people. It is recommended to limit the number of roles to as few as possible e.g. read-only, operator, engineer and administrator.

The principle of segregation of duties should be implemented. A user with high privileges should not be allowed to give these privileges to others.

Most network devices can be configured to utilize RBAC. The network device will be part of the Active Directory Service just like a server or client, implemented with e.g. the RADIUS protocol. RADIUS protocol is preferred as it is an open standard supported by many vendors, including Microsoft and Active Directory (AD) which will be used as the catalogue service for AAA, however other protocols may be used. Microsoft Network Policy Server (NPS) is a module that can be activated on Windows Servers and can be used to integrate RADIUS with AD.

5.2.3 Patch management

Patch management is the process of managing software updates. This chapter describes how to set up patch management in the detailed engineering phase. Information about how patches are managed in the operation phase is described in [6.2.2].

Requirements:

The requirements for patch management are given in IEC 62443-2-4 /2/ SP 11.01 – SP 11-06. Information about patch management in the IACS environment can also be found in IEC 62443-2-3 /16/.

A patch management system is the best solution for distributing the patches. The patch management system should enable the asset owner to access patch status reports, information about which versions of patches that are installed on the automation solution software. A patch management policy should outline the requirements related to a new patch release, how to evaluate the impact of installing the given patch, and the roles and responsibilities of approving installation of patches. The patch management policy should also refer to a procedure on how to perform patching.

For non-Windows systems, vendor specific solutions may be used, or a generic vendor independent patch management system may be implemented.

How to implement:

For control systems based on Microsoft Windows, Windows server update services (WSUS) offers patch management services for many Microsoft products.

The computers should be centrally managed with GPOs that configure the computers to download updates automatically and notify when the updates are ready to install. This will make the security update installation start immediately when an administrator starts the installation.

Direct communication with Microsoft update services on the Internet should be avoided for the control system. A WSUS server hierarchy should be created where the control systems request updates from a dedicated control system WSUS server placed in a dedicated zone or in the DMZ. This dedicated server is connected to an upstream WSUS server that may be an integrated part of the remote access solution or located on the office network.

For non-Windows systems, vendor specific solutions may be used, or a generic vendor independent patch management system may be implemented.

5.2.4 Malware protection

Requirements:

The requirements for malware protection are given in IEC 62443-3-3 /4/ FR3 and IEC 62443-2-4 /2/ SP 10.01 – SP 10.05.

The malware protection product must be configured according to vendor guidelines to ensure it does not interfere with the control system operation and that the impact on performance and reaction times are negligible.

All computers in the system should have a malware protection solution installed. The latest version of a malware protection solution qualified by the vendor should be used. The asset owner should have formal documentation of instructions on how to install and configure the malware protection solution. It is important that the asset owner has an overview of the installed malware protection solutions and a procedure covering configuration of the malware protection solution. A recommendation is to test the malware protection solution to verify that malware can be detected (see EICAR test-string /14/). If the use of portable storage devices is allowed in the process domain, special procedures for malware cleaning of such devices should be established. In general, file transfer to the process domain should be performed through the remote access solution (see [5.2.6]).

The malware protection solution configuration should be harmonized between the asset owner and the vendor to avoid unwanted behaviour, such as performance degradation due to the scanning of files that are frequently modified by the control system.

How to implement:

The malware protection solution should have a centralized management server, placed in a separate zone or in the DMZ, which provides policies, updates and reporting functionality to the malware protection solution. A centralized management server makes sure all computers are protected and administrators can easily check the status of all computers. Alerts and potential status information should be sent to a plant-wide monitoring system.

Whitelisting of software is a supplement to traditional antimalware solutions that may be implemented for high-risk systems. The administrative burden of such solutions may be high due to changes in software based on patching.

5.2.5 Backup restore

The continuous availability of the systems and the data they provide are critical to operations. In order to minimize any potential downtime for systems and loss or corruption of data, projects need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure. This chapter describes how to set up backup and recovery in the detailed engineering phase. Information about how backup and recovery are managed in the operation phase is described in [6.5.2].

Requirements:

The requirements for backup and recovery are given in IEC 62443-3-3 /4/ FR7 and IEC 62443-2-4 /2/ SP 12.01 – SP 12.09.

Detailed procedures for restore and recovery based on all the different backups taken must be created during installation of the system. The asset owner should have the capability to continue normal operations during backup, and the ability to restore full operations as quickly as possible during recovery.

How to implement:

The system delivered may have an integrated backup and restore application. In such case, it should be the preferred method to make a backup of system information. System backups can typically be scheduled to take place at recurring points in time to perform backups on a running system.

The need for additional backups to complement the system backup for applications or process data storage running on application servers must be evaluated. The configuration files of network devices should be transferred to the backup server. Encryption of passwords stored in the configuration files must be activated.

For easy recovery of the computers in the system in the event of failure, a general purpose disk imaging backup system is needed. Such solutions can typically create both full (or base) images and incremental images on running computers. Numerous options for scheduling and storage of images are available.

The recovery operation for a disk imaging backup system can be done by booting the computer in a recovery environment and restoring the hard disk data from a central management console. Another distinguishing feature of these system are their ability for hardware independent recovery. As computer hardware models change rapidly this is a critical feature if a computer needs to be exchanged with a new one.

A separate backup server should be assigned the task of managing the different backup types used. The backups are typically created by the server which holds the data and are sent to the backup server for storage. This will be the primary storage location. The data should be copied to a secondary location, either to a physical media that is detached from the system and stored in a safe location, or be transmitted over the network to a secondary backup server in a different location. The solution shall be designed to ensure that malware (e.g. a ransomware virus/worm) does not affect backup availability.

5.2.6 Remote access

5.2.6.1 Overall principles

Due to large distances, costly transport and safety requirements, it is practical to allow remote online access to oil and gas installations for maintenance. By doing so, a large cyber security attack surface is exposed, and it is vital to design and build a secure solution. It is recommended to select an operator-supplied solution designed for this purpose. Operators may allow vendor-specific solutions or third-party solutions, but the operator must still verify conformance to this recommended practice.

The requirements for remote access are given in IEC 62443-2-4 /2/ SP.07.01-SP.07.04.

The concept for secure remote access is also described by CPNI's *Configuring and Managing Remote Access for Industrial Control Systems*, NIST-800-46 /9/ and NERC's *Guidance for Secure Interactive Remote Access /12/*.

Good practice:

— Production data should in general not be accessed at the production equipment, but should be transported to the enterprise network through the process data/plant information solution.

— Remote access should be authorized manually or automatically based on a work-order system. It is essential to close permissions after the work is finished, but care should be taken in terminating ongoing sessions.

— Transfer of files should be integrated into the remote access server solution. End-users should be able to upload files to a storage area in the remote access solution. These files should be accessible from computers in IACS local on the plant (if needed). Files should be scanned for malware when stored and at periodic intervals. It is also considered as good practice to scan files transferred for unknown malware using a sandbox solution.

— Ensure service computers are managed, hardened, patched and updated with latest antimalware software before being connected to IACS zones.

The following security barriers are needed for a secure remote access solution:

5.2.6.2 Identification and authentication control

Authentication describes the process of positively identifying potential network users, hosts, applications, services and resources using a combination of identification factors or credentials.

Different mechanisms can be broken down into:

— something you know (password or PIN)

— something you have (token or object that is unique)

— something you are (fingerprints, facial features, etc).

Requirements:

The requirements for authentication are given in IEC 62443-2-4 /2/ SP.09.01-SP.09.09 and IEC 62443-3-3 /4/ FR1.

Multifactor authentication should be used for remote access. Remote users should have unique accounts so that an account management process can identify the users. Other login credentials should be used to the RAS than to the office network.

Whenever feasible, mutual authentication should be implemented. One example is to give the remote user the ability to verify the legitimacy of the remote access server before providing authentication credentials.

It is recommended to have timeout for inactivity during the authentication process.

How to implement:

Select remote access solutions with integrated support for two-factor authentication. SMS codes may be used for less critical systems, but the risk of e.g. SMS forwarding to e-mails should be considered. For critical systems, tokens or smartcards are recommended with procedures for secure delivery to the correct person. Make sure cryptographic mechanisms are used for transferring authentication information.

More information:

More information can be found in NIST SP 800-63-3 /17/.

5.2.6.3 Authorization

Authorization is the right or permission that is granted to a system entity to access a system resource. Proper authorization is dependent upon authentication.

Requirements:

The requirements for authorization are given in IEC 62443-2-4 /2/ SP.09.01-SP.09.09 and IEC 62443-3-3 /4/ FR2.

Remote access privileges should be established in accordance with the organization’s authorization security policy. The accounts should be role-based and grant users only those privileges and access to resources that are needed to perform their particular job /1/. RBAC reduces the complexity and cost of security administration in networks with a large number of intelligent devices, such as in IACS systems.

How to implement:

The best practice to implement an authorization solution is to establish one common user repository. This tool should enable the definition of roles, and the target systems should retrieve user rights from the central source. Such central solutions must be redundant, and backup local accounts must be available.

It is recommended to establish a solution for read-only access.

Remote access with write permissions should be authorized manually or automatically based on work-orders in the work-order system. It is essential to close permissions after the work is finished, but care should be taken in terminating ongoing sessions.

5.2.6.4 Zones and conduits

Separation into zones and conduits is described in [4.4.5].

5.2.6.5 Monitoring

Guidance on monitoring is described in [6.3].

5.2.6.6 Encryption/endpoint authentication

Encryption is an effective way to achieve data confidentiality. In order to read an encrypted file, you need access to a secret key or password to decrypt it.

Requirements:

The requirements for encryption are given in IEC 62443-2-4 /2/ SP.03.08, SP.03.10, SP.04.02, and SP.07.04.

Currently, the following algorithms and key lengths are recommended:

- Symmetric encryption: AES 128 or better
- Asymmetric encryption: RSA 2048 or better
- Hash: SHA-224 or better.

Encryption devices used to protect the IACS should be thoroughly tested to verify that the technology is compatible with the application. This includes the verification of delays and other traffic characteristics of the implementation.

How to implement:

Whenever possible, full tunneling cryptographic technology should be used to ensure a secure communication tunnel from the external user, through the corporate network and to the RAS server (also called jump server or jump host). This can be achieved by using a VPN gateway, which should include both encryption and two-way endpoint authentication with digital certificates. The most common VPN technologies are:

- Internet protocol security (IPsec)
- Transport layer security (TLS (V 1.2 is required))
- Secure shell (SSH)(SSH 2 as implemented in OpenSSH 2.3.0 or higher is required).

More information:

Relevant requirements for encryption strength are given in FIPS PUB 140-2 /11/. There are also national requirements, such as e. g. the Norwegian NSM Cryptographic Requirements /13/ which may be relevant.

5.2.6.7 Hardening

Remote access components, especially the RAS server (jump server), represent a large attack surface, and must therefore be hardened according to best practice. Guidance on hardening can be found in [5.2.1].

5.2.6.8 RAS server

A RAS server (also called , jump server, jump host or jump box) is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. On-line access and file transfer to control systems from resources outside the process control domain should only be allowed through the RAS server.

How to implement:

The RAS server should be placed in a separate RAS zone or in the DMZ. The device should terminate the secured tunnel (e.g. IPSec tunnel) from the remote user, and perform a new authentication and authorization. Then a new tunnel/secured session based on another protocol (e.g. terminal server session) should be established to the target system. All target systems should be predefined in the RAS server.

The file transfer solution should implement a temporary storage area where remote users can upload files. After malware scanning, the files should be moved to a new storage area available from the process control domain.

It is recommended to use a RAS server from a vendor specializing in such products.

5.3 FAT

Since cyber security can also impact the safety of critical systems if a system is compromised, it naturally makes sense to integrate cyber security with the FAT. It is important to ensure the equipment/software is not tampered with in this phase. Testing of cyber security controls should be done as part of the FAT.

Best practice:

- Ensure cyber security is included in FAT planning.
- Protect the IACS system from the time it is installed to it is handed over to the asset owner. In this phase of the IACS lifecycle, control of physical access to the equipment is a good way to ensure it is not tampered with. Ensure equipment is stored and transported in a way that reduces the likelihood of unauthorized access.
- The FAT should include testing of security controls:
  - Verify and test that the controls specified in the CSRS are in place (backup and restore included).
  - Perform a vulnerability scan to identify vulnerable software that should be fixed.
  - Network/interface load test.
- Consider to create a footprint (hash) of very critical systems (such as EWS) at FAT. This footprint can be verified at the commissioning site to ensure software and configuration files are not tampered with.
- In the case of virtual machines, consider to take snapshot of virtual machines. Store the images in a secure way, and verify that the approved version is used at commissioning.
- The project should demonstrate a successful backup and restore test during FAT for all systems that are included in the backup and restore procedures.
- At the close of the FAT the asset owner or delegated representative should be provided with a full copy of all software applications and configuration data. This version will be used to restore the system at the commencement of the commissioning phase.

5.4 Mechanical completion phase/SAT

In this phase, the IACS system is powered up at site for the first time, and many new connections to the system are made (interfaces, packages, temporary stations etc). This period is normally very busy at site and a lot of people have access to the instrument rooms where IACS equipment are installed.

The owner of the IACS should have the full authority to regulate when and who can connect to the IACS. This is very important as it usually is a high focus on progress in this project phase.

Best practice:

- Ensure that critical server and network components are stored at a safe place at site prior to being installed in the instrument rooms.
- Include cyber security checks according to CSRC in the SAT/power-up procedure.
- Ensure key personnel on MC activities are aware of cyber security risks and have the necessary awareness training.
- Have a daily or weekly review of the users allowed to access the IACS system.
- For every external connection into the IACS, there should be a cyber security checklist prior to connection and after the connection is tested and approved. The checklist should ensure that the CSRS for the connection is maintained in the MC and commissioning period. The checklist can be included in the SAT procedure or be a separate MCCR sheet per interface.
- On the MCCR for every server/network component, include cyber security checks according to CSRS.
- Any change of the IACS that affects the CSRS should be assessed and approved by cyber security team before being implemented.

5.5 Commissioning phase

Since cyber security can also impact the safety of critical systems if a system is compromised, it naturally makes sense to integrate cyber security with the commissioning activities. It is important to ensure the equipment/software is not tampered with in this phase. Testing of cyber security controls should be done as part of commissioning phase.

Best practice:

1) Verify that the installed software and configuration correspond to approved FAT versions or approved changes.
2) Asset owner policies for the management of removable media and remote access must now apply.
3) Ensure cyber security is included in the planning of commissioning phase.
4) Ensure key personnel on commissioning are aware of cyber security risks and have the necessary awareness training.
5) Protect the IACS system from being tampered with on the commissioning site. A lot of people from many companies are present on the commissioning site and proper access controls should be in place to reduce the likelihood of unauthorized access to IACS. Ensure unauthorized people do not have access to the IACS on a 24/7 basis.
6) Ensure that the IACS components:
    a) Have implemented the cyber security controls described in the CSRS. Ensure proper access control (username/passwords) is enabled.
    b) Can be updated with the latest security patches and antimalware software.
    c) Can have remote access by a managed remote access solution (avoid temporary solutions with poor cyber security controls – backdoors included).
    d) Usage of USB storage is blocked or that procedures and equipment for malware scanning are established.
7) Roles and responsibilities for cyber security must be agreed and understood. It is the package vendor, contractor or asset owner that is responsible – before and after equipment are commissioned.
8) Lock equipment cabinets.

9) Logging and monitoring should be enabled to be able to detect possible incidents.

10) Ensure cyber security incidents and/or potential incidents are reported to the asset owner.

5.6 Handover to operations

The handover from the project phase (EPC contractor) to the operation phase (asset owner) can introduce cyber risks if not done in a structured manner. The step of going from project phase into operation includes a significant change of personnel over a short time-frame. For the account management system, it means many new user accounts must be created and user accounts of personnel involved in the project phase should be terminated or disabled. From day one of operation, the new personnel should be familiar with the security roles and responsibilities and the security procedures related to all processes of the cyber security framework. Experience shows that for many operational assets this is not established in due time. During handover, a reassessment of risk should be completed to ensure the system delivered matches the design requirements.

A good practice is to involve operation personnel in the final testing of the project phase. Checklists should be created to verify that all system documentation is available and procedures should be established to securely store system passwords.

SECTION 6 OPERATIONS PHASE

6.1 General

In the operations phase, systems installed to ensure the security of the operational asset should be maintained and monitored. Security should be part of the change management processes and approved incident response and recovery procedures should be in place.

6.2 Maintenance

6.2.1 Account management

The proper management of user accounts is vital to secure the system and provide assurance of actions performed. The setup of the account management system is described in [5.2.2].

Requirements:

The requirements for account management are given in IEC 62443-2-4 /2/ SP.09.01-09 and IEC 62443-3-3 /4/ SR1.3.

Personal and unique user accounts should be used. Users who are allowed administrator access should have a separate account with these privileges in addition to their normal user account. The user accounts should give different access rights and privileges based on the user’s role and function.

Unsuccessful user logon attempts should be logged. Accounts that are no longer required should be disabled or removed.

Procedures should be developed for handling new accounts and for changing and removing of accounts. Users that leave the project should have their accounts terminated. If it is only a temporary leave, the account may be disabled.

How to operate:

The following procedures for user management must be defined and communicated to relevant stakeholders:

- Request process for a new user or changes to an existing user, which should include:
  - administrative processes for approval by the asset owner
  - general cyber security training requirements
  - work on hot plant procedure training
  - user role-specific training requirements
  - confidentiality agreement.
- User account modifications:
  - creating a new user
  - modifying a user
  - disabling a user
  - resetting a user account password
  - removing a user.

In addition, guidelines on how to document user setup should be prepared.

6.2.2 Patch management

A patch management policy should be in place to operate a patch management system. This policy should describe the process to evaluate the risk of implementing patches. If the risk of applying patches is greater than the risk of running un-patched, the policy for delaying patching and implementing other risk mitigation actions should be defined.

Patch management in the operations phase is a dynamic, ongoing process, where it may be required to adjust and improve parts of the process. The organization should routinely analyse its patch management process and routines to find areas that can be improved. The setup of the patch management process is described in [5.2.3].

Requirements:

The requirements for patch management are given in IEC 62443-2-4 /2/ SP11.01-SP11-06. Information about patch management in the IACS environment can also be found in IEC 62443-2-3 /16/.

Patches can only be distributed after approval has been given by the system vendor. A patch management system is the best solution for distributing the patches.

Many updates require restart. Restart can only be performed if this has been cleared with the system and data owners. Make sure to have a consequence analysis and a rollback solution.

Patch management needs to cover more than operating system security updates. Other examples are control system software, third-party software, computer and network device firmware. All these should be closely inspected for critical security issues on a regular basis. If there are any such issues, the patch or upgrade should be installed as soon as possible.

How to operate:

The control system vendor should test all security updates for third-party software which the system relies on. This is to ensure that the updates do not change or disable functionality used by the control system.

A conformance list for security updates should be released within a time period that is agreed upon between the asset owner and the vendor. A typical example for a major control system vendor is 7 days after patch release, but for smaller third party vendors this time may be significantly longer. When this is done, patches should be installed on the running plant system as soon as possible. It is important that a risk evaluation is conducted prior to installation of patches.

Approved security updates can only be installed as part of a planned maintenance process. An updated consequence analysis which describes the effects of restarting each computer must be available.

Control system software updates and third party software updates should also be validated in the process used by the system vendor for testing security updates. Network devices must be updated with the latest stable software/firmware version.

For all software or firmware updates where system vendor validation cannot be provided, a test system should be used to verify the operation before implementation in the production system. For critical systems, a test system may also be a necessary precaution even if system vendor validation is present, due to the risk of issues due to a different system environment.

More information:

Recommendations for how the asset owner and IACS product supplier should cooperate on patch management are given in IEC TR 62443-2-3 /16/.

6.2.3 Malware protection

The malware protection product must be configured to ensure it does not interfere with the control system operation, and that the impact on performance and reaction times are negligible. The setup of the malware protection solutions is described in [5.2.4].

Requirements:

The requirements for malware protection are given in IEC 62443-2-4 /2/ SP.10.01-SP.10.05 and IEC 62443-3-3 /4/ FR3.

All computers in the system should have a malware protection solution installed. The latest version of a malware protection solution qualified by the vendor should be used.

Definition files for the malware protection solutions should be tested by the vendor to ensure that the new definitions do not detect legal code as a false positive. Approved engine updates should also be published on a regular basis.

How to operate:

The vendor should verify definition files for the qualified malware protection solution on a regular basis to ensure that the new definition files do not detect legal code as malicious. Definition files should thereafter be uploaded to the running plant system as soon as possible. A typical example is to update definition files at least every week.

The centralized management server collects updates from a protected location in the remote access solution or on the office network and stores them in a local repository. The updates are then collected by the computers running the malware protection software.

6.2.4 Vulnerability management

A cyber security risk is the likelihood of a threat exploiting a vulnerability that has negative consequences for an IACS. A key element in managing these risks is managing new vulnerabilities in the IACS. This includes software vulnerabilities, but also vulnerable configurations. Such vulnerabilities are discovered continuously, and since they may change the risk picture in IACS, they must be managed. The goal is to prevent exploitation of vulnerabilities. An example includes Stuxnet exploits of software vulnerabilities in specific systems. It is of vital importance to identify whether the IACS is vulnerable to this threat and take actions to close the software vulnerabilities to prevent them from being attacked.

Requirements:

The requirements for vulnerability management are given in IEC 62443-2-1 [draft version] chapter 12.6 Technical Vulnerability Management

How to:

Vulnerability management is a continuous process. It includes having an organization with roles and responsibilities to manage the process. Information should be received from relevant sources like software vendors, system vendors or various cyber emergency response teams (example ICS-CERT).

After information about a new vulnerability is received, the information should be evaluated to obtain a good understanding of how it may introduce new risk. This evaluation should include how the vulnerability can be exploited, and whether the IACS are exposed for the vulnerability. Based on this evaluation it should be decided whether actions to close the vulnerability are necessary or not.

If actions must be taken, the next step is to identify which IACS are vulnerable. This can be identified by comparing the vulnerable software to the IACS software inventory lists.

After the vulnerable IACS are identified, a more thorough analysis of the vulnerable IACS should be performed, and measures to close the vulnerability should be identified and implemented. Typical measures can be to install a security patch or change a configuration.

6.2.5 Portable media and portable computers

It is not recommended to use portable media and portable computers. Solutions for file transfer in a RAS should be used instead of removable media. If portable media and computers are necessary, there should be a documented policy ensuring the use of portable media and computers meets all of the following requirements:

— All portable data storage media, including portable computers, should be inspected and found to be free from malicious software by using a current version of antivirus software and signature files before being installed in, or connected to, an IT component in the IACS. The anti-virus software used at the time of initial inspection should be of the latest or second latest version and the signature files used should be no older than 7 days after qualification of the signature file by the vendor.

— Restrict portable computers from connecting to an alternative or secondary network, e.g. to download software or updates, while being connected to the IACS (via a network or discrete/serial connection).

— Require the removal of data prior to the disposal or removal of equipment containing storage media. This includes, but is not limited to, portable computers and other devices containing (configuration) information such as network devices (e.g. switches, routers, firewalls). Reformatting storage media is not considered an appropriate method for secure overwriting, as technology exists to recover data from (re)formatted media. If overwriting or removal of data or licensed software is unfeasible (e.g., caused by media failure), other methods should be considered, such as physical destruction.

— Restrict portable computers and other IACS IT components used for configuring/engineering IPS from being used for other purposes.
— Require registration and authorization of portable computers and other devices to be connected to the IACS, including wireless devices. These computers and other devices should follow the applicable policy for hardening and configuration management.

6.3 Monitoring

A cyber security defence must be monitored both to make sure the countermeasures are operating according to intention and to detect and initiate a response to incidents. Incident response and recovery is handled in [6.5], and the system and procedure for keeping countermeasures updated are described in [6.2.2]. This chapter focuses on how to monitor that the countermeasures are operating as intended and that alarms and event log entries are generated, collected, retained and analysed.

Requirements:

The requirements for event management are given in IEC 62443-2-4 /2/ SP.08.01-SP.08.04, in IEC 62443-2-1 /1/ chapter 12.4 and in 62443-3-3 /4/ FR 6 – Timely response to events.

How to operate:

The asset owner should establish policies and guidelines on how to collect, report, preserve and correlate alarms and events from the systems able to detect security violations. A security information and event management (SIEM) system should be considered.

For security level 1, local logs and manual inspection are sufficient. The overall intention is to be able to produce evidence information after an incident is identified. Service providers should be able to detect, report to asset owner and respond to incidents. The asset owner should be given access to events over a network. Log information from antivirus products and firewalls should be available.

For security level 2 and higher,information must be actively collected. The recommended approach is to establish a central system where alarms and relevant events are collected. The system should have search facilities to do manual threat intelligence or support advanced threat intelligence. These facilities should enable a proactive response and evidence collection. It should be possible to verify that the security mechanism is operating as intended, for example by the virus protection vendor supplying a test-virus.

At security level 2 and higher, the performance of all security mechanisms must be continuously monitored. Monitoring devices like IDS or probes should be placed at selected perimeter locations.

To get management attention and to prioritize activities, a good understanding of the actual threat situation is needed. The alarm and event system should be capable of producing report with statistics about security systems availability, alarms and events.

To enable alarm and event correlation, clock synchronization for all systems should be implemented.

The processing load and network capacity of logging and alarming on older control systems must be considered. The size of log-files may as well be considered. Define a rotation strategy and decide when to overwrite or back up logs.

Create events that humans can read and analyse and include unique identifiers.

6.4 Managing change

6.4.1 Configuration management

Proper change management and stakeholder engagement processes should be followed when component information is changed or updated. A log of changes should be kept current.

Requirements:

An inventory of all IACS IT components should be built and maintained.

How to operate:

The following information should be documented for each component:

- unique identifier or network address or MAC address
- operating system name and version
- application software name and version
- hardware manufacturer and model
- device type
- security level (SL)
- restore time objective (RTO)
- restore point objective (RPO)
- custodian.

Documentation of the IACS architecture should be maintained using logical network diagrams identifying the IACS IT components and describing the interconnections between IACS IT components in the infrastructure.

6.5 Incident response and recovery

6.5.1 Incident response

An incident response capability is needed to rapidly detect incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore services. The incident response lifecycle includes:

- Preparation (establish an incident response plan, implement tools and create and train procedures).
- Detection and analysis (quickly detect signs of an incident, understand sources, and prioritize and analyse incidents).
- Containment, eradication and recovery (isolate affected environments, stop ongoing activity and restore systems to original state).
- Post-incident activities (learn and improve, report).

Requirements:

The requirements for incident response handling can be found in IEC 62443-2-4 /2/ SP 08.01- SP 08.04.

The service provider should ensure there are processes and systems that detect security incidents and report them to the asset owner. The asset owner should have procedures in place to respond to incidents that compromise operations and safety. There should be an incident response team that acts according to defined procedures.

How to operate:

Each location should implement and maintain an IACS IT security incident management procedure, aligned with the companies' information risk incident management (IRIM) process, which includes the following elements:

- site responsibility to report all suspected or actual IACS IT security incidents via the global IRIM process
- roles and responsibilities, management, communications and escalation
- containment, investigation, resolution, lessons learned and close out.

As imminent threats are handled as incidents, the IACS IT security incident management procedure should also address:

- a threat response structure specific to the site, documenting a number of actions to be executed
- roles and responsibilities concerning the follow-up of an imminent threat
- response time and service time.

More information:

NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* and NERC CIP-008 *Cyber Security – Incident Response and Response Planning*.

6.5.2 Backup and restore

Requirements:

The requirements are given in IEC 62443-2-4 /2/ SP 12.01-SP 12.09 and IEC 62443-3-3 /4/ FR7.

The asset owner should have procedures for restoring the Automation Solution or its components to their normal operation.

How to operate:

1. There should be a documented policy stating that all PCD IT components should have documented data backup and restore and hardware/software recovery procedures during all phases of the project until handover and acceptance by the operating organization. These data backup and restore procedures should also address the following requirements:

— Backup media should be protected from unauthorized disclosure or misuse.

— Backups should be capable of being restored on new IACS IT component hardware or a virtual host.

— Backups should be tested at a frequency determined by the IACS IT security project focal point. The data backup and restore systems and procedures used may be influenced by what the operating organization is already using. The project should collaborate with the operating organization to determine the optimal strategy.

2. All IACS IT components should have a recovery point objective (RPO) assigned and recorded in the IACS asset inventory register as follows. The project should ensure that data backup and restore systems and procedures are designed to support achieving these objectives.

— RPO-0, no tolerance for data loss; all components should be redundant.

— RPO-1, tolerance for data loss is 4 hours.

— RPO-2, tolerance for data loss is 24 hours.

— RPO-3, tolerance for data loss is 72 hours.

— RPO-4, tolerance for data loss is greater than 72 hours.

3. All IACS IT components should have a Recovery Time Objective (RTO) assigned and recorded in the IACS asset inventory register as follows:

— RTO-0, no tolerance for a recovery timeframe; all components shall be redundant.

— RTO-1, tolerance for recovery timeframe is 4 hours.

— RTO-2, tolerance for recovery timeframe is 24 hours.

— RTO-3, tolerance for recovery timeframe is 72 hours.

— RTO-4, tolerance for recovery timeframe is greater than 72 hours.

4. Documented and approved backup and restore procedures should be provided for all systems that will be installed in the IACS.

SECTION 7 REFERENCES

7.1 References

/1/ IEC 62443-2-1, Draft 7, Edit 5, 2015. *Security for industrial automation and control systems, Industrial automation and control system security management system.* International Electrotechnical Commission.

/2/ IEC 62443-2-4, 2015. *Security for industrial automation and control systems, System Security program requirements for IACS service providers.* International Electrotechnical Commission.

/3/ IEC 62443-3-2, Draft 6, Edit 3, 2015. *Security for industrial automation and control systems, Security risk assessment for system design.* International Electrotechnical Commission.

/4/ IEC 62443-3-3, 2013. *Security for Industrial Automation and Control Systems, System Security Requirements and Security Levels.* International Electrotechnical Commission.

/5/ IEC 62443-1-2, Draft 1, Edit 5, 2014. *Security for Industrial Automation and Control Systems, Master glossary.* International Electrotechnical Commission.

/6/ IEC 61508, 2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission.

/7/ IEC 61511, 2016. Functional safety, Safety instrumented systems for the process industry sector*.* International Electrotechnical Commission.

/8/ ISO/IEC 27001, 2013. *Information technology - Security techniques - Information security management systems - Requirements*. International Organization for Standardization.

/9/ NIST 800-46, 2011. *Guide to Enterprise Telework and Remote Access Security*. National Institute of Standards and Technology.

/10/ NIST 800-82, 2011. *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standards and Technology.

/11/ FIPS PUB 140-2, 2001 May 25, Security Requirements for cryptographic modules with change notices (12-03-2002). Federal information processing standards.

/12/ The concept for secure Remote Access is also described by CPNI's "*Configuring and Managing Remote Access for Industrial Control Systems*", NIST-800-46 and NERC's *"Guidance for Secure Interactive Remote Access"*.

/13/ NSM Cryptographic Requirements, Version 2.2 2008.

/14/ EUROPEAN EXPERT GROUP FOR IT-SECURITY, http://www.eicar.org/86-0-intended-use.html

/15/ NORSOK S-001 Technical safety, Edition 4, 2008. NORsk SOkkels Konkurranseposisjon.

/16/ IEC 62443-2-3, 2015. *Security for Industrial Automation and Control Systems, Patch management in the IACS environment.* International Electrotechnical Commission.

/17/ NIST SP 800-63-3, 2017. Digital Identity Guidelines. National Institute of Standards and Technology.

/18/ Analyzing Threat Agents & Their Attributes, Dr. Stilianos Vidalis et. al, 2005

/19/ NIST SP 800-153, 2012. Guidelines for Securing Wireless Local Area Networks (WLANs)

/20/ Theodore J. Williams (1992). *The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation*. Research Triangle Park, NC: Instrument Society of America

/21/ ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)

/22/ Health and Safety Executive, 2017. Cyber Security for Industrial Automation and Control Systems (IACS)

/23/ NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, 2014

APPENDIX A EXAMPLE OF A CYBER SECURITY REQUIREMENT SPECIFICATION

The detailed content of the CSRS will highly depend on:

1) Mandatory requirements as described by the asset owner. These requirements must be provided to the project by the asset owner and must include requirements for design and for the operational phase.
2) The SL-T for the zones and conduits as requested by the asset owner.
3) Mitigating actions identified in detailed risk assessments for zones and conduits. These are countermeasures needed to keep the cyber security risk to an acceptable level.
4) Other requirements that need to be in place to ensure identified risks are mitigated to an acceptable level

The following table of contents describes topics that should be included in the CSRS. The actual content of the CSRS must be described for each SuC and the mandatory requirements and SL-T (requested by the asset owner) will influence the actual content in each chapter.

1. Introduction. Describe the purpose of the CSRS.

2. Short description of the scope of the SuC. Name, high-level description of the function and the intended usage of the SuC – as well as the equipment or process under control

3. Short description of the threat landscape that may impact the SuC

4. Description of mandatory cyber security requirements described by the asset owner. These requirements must be provided to the project by the asset owner and must include requirements for design and for the operational phase

5. The asset owner's tolerable risk for the SuC. Description of the required (and decided) mitigating countermeasures identified in the detailed risk assessment for the involved zones and conduits to keep risk at an acceptable level. The description should state the risks identified in the detailed risk assessment that are accepted and for which no mitigating actions are required.

6. Any relevant cyber security regulatory requirements

7. Short description of physical and logical environment in which the SuC is located or planned to be located. The description must include zone and conduit drawings with the required SL-T. Logical description of the SuC and how it is divided into zones and conduits.

8 Description of how components in the SuC connect in a network topology

8.1 Desciption of the SuC logical infrastructure and how it should be segmented

8.1.1 Office network (L4)

8.1.2 Process information network (L3)

8.1.3 Vendor networks and systems (L2)

8.1.4 Process control and SIS networks (L2)

8.1.5 Client server networks (L2)

8.1.6 Control networks (L1)

8.2 Short description of the SuC physical infrastructure

8.2.1 Description of customer-provided items (IT networks and IT infrastructure) considered as a part of the SuC

8.2.2 Description of temporary devices that will need to connect to the SuC (such as service-laptops and USB storage devices) during operation and maintenance work

8.2.3 Firewalls, IT networks, hypervisors

9 Implementation of cyber security controls

9.1 Physical security

9.1.1 Power, cooling, access control

9.2 Backup and recovery

9.2.1 System backup

9.2.2 Application backups
9.2.3 Recovery images
9.2.4 Backup automation and verification
9.2.5 Backup scheduling
9.2.6 Recovery procedures
9.2.7 Criticality and priority evaluation (what should be recovered first)
9.2.8 Protection of backup files/media
9.3 Patch management
9.3.1 Patch approval process
9.3.2 Security update services
9.3.2.1 Windows clients' and servers' operating systems
9.3.2.2 Other IT equipments
9.3.2.3 Applications
9.4 Use of anti-virus solutions
9.4.1 Architecture and policies for malicious code protection
9.4.2 Antivirus update services
9.4.3 Monitoring of antivirus logs
9.5 Hardning for clients and servers
9.5.1 Disabled services that are not needed in the IACS (least functionality)
9.5.2 Removal of default user credentials and credentials that are not needed
9.5.3 Application whitelisting
9.5.4 Session timeouts
9.6 Computer and user configurations
9.6.1 System security
9.6.1.1 Protection of user credentials in transit and in storage
9.6.1.2 Protection of sensitive information
9.6.2 Management of user credentials
9.6.2.1 Policy for end-user accounts
9.6.2.2 Policy for functional user accounts
9.6.2.3 Policy for accounts with high privileges (admin)
9.6.2.4 Password strength, password change intervals
9.6.3 Group policy management
9.6.3.1 Unsuccessful login attempts
9.6.3.2 Enforcement of password rules
9.6.3.3 Use of screen savers (session locks)
9.6.4 Structure of organizational units
9.6.5 Local computer settings
9.6.6 Role-based access control
9.6.6.1 Role groups
9.6.6.2 Permission groups and mapping of permission groups to roles
9.6.6.3 Application groups
9.6.7 Access control to fileshares
9.6.8 Access control to databases
9.6.9 Security configuration for applications

9.6.9.1 User management
9.6.9.2 Input validation
9.6.9.3 Use of mobile code
9.6.9.4 Management of access to information and functionality
9.6.9.5 Remote session termination
9.7 Networks and interfaces
9.7.1 Network planning and documentation
9.7.1.1 IP network plan for SuC
9.7.1.2 Network segmentation
9.7.1.3 Use of FW, FW rules and administration of FW and rules
9.7.1.4 Use of computer certificates and PKI (public key infrastructure)
9.7.1.5 Protection of communication over untrusted networks
9.7.1.6 Protection of network fileshares
9.7.1.7 Security configuration of wireless networks
9.7.1.8 Denial-of-service (DOS) protection
9.7.2 Functional communication interfaces
9.7.2.1 Remote access solution
9.7.2.2 File transfers to/from SuC
9.7.2.3 Data interfaces to applications in other zones
9.7.2.4 Domain name services
9.7.2.5 Network time protocol
9.7.3 Communication interfaces for security services
9.7.3.1 Operating systems and application patch distribution
9.7.3.2 Antivirus updates
9.7.3.3 Transport of logging information
9.8 Logging and monitoring
9.8.1 Logging sources and machine-readable formats
9.8.2 Transport of logging information to security operations center
9.8.3 Intrusion detection systems and/or intrusion prevention systems

APPENDIX B DETAILED RISK ASSESSMENT WORKFLOW

B.1 General

The sections reflect the workflow in a detailed risk assessment described in the IEC 62443 standard. It is up to the asset owner to define the appropriate risk methodology for the SuC.

B.2 Identify the threats

Threat scenarios in IACS can cause control devices to be reprogrammed, control logic to be manipulated, denial of control actions, spoofed system status information – and even SIS systems to be modified. This chapter describes relevant threat agents (source of threats) and some cyber security threats that are relevant for IACS.. Threat intelligence input from governments and other sector-specific information-sharing and analysis centres (ISACS), if such exists, should be considered. .

Identify threat agents:

The likelihood of a cyber security incidentdepends on the combination of the threat agents' capability, motivation and opportunity, as described in /18/. Opportunity is dependent on vulnerabilities.

It is recommended to use the asset owner's characteristics of threat agents, for example their capability, motivation and opportunity.

More information:

A list of threat agents to IACS can be found in NIST SP 800-82 Revision 2 /10/ – Appendix C.

Identify threat scenarios:

Threats may change over time, and it is important to ensure that relevant threat scenarios are described. A good threat description includes:

- a description of the threat source
- a description of the capabilities, motivation and opportunity
- a description of possible threat vectors; and
- an identification of the potentially affected asset.

NIST SP 800-82 Rev.2 /10/ Appendix C Table C8 includes a list of possible threat scenarios.

B.3 Identify vulnerabilities

Vulnerabilities are weaknesses in IACS and procedures that can be exploited by a threat agent.

The output of this step should be a list of vulnerabilities which are paired with the relevant threats.

More information:

It is recommended to review the list described in NIST SP 800-82 Revision 2 /10/ – Appendix C Table C-2 to C-7 to verify that no relevant vulnerabilities are missing before finalizing this step.

B.4 Determine consequences

Each threat and vulnerability should be evaluated to determine the consequence should the threat be realized. It is recommended to describe the worst-case consequence of the described threat scenarios on risk areas such as personnel safety, business impact (loss of production, damage), reputation damage and environment.

The output of this step is a list of the consequences of each threat and vulnerability if the threat should be realized.

Some systems have non-software-based mechanical barriers (e.g. a relief valve) that are not directly impacted by cyber threats. This should be credited and formally documented when evaluating consequence reduction. It is recommended to consult functional safety personnel.

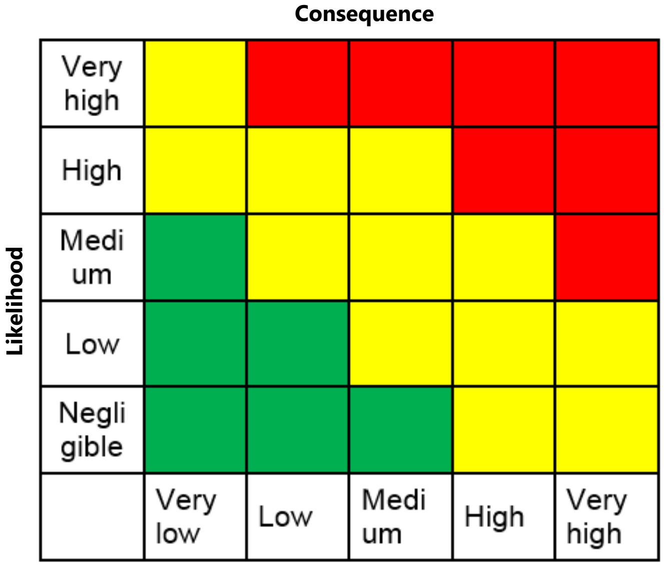
B.5 Determine the initial likelihood

Use the output from [B.1], [B.2] and [B.3] to assess the initial likelihood of each of the scenarios. Existing cyber security countermeasures should not be considered when assessing the initial likelihood. The likelihood determination should recognize any non-cyber independent protection layers (IPLs) such as physical security or mechanical barriers (such as pressure safety valves) that are in place to mitigate the threat.

The measure of likelihood is recommended to be qualitative and for example be based on the threat agents' capability, motivation and opportunity. Opportunity is dependent on vulnerabilities.

B.6 Determine the initial cyber security risk

The initial cyber security risk for each threat and vulnerability pair identified should be estimated by combining the consequence measure and the initial likelihood measure. The result can be communicated in a risk matrix, as shown in Figure B-1 Company risk matrix. Note that this figure is one example of a risk matrix and the format and colour scheme can vary between companies.



Consequence

Likelihood					
Very high	🟨	🟥	🟥	🟥	🟥
High	🟨	🟨	🟨	🟥	🟥
Medium	🟩	🟨	🟨	🟨	🟥
Low	🟩	🟩	🟨	🟨	🟨
Negligible	🟩	🟩	🟩	🟨	🟨
	Very low	Low	Medium	High	Very high

Figure B-1 Company risk matrix.

B.7 Determine the security level target (SL-T)

The security level target is the level of technical protection a system must provide against the agreed threats to a system, zone or conduit. A SL-T represents a set of technical countermeasures listed in /4/, which should be defined for each zone and conduit. The asset owner should define how the security level target and associated countermeasures relate to the risk and the risk level that is considered tolerable.

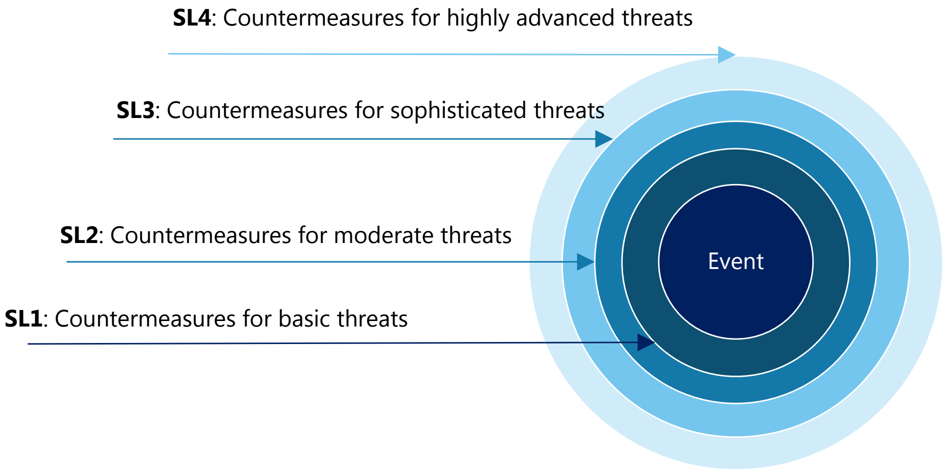

SL4: Countermeasures for highly advanced threats
SL3: Countermeasures for sophisticated threats
SL2: Countermeasures for moderate threats
SL1: Countermeasures for basic threats
Event

Figure B-2 Security levels

Instead of selecting one common SL-T for all functional requirements (FRs) for the given zone or conduit, an option is to differentiate. This is expressed by the SL-T vector = {IAC UC SI DC RDF TRE RA} /2/:

1) identification and authentication control (IAC),
2) use control (UC),
3) system integrity (SI),
4) data confidentiality (DC),
5) restricted data flow (RDF),
6) timely response to events (TRE), and
7) resource availability (RA).

If there is a gap between the initial risk and the mitigated and accepted risk, then sufficient countermeasures will be required to mitigate the risk and address the security gap. Identified countermeasures should be evaluated to ensure effectiveness.

The best practice is to use SL-1 as a minimum level. Based on the risk assessment, exposed solutions like the remote access solution should have a minimum SL-3. High criticality systems in the IACS and SIS zones should have a minimum SL-2.

B.8 Identify and evaluate existing countermeasures

Existing countermeasures should be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or consequence and to determine the residual risk.

B.9 Re-evaluate the likelihood and consequence

The likelihood and consequence should be re-evaluated considering the decided countermeasures and their effectiveness.

B.10 Determine the residual risk

Calculate the residual risk by combining the mitigated likelihood measure and mitigated consequence measure. Calculating the residual risk provides a measure of the effectiveness of existing countermeasures.

B.11 Compare the residual risk with the tolerable risk

The estimated residual risk should be compared to the asset owner’s tolerable risk. The asset owner should either accept the risk, or apply additional countermeasures to further mitigate the risk to an acceptable level.

B.12 Apply additional cyber security countermeasures

Based on the chosen SL-T, countermeasures should be identified and evaluated to determine their effectiveness of reducing the likelihood or consequence in order to achieve the SL-T. Asset owner may also want to evaluate the cost and complexity of countermeasures as part of the risk acceptance. Non-technical countermeasures can provide additional risk mitigation. For example, the asset owner’s operational procedures and maintenance work processes.

B.13 Document and communicate results

The results of the cyber security detailed risk assessment for zones and conduits should be documented, reported and made available to the appropriate stakeholders in the project organization (IEC 62443-3-2 /3/). Appropriate information security classification must be assigned to protect the confidentiality of the documentation. Countermeasures that have been decided on should be included in the cyber security requirement specification.

B.14 Cyber security requirement specification (development and implementation phase)

The previous steps in the assessment phase are all important activities in developing a CSRS for the SuC. The objective of the CSRS is to have a clear specification of the cyber security requirements that must be included in the development and implementation phase (detailed engineering phase). The CSRS does not need to be one single document. It can consist of several documents or be part of other documents, however it must give a clear description of the requirements for the SuC before the detailed engineering activities start. The detailed engineering phase must implement the requirements in the CSRS during development and implementation activities.

The cyber security requirement specification must ensure:

- A secure design of the SuC.
- The SuC can be operated in a secure way (according to asset owner policies, procedures and work processes) in the operations and maintenance phase (after handover to production).

Example 1: Requirement related to secure design.

The SuC must be divided into zones that are properly segmented by using network firewalls.

Example 2: Requirement related to secure operation:

Equipment like firewalls and antivirus systems should be implemented and configured to deliver information security logs to the asset owner's security operations center (SOC).

This means that the CSRS needs to be based on the following:

- Mandatory requirements as described by the asset owner. These requirements must be described to the project by the asset owner and should include requirements for the design and for the operational phase.
- The SL-T for the zones and conduits as requested by the asset owner.
- Countermeasures identified in detailed risk assessments for zones and conduits. These are countermeasures needed to keep the cyber security risk to an acceptable level.
- Other requirements that need to be in place to ensure identified risks are mitigated to an acceptable level.

See App.A for a more detailed description of what a CSRS may look like.

CHANGES – HISTORIC

There are currently no historical changes for this document.

About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping our customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER