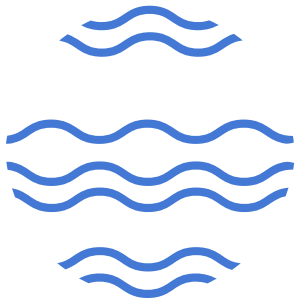

OFFSHORE NORGE

104 – Recommended guidelines on cyber security baseline requirements for Operational Technology (OT) systems

PREFACE

These guidelines are supported by the Security/Cyber Security Specialist Network, the HSE Managers Forum and by the Offshore Norge Operations Committee.

The guidelines are approved by the director general and the person responsible in Offshore Norge is the technical director HSE and standardisation.

These guidelines have been prepared with the broad-based participation of interested parties in the Norwegian petroleum industry and are owned by the Offshore Norge on behalf of the Norwegian petroleum industry.

Offshore Norge
Hovedkontor Hinna Park:
Fjordpiren, Laberget 22,
4020 Stavanger
Postboks 8065, 4068 Stavanger
Telefon: + 47 51 84 65 00

Website: www.offshorenorge.no
Email address: firmapost@offshorenorge.no

CONTENT

1. Introduction

1.1 Purpose

The purpose of this guideline is to enhance cyber security in the petroleum industry and thereby support safe, reliable and regular operations on the Norwegian continental shelf (NCS).

The increasing digitalisation and connectivity of Operational Technology (OT) systems have introduced cyber risks that may impact safety, the environment and production. Cyber security is therefore an integral part of the overall barrier and risk management strategy for onshore and offshore assets.

In this guideline, Operational Technology includes systems that directly control and safeguard production, such as safety, automation, and instrumentation systems, together with supporting systems, including telecommunications, where these are essential to safe, reliable, and continuous operations and where cyber compromise may have safety, environmental, or production consequences.

This guideline defines a set of Cyber Security Baseline Requirements (CSBRs) for OT systems, representing industry-agreed good practice. The CSBRs are intended to standardise and simplify the application of cyber security measures, promote consistency across the industry, and enable learning from operational experience and recognised standards.

The CSBRs define minimum cyber security requirements applicable to typical system solutions and operating conditions where cyber risks are reasonably well understood. Organisations may choose to apply their own standards or controls, provided they meet or exceed the minimum expectations set out in the CSBRs. The CSBRs are not intended to replace company-specific risk assessments, management systems, or regulatory obligations, but to complement them. Organisations should establish governance, assurance, and continuous improvement mechanisms to ensure cyber security maturity evolves beyond baseline compliance.

Implementation of the CSBRs does not in itself eliminate cyber risk or prevent all cyber incidents. Each organisation remains responsible for assessing its own risk exposure and implementing additional measures where necessary to achieve an acceptable level of cyber security.

A self-assessment tool is provided as a supplement to this guideline to support evaluation of compliance with the CSBRs and to facilitate continuous improvement of cyber security in OT systems.

1.2 Definitions and Abbreviations

WORD/ EXPRESSION/ ABBREVIATION	**DEFINITION**
Availability	The property of being accessible and usable upon demand by an authorised entity.

WORD/ EXPRESSION/ ABBREVIATION	DEFINITION
Access	The ability to interact with, control a system or retrieve data either directly or remotely.
Accessibility	The ease with which authorised users or systems can interact, monitor or control.
Asset owner	Role of an organisation that is responsible for one or more automation and control solutions and the associated equipment under control.
Attack surface	The total sum of all the potential entry points or vulnerabilities that an attacker could exploit to gain unauthorised access to a system, network, or application. This includes hardware, software, and human aspects, encompassing both digital and physical components.
Authorised	Individuals, devices or systems that have been granted explicit permission to access, interact with or control.
CERT	Computer Emergency Response Team
Awareness	Promoting a general understanding and vigilance.
CIS	Center for Internet Security
Confidentiality	The property which ensures that information is not made available or disclosed to unauthorised individuals, entities or processes.
Effective	Producing the intended result or achieving a desired goal with minimal time, effort, or resources.
IT system	An application, service, asset, or other component that manages information.
Information security	All aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information or information processing facilities.
Infrastructure	Hardware, software, networks, and facilities that enable the management, monitoring and control of OT systems.
Island mode	The capability to prevent any communication through the OT system boundary while retaining essential functions.

WORD/ EXPRESSION/ ABBREVIATION	DEFINITION
Malware	Software specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Network	Communication framework that connects devices, systems, and components, allowing exchange of data and control signals.
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NSM	Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet)
Operational technology	Hardware and software used to monitor, control, safeguard, and optimise processes, physical devices and infrastructure in the petroleum industry. OT includes both systems that directly control and safeguard production – such as safety and automation systems and instrument systems – and supporting systems, such as telecommunications systems, which provide essential connectivity, coordination, and operational continuity. See also IEC 62443-1-1 for concepts and reference architectures for OT systems.
OT DMZ	A controlled network layer that acts as a secure buffer between the IT (Information Technology) network and the OT (Operational Technology) or Industrial Control System (ICS) network. Its purpose is to reduce cyber-risk by preventing direct communication between enterprise systems and critical industrial assets.
Purdue model	A model with diagrams based on the Purdue Enterprise Reference Architecture (PERA) model, which is widely used in industrial control system (ICS) and operational technology (OT) cyber security.
Risk	Risk is the effect of uncertainty on objectives. In the context of cyber security, risk arises from the combination of the likelihood of a threat exploiting a vulnerability and the impact on the organisation’s assets if that exploitation occurs.
RPO	Recovery Point Objective (RPO) is the point in time to which systems and data shall be recovered after a disaster has occurred.

WORD/ EXPRESSION/ ABBREVIATION	DEFINITION
RTO	Recovery Time Objective (RTO) refers to the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organisation. This is the maximum agreed time for the resumption of the critical business functions.
SBOM	Software Bill of Material (SBOM) a formal, machine-readable inventory of all software components, their dependencies, and their relationships. It functions like a list of ingredients for software, detailing open-source libraries, third-party components, and their versions, which is crucial for tracking vulnerabilities, managing supply chain risk, and ensuring software security.
SDLC	Software Development Life Cycle process (SDLC) is a framework for the systematic planning, creation, testing, and deployment of high-quality software.
Security event	An identified occurrence of a system, service, or network state which indicates a possible breach of information security policy or a failure of safeguards, or a previously unknown condition which may be security relevant.
Security incident	A single unwanted or unexpected information security event or a series of such events which has a significant likelihood of compromising business operations and threatening information security.
Shall	Expression in the content these guidelines conveying objectively verifiable criteria to be fulfilled and from which no deviation is permitted if compliance with the guidelines is to be claimed. Ref. NORSOK.
Should	Expression in the content of these guidelines conveying a suggested possible choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others. Ref. NORSOK.
SOC	Security Operations Centre (SOC) is a centralised team or facility responsible for monitoring, detecting, analysing, and responding to cyber security incidents.

WORD/ EXPRESSION/ ABBREVIATION	DEFINITION
Supplier	An organisation that provides products and/or services as part of the supply chain, and that is responsible for the cyber security of the product throughout its life cycle.
System owner	The system owner is a function within an organization that has the overall responsibility for the operation and maintenance of one or more OT systems in operation.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organisation
Trusted zones	A logically or physically segmented area within an OT network where assets share a common trust level and security requirements, allowing controlled communication and reducing exposure to external threats.
Triage	Process of identifying, assessing, and prioritising security alerts.
Virtualisation	Technology that creates simulated, rather than physical environments, such as virtual machines, networks, storage, or applications. In cyber security, virtualisation is used to isolate systems and workloads, limit the impact of attacks, safely analyse malware, improve resource control, and enhance security monitoring.
Virtualisation infrastructure	The underlying hardware, software, and management systems that enable the creation and operation of virtual environments, such as virtual machines, virtual networks, and virtual storage. In cyber security, it is the framework that supports secure isolation between virtual environments, controls resource access, enforces security policies, and provides monitoring and protection mechanisms to prevent threats from spreading across the virtualised environment.
Wireless	Communication that transmits data between devices without physical cabling, using radio-frequency or other electromagnetic means.

1.3 References

Each CSBR has a section on references to relevant information including the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST). This framework is mapped to relevant IT security standards such as ISO 27001, IEC 62443 and others. It is also easy to relate the CSF functions with their categories to the process-oriented Plan–Do–Check–Act approach to defining proactive and reactive activities.

The following references, listed in alphabetical order, are used in this document.

DOCUMENT CODE	TITLE
CSA	Cloud Security Alliance https://cloudsecurityalliance.org
DNV-RP-G108 September 2017, Amended October 2021	Cyber security in the oil and gas industry based on IEC 62443. DNV.
IEC 62443-1-1 Editon 1.0 July 2009	Security for industrial automation and control systems, Part 1-1: Terminology, concepts, and models. International Electrotechnical Commission.
IEC 62443-2-1 Edition 2.0 August 2024	Security for industrial automation and control systems, Part 2-1: Security programme requirements for IACS asset owners. International Electrotechnical Commission.
IEC 62443-2-2 Edition 1.0 March 2025	Security for industrial automation and control systems, Part 2-2: IACS security protection scheme. International Electrotechnical Commission.
IEC 62443-2-3 Edition 1.0 June 2015	Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment. International Electrotechnical Commission.
IEC 62443-2-4 Edition 2.0 December 2023	Security for industrial automation and control systems, Part 2-4: Security programme requirements for IACS service providers. International Electrotechnical Commission.
IEC 62443-3-2 Edition 1.0 June 2020	Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design. International Electrotechnical Commission.
IEC 62443-3-3 Edition 1.0 August 2013	Security for industrial automation and control systems, Part 3-3: System security requirements and security levels. International Electrotechnical Commission.

DOCUMENT CODE	TITLE
IEC 62443-4-2 Edition 1.0 2019	Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components. International Electrotechnical Commission.
ISO 27001:2022 Amendment 1: 2024	Information security, cybersecurity and privacy protection — Information security management systems - Requirements. International Organisation for Standardization.
ISO 29147:2018 Edition 2, 2018	Information technology — Security techniques — Vulnerability disclosure. International Organisation for Standardization.
NIST CSF 2.0	Cybersecurity Framework. Revision 2.0 National Institute of Standards and Technology (NIST).
NIST SP 1305 October 2024	NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM). National Institute of Standards and Technology (NIST).
NIST SP 1326 October 2024	NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide. National Institute of Standards and Technology (NIST).
NIST SP 800-53 Rev. 5.2.0	Security and Privacy Controls for Information Systems and Organisations National Institute of Standards and Technology (NIST).
NIST SP 800-61 Rev. 3	Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. National Institute of Standards and Technology (NIST).
NIST SP 800-82 Rev. 4	Guide to Operational Technology (OT) Security. National Institute of Standards and Technology (NIST).
NISP SP 800-83 Rev. 1	Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology (NIST).
NIST SP 800-125 Updated April 2020	Guide to Security for Full Virtualization Technologies. National Institute of Standards and Technology (NIST).
NIST SP 800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations. National Institute of Standards and Technology (NIST).

DOCUMENT CODE	TITLE
Offshore Norge 123 Revision 1: 2009	Norwegian Oil and Gas Association Guideline for Classification of process control, safety and support ICT systems based on criticality. Offshore Norge.

2. Cyber Security Baseline Requirements (CSBR)

Cyber security measures shall be implemented in OT systems. These measures shall be managed in a life cycle perspective and include both the project phase, when solutions are built, and the operational phase after solutions have been handed over to operations. For each life cycle phase, the organisation shall identify the roles and parties responsible for implementing and managing the applicable cyber security measures, recognising that these may differ between project and operational contexts.

These guidelines consist of 21 CSBRs structured in accordance with the six core functions for security measures specified by the NIST CSF, see Figure 2.1. The NIST CSF provides guidance to industry, government agencies, and other organisations to manage cyber security risks.

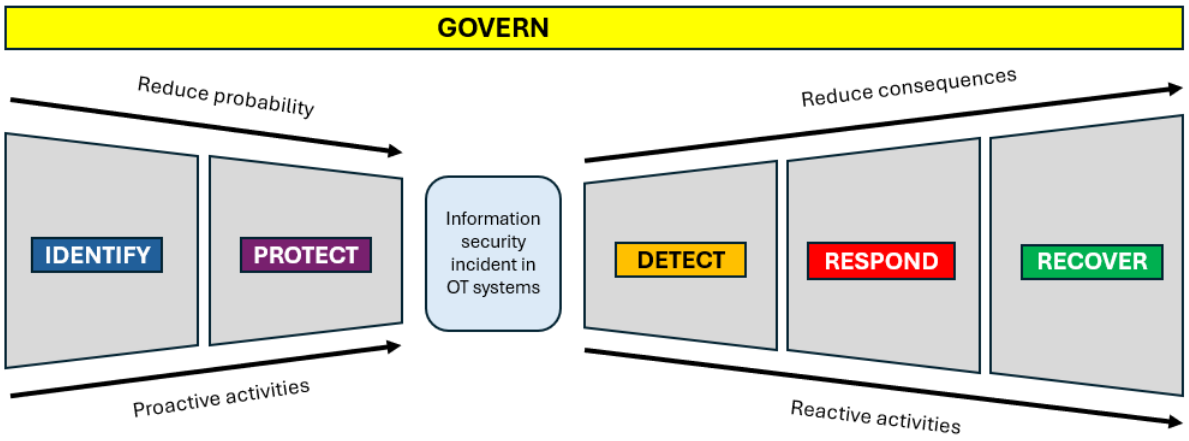

Figure 2.1 NIST CSF six core functions

Govern – develop the organisational cyber security risk management strategy, expectations, and policy. Provides outcomes to inform what an organisation may do to achieve and prioritise the outcomes of the other five functions in the context of its mission and stakeholder expectations.

Identify – develop the organisational understanding required to manage the cyber security risk to systems, assets, data and capabilities. That includes planning and activities required in an early phase, before potential information security incidents can occur. Examples could be asset management and vulnerability management.

Protect – develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. That includes measures and activities to protect the actual systems. Examples could be training, access controls and proper network segmentation.

Detect – develop and implement the appropriate activities for identifying the occurrence of a cyber security event. That includes continuous security monitoring and detection processes. Example could be logging and analysis of malicious anomalies and events.

Respond – develop and implement the appropriate activities for responding to a detected cyber security event. Examples could be executing response plans and mitigating actions.

Recover – develop and implement the appropriate activities to maintain resilience plans and to restore any capabilities or services impaired by a cyber security event. An example could be executing a recovery plan.

Figure 2.2 shows the NIST CSF core functions as a wheel since all the functions relate to one another.

Figure 2.2 NIST CSF core functions

The CSBRs are built up according to a common framework.

Control – The overarching high-level statement of what must be achieved to comply with the CSBR.

Objective – A description of the rationale or intended outcome of the CSBR.

Requirements – A set of specific requirements that when implemented will achieve the objective.

Supplementary Guidance – Information that will help the user understand the requirements and how these can be implemented.

References – Reference to documents or similar that provide further information and guidance to help the user understand the requirements and how these can be implemented.

The CSBRs cover all the six core functions as advocated in the NIST CSF. Figure 2.3 shows which core function each CSBR is intended to address. For this figure the NIST CSF core functions 'Respond' and 'Recover' are combined. It should be noted that some of the CSBRs may cover two or more NIST CSF core functions. In these cases, the CSBR is shown in the most relevant function.

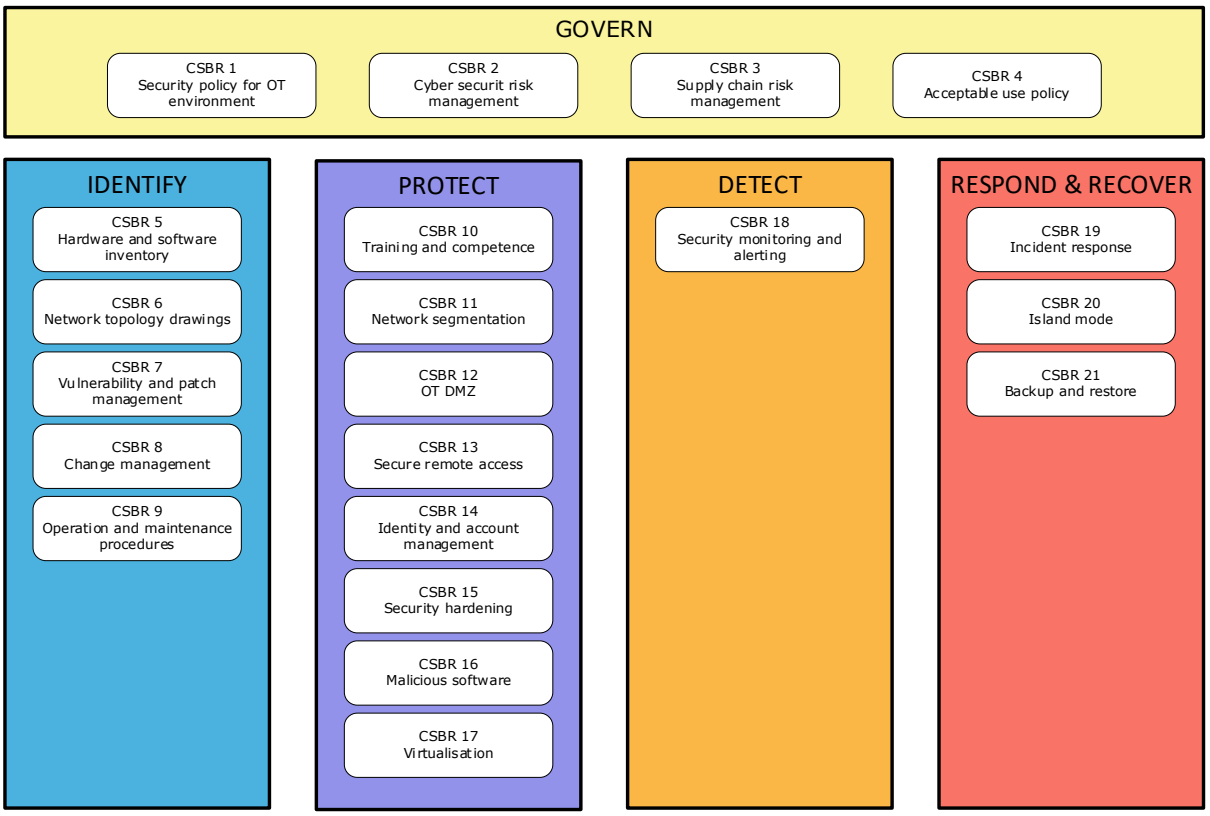

Figure 2.3 CSBRs arranged according to the NIST CSF core functions

2.1 CSBR 1 Security policy for OT environment

Control

A security policy for the OT environment shall be developed, maintained, documented, and approved as part of the organisation's management system.

Objective

To describe the overarching principles, targets, and responsibilities for management of cyber security for the OT environment.

Requirements

1-1 The security policy shall define the overarching objectives, priorities, and strategies for management of cyber security for the OT environment in the organisation.

1-2 The scope of the security policy shall include all aspects of the OT environment, including systems, processes, and organisations.

1-3 The security policy shall address cyber security for the OT environment throughout all life cycle phases of the asset, including project, handover, operation, modification, and decommissioning.

1-4 Internal and external stakeholders, and their needs and expectations regarding cyber security for the OT environment shall be understood and considered.

1-5 Roles, responsibilities, and authorities related to cyber security for the OT environment shall be established, communicated, understood, and enforced.

1-6 Accountability for cyber security shall be anchored at the board of directors and senior management level.

1-7 Legal, regulatory, and contractual cyber security requirements that affect the OT environment and its operation shall be understood and managed.

1-8 The security policy shall be regularly reviewed, updated, and communicated to reflect changes in requirements, threats, technology, or organisational mission.

1-9 The organisation shall develop and implement cyber security procedures, based on the security policy, and provide guidance in how to meet the policy.

Supplementary Guidance

Relevant and thorough recommendations for the development of a security policy for the OT environment is given in section 3 of NIST SP 800-82 Rev. 3.

It is recommended to ensure that the security policy for the OT environment is consistent and integrated with existing IT cyber security policies and practices to the extent possible, while accounting for the specific requirements and characteristics of OT systems and the OT environment.

The security policy should describe how the performance of cyber security controls is measured, and continuous improvement is ensured. Performance indicators and success criteria should be established and used to assess whether the security policy is functioning as intended.

References

NIST CSF 2.0: GV.OC, GV.PO, GV.RR

IEC 62443-2-1: ORG 1.1, ORG 1.3, ORG 2.4

NIST SP 800-82 Rev. 3: Clause 6.1.2, Section 3

2.2 CSBR 2 Cyber security risk management

Control
A process for identifying and managing cyber security risks in the OT environment shall be in place and effective.

Objective
To ensure that risks associated with the OT environment are managed effectively and maintained at an acceptable level.

Requirements

2-1 Threats to and vulnerabilities of the OT environment shall be identified.

2-2 Consequences of threats and vulnerabilities materializing in the OT environment shall be identified, analysed, and documented.

2-3 Risk acceptance targets shall be established and documented.

2-4 Risks shall be assessed and risk mitigation measures identified.

2-5 A process for implementing risk measures shall be established and documented.

2-6 Cyber risk assessments shall be carried out regularly, and upon installation of new OT systems and changes to existing OT systems.

2-7 When introducing a supplier and their products and services into the OT environment, a specific cyber risk assessment shall be carried out.

2-8 Criteria for updating of cyber security risk assessments shall be in place.

Supplementary Guidance

OT cyber security risk management should ensure that risks to the OT environment are understood, assessed, and maintained at a level consistent with the organisation's defined risk appetite. Relevant threat actors – including state-sponsored actors, cyber-criminals, hacktivists, opportunistic attackers, and insiders – should be systematically identified and analysed. Their motivations, capabilities, and likely attack techniques should be evaluated using structured threat-modelling sources such as the MITRE ATT&CK for ICS framework to provide a consistent basis for understanding realistic attack vectors and adversary behaviour patterns.

Capabilities and adversary techniques should then be mapped against existing vulnerabilities in the OT environment. Known vulnerabilities should be identified through reputable sources such as the National Vulnerability Database (NVD) and verified against deployed hardware, firmware, and software components. This mapping supports a more accurate understanding of the potential likelihood and impact of cyber events affecting OT functions. The identification of vulnerabilities is part of *CSBR 7 Vulnerability and patch management* and serves as an input to risk management.

NIST SP 800-82 Rev. 3 Chapter 4 emphasizes the importance of combining threat, vulnerability, and consequence perspectives when framing and assessing OT cyber risk. In line with this guidance, risk assessments should consider system and function criticality, including potential consequences for

safety, environmental protection, production continuity, and operational integrity. The outcome should be evaluated against documented risk acceptance criteria, ensuring that any identified risk is treated or justified according to the organisation’s governance processes.

It is recommended to use criticality assessments (e.g., following the methodology described in Offshore Norge 123) to prioritise risk management efforts on the OT systems where it matters the most.

Mitigating measures should be identified based on risk levels and aligned with recognised best practices. This may include architectural protections such as zoning and segmentation, access control improvements, protective monitoring, hardening, and other layered defence-in-depth strategies appropriate for the OT domain. Mitigations should be implemented with consideration for operational feasibility, system dependencies, and life cycle management.

When introducing new OT systems or making changes to existing ones, the organisation should review and, if necessary, adjust the established cyber controls and measures to account for any changed risks. This ensures that system modifications do not inadvertently weaken existing protections and that cyber risks associated with design choices, supplier components, or integration points are adequately addressed prior to deployment.

Because the OT threat landscape evolves continuously, the risk assessment methodology should be reviewed and updated on a regular basis. Updates should reflect new threat intelligence, newly discovered vulnerabilities, technological changes, and lessons learned from incidents or assessments. The revised methodology should then be applied as part of a continuing risk assessment cycle to identify gaps between current cyber barriers and the evolving threat environment. This continuous, feedback-driven approach ensures that the organisation maintains an up-to-date understanding of its OT cyber posture and takes timely steps to improve resilience.

OT cyber security risk management should remain an integral and embedded component of the organisation’s overall risk management process. This integration ensures consistency in governance, prioritisation, documentation, and decision-making across operational, safety, and security domains. A disciplined, structured, and continuously improving approach helps ensure that OT cyber risks are proactively managed and maintained at an acceptable level over time.

References

NIST CSF 2.0: GV.RM-02, GV.RM-03, GV.RM-06, ID.RA-03, ID.RA-04

IEC 62443-2-1

IEC 62443-2-2

IEC 62443-3-2

NIST SP 800-82 Rev. 3: Section 4.1.1, "Framing OT Risk"

Offshore Norge 123

2.3 CSBR 3 Supply chain risk management

Control

A process to identify, monitor and manage cyber security risk from suppliers, products and services shall be in place and effective.

Objective

To avoid use of products, systems or services that negatively impact cyber security, as well as ensuring that suppliers maintain a high level of cyber security in their products and services throughout the system lifetime.

Requirements

3-1 An overview of suppliers and service providers shall be established and maintained, including a list of products and services provided, as well as a cyber security contact point for each supplier.

3-2 The supplier shall have a documented and effective cyber security programme in place. The programme shall include regular self-assessments of own products and practices or evidence verified through external audit.

3-3 Contracts and agreements shall specify cyber security requirements for products and services provided, as well as equipment used by the supplier in the delivery of the products and services.

3-4 Documentation of technical and cyber security configurations and implementations shall be included as part of the delivery.

3-5 Software shall be developed according to a documented Software Development Life Cycle (SDLC) process. The SDLC shall also include processes for ensuring vulnerability management and responsible disclosure.

3-6 Procurement and service contracts shall include cyber security requirements for personnel working with products and services delivered to the OT environment.

3-7 Procurement and service contracts shall require obligation to cooperate with internal and external audits.

3-8 Reporting of incidents affecting the supplier, their products, or their services, as well as supplier's response time to such incidents, shall be defined in a service level agreement (SLA).

3-9 Upon service termination, the supplier shall ensure no customer assets or sensitive data are retained.

Supplementary Guidance

Relevant and thorough recommendations for the development of a cyber security supply chain risk management practice are given in section 3 of NIST SP 800-161 Rev. 1 chapter 2 and appendix A.

System documentation should include all deliveries related to system architecture and configuration, as a minimum hardware and software inventories, network topology diagrams, secure configuration baseline, detailed design specifications and operation and maintenance procedures.

Suppliers should use secure product development processes (including Software Development Process, SDLC) throughout the entire software development process. Defining security requirements, secure design, secure implementation, verification and validation, defect, vulnerability and patch management, as well as end-of-life management ensures that OT systems are built with cyber security in mind from start to finish.

Supplier should maintain a Software Bill of Material (SBOM) for the supplier's delivery, describing the elements of software applications delivered. The SBOM should be machine readable and compatible with the system integrator or operator's system for inventory control.

Requirements for supplier personnel should include that supplier personnel working on OT systems have gone through relevant screening and training before being granted access to production systems. Cyber security competence, and operational training for relevant systems should be clearly stated in the requirements.

Use of 3rd party devices for access to the OT environments should be tightly restricted and subject to explicit risk-based approval. Where use of 3rd party devices is permitted, the devices should comply with a defined security baseline, including secure configuration and hardening, current security updates, endpoint protection, and malware scanning prior to and during access. Access should be limited to approved tasks and technically constrained to prevent direct interaction with high criticality OT assets.

SLA with system supplier should include reporting obligations ensuring cyber security incidents affecting a supplier or its associated products, systems or services are reported within reasonable time of the incident being known by the supplier.

Responsible disclosure should be required as described in ISO 29147. Contracts or SLA should include that suppliers report vulnerabilities as quickly as possible when the vulnerability has been made public. Suppliers should also ensure that an initial list of remediation actions is included in the initial report.

The process for evaluation of supplier cyber security should follow a risk-based approach, including criticality of products and services delivered as well as performance in previous reviews.

Upon discontinuation of a system or service, measures ensuring that supplier no longer retain any assets or sensitive information belonging to the asset owner should be in place.

References

NIST CSF 2.0: GV.SC-01-10, ID.SC-1

NIST SP 800-53 Rev. 5: PM-30, SR-2, SR-3

NIST SP 800-161 Rev. 1

NIST SP 1305

NIST SP 1326

ISO 29147

2.4 CSBR 4 Acceptable use policy

Control

A policy defining the acceptable use of OT systems shall be developed, maintained, and documented as part of the company's management system.

Objective

To ensure that OT systems are used for their intended purpose only and that the use of any OT system does not increase cyber security risk.

Requirements

4-1 The acceptable use policy shall be read and accepted by all personnel, both own employees and personnel of external parties (suppliers, contractors, etc.), before any work on OT systems.

4-2 Requirements for OT specific cyber security training and competence shall be included in the policy.

4-3 Requirements for approval and screening of devices by the asset owner shall be included in the policy.

4-4 The policy shall describe rules for the use of portable devices such as service laptops, smart phones, tablets, USB memory sticks, and CDs/DVDs.

4-5 The policy shall include requirements related to the installation of software and hardware on OT systems, approval process, and be linked to the relevant change management process.

4-6 The policy shall contain guidelines for creating and storing passwords for OT accounts.

4-7 The policy shall state that default credentials shall not be used on OT systems.

4-8 The policy shall include requirements prescribing that OT systems shall not be used for general internet access, e-mail, personal use, or office related activities.

4-9 The policy shall include requirements prescribing that OT systems shall not be left unattended while logged in/unlocked with configuration privileges.

4-10 The policy shall explain how cyber security incidents shall be reported.

Supplementary Guidance

The acceptable use policy should define acceptable and unacceptable use of OT systems and associated devices to prevent unintended changes, malware introduction, and misuse that may affect safety, availability and integrity of the OT environment. The policy should apply to all personnel, including employees and external parties, and be provided and accepted before access to OT systems or remote connectivity is granted.

The policy should describe expected user behaviour when working on OT systems, including restrictions on personal use, use of portable media, installation of software and hardware, and

handling of credentials, consistent with the intent of limiting common OT incident vectors and risks. It is recommended that the policy details that only devices provided by or checked and approved by the asset owner specifically for the OT environment should be considered acceptable.

The acceptable use policy should include requirements for OT systems to be clearly marked. It can also include other user focused elements like “working in restricted areas”, “use of photo, video and recording in restricted areas”. Clear identification of OT systems and explicit rules for their use support consistent enforcement and reduce the likelihood of accidental or unauthorised activities.

For further reference on how to create an acceptable use policy for the OT environment the SANS “Acceptable use policy template” may be used as a starting point and adapted to reflect OT specific and asset specific constraints and risks.

References

NIST CSF 2.0: PR.AT

IEC 62443-2-1: ORG 1.4, ORG 1.5

NIST SP 800-82 Rev. 3: Clauses 3.3.3 and 3.3.5

2.5 CSBR 5 Hardware and software inventory

Control

All OT hardware and software systems shall be clearly identified, registered and continuously updated in an inventory.

Objective

To create and maintain detailed records of the components within the OT environment that are essential for ensuring secure operations, vulnerability management and effectively handling cyber security incidents.

Requirements

5-1 A documented process for creating and maintaining hardware and software inventories shall be implemented.

5-2 Inventories shall contain information about hardware, software, services, and systems managed by the asset and by suppliers.

5-3 Inventories shall contain the following information at a minimum:

a) Unique identifiers / tags
b) Description
c) Manufacturer
d) Model
e) Location
f) Version numbers
g) Serial numbers
h) Network interfaces
i) Communication addresses
j) Revision / patch levels
k) End of Life information
l) Criticality level of components

5-4 Controls shall be in place to minimise the number of people with access to restricted information in the inventories.

Supplementary Guidance

Inventories should reflect the implemented system and be maintained throughout the systems design, specification, implementation, verification and validation, operations, maintenance and decommissioning.

An inventory should include software details at the level deemed necessary for ensuring secure operations, vulnerability management and effectively handling cyber security incidents. It should be possible to identify the system owner for the hardware and software components from information stored in the inventory.

An automated asset inventory tool is recommended for continuously maintaining an updated asset inventory.

Inventories should include information about communication ports and protocols. Information about configuration settings of devices and software, and VLAN details indicating where on the network devices reside is also useful.

Only share inventories with authorised external parties using a controlled and secure method.

References

NIST CSF 2.0: ID.AM

NIST SP 800-53 Rev. 5: CM-8

IEC 62443-2-1: CM 1

IEC 62443-3-3: SR 7.8

NSM ICT Security Principles: Chapter 1.2

2.6 CSBR 6 Network topology drawings

Control

Accurate drawings of physical and logical network topologies of the OT environment shall be developed, verified and maintained.

Objective

To ensure the availability of accurate information about the networks to support operation, maintenance, and incident handling of the OT environment.

Requirements

6-1 The drawings shall describe logical and physical network topologies, including its network devices, internal interfaces, and external interfaces.

6-2 The level of detail shall make it possible to identify all network connected devices, such as servers, operator stations, network devices, gateways, automation devices, electrical devices, and telecommunication devices.

6-3 Individual devices shall be documented with device name and/or tag to enable locating more device details in the hardware and software inventory.

6-4 The drawings shall identify and document the network segments and their interfaces to other segments, covering both physical and logical infrastructure.

6-5 The hierarchy of network devices (switches, routers, and firewalls) shall be documented, showing how the various network segments are interconnected.

6-6 The drawings shall include critical communication paths and data flows internally within the OT networks, externally with corporate IT networks, and externally with cloud services or third parties.

Supplementary Guidance

Documenting network topologies and data flows enables organisations to understand the expected behaviour of their networks. This understanding of how devices communicate assists with troubleshooting, anomaly detection, and response and recovery activities.

Physical network topology refers to the actual layout of devices and cables in a network, while logical network topology describes the flow of data and how devices communicate within the network, regardless of its physical arrangement.

Documenting the hierarchy of network devices helps visualise how switches, routers and firewalls are organised and connected. This structure often reflects the layers in the network, which is important in understanding the flow of data through the network.

Below is a guide on how to develop network topology drawings:

- Gather information about all devices within the network from hardware and software inventories, including switches, routers, firewalls, servers, operator stations, automation devices, electrical devices, and telecommunication devices.
- Map out how these devices are connected, including both physical (cabling) and logical (addressing, VLANs) connections.
- Identify the communication protocols and data flow in use between devices, focusing on the critical data flow that is required for understanding how systems interact to perform their functionality.
- Create multiple drawings as required based on functional need to avoid cluttering the drawings.
- Break down the network into layers based on the Purdue model to simplify complexity.
- Ensure consistency by using the same symbols for each device type (e.g., firewalls, switches, PLCs) throughout the drawings.
- Add necessary details like device name, tags, VLAN IDs, and physical location, but avoid cluttering the drawings with information.
- Highlight network segmentation and security zones to assist in identifying potential security vulnerabilities.

Consider creating network topology diagrams for both IP-based networks and for bus networks (e.g., Profibus, Modbus) as required to ensure the system interaction is fully understood and documented.

Implement a change management process where network changes are documented, and the network topology drawings are updated accordingly. Use version control for the drawings, maintaining a history of changes to revert to older versions if necessary.

Consider if network topology drawings contain sensitive information and implement procedures to restrict access to the drawings to only authorised personnel if required. The classification and need for protection of network topology drawings should be based on the information classification scheme of the organisation.

References

NIST CSF 2.0: ID.AM

IEC 62443-2-1: CM 1.2, CM 1.4, NET 1.2

IEC 62443-2-4: SP.06.01, SP.03.02

NIST SP 800-82 Rev. 3: Clause 6.1.1

2.7 CSBR 7 Vulnerability and patch management

Control

A vulnerability and patch management process for OT systems shall be in place and effective.

Objective

To ensure OT systems are protected from known vulnerabilities by implementing a structured and risk-based approach to identifying, assessing, prioritising, and remediating vulnerabilities through mitigating actions or patching.

Requirements

7-1 The vulnerability and patch management processes shall include identification and prioritisation of reported vulnerabilities and available patches and fixes.

7-2 Patches, updates, and upgrades shall only be obtained from authenticated, verified, and explicitly approved sources.

7-3 A procedure for installing security patches shall be in place.

7-4 Compensating measures shall be implemented to mitigate vulnerabilities in systems that cannot be updated with security patches and where the risk of running a vulnerable system is unacceptable. These measures shall be documented, and a process shall be in place to verify their effectiveness over time.

7-5 The risk posed by running a vulnerable system as part of the operational environment shall be documented, communicated and accepted by the risk owner. Accepted vulnerabilities shall include defined review intervals and expiration criteria approved by the risk owner.

Supplementary Guidance

Vulnerability reports from suppliers, known exploited vulnerabilities (KEV) catalogue, CERTs, and national security agencies should be continuously monitored and assessed for relevance to the OT environment. Capabilities and adversary techniques should be mapped against known vulnerabilities in the OT environment.

The “Now”, “Next”, “Never” is a simple risk-based approach to vulnerability management that may be used to prioritise remediation efforts. “Now” covers high-risk vulnerabilities that should be fixed immediately (e.g., exploitable or actively attacked flaws), “Next” includes issues that should be addressed but are not urgent. “Never” refers to low-risk vulnerabilities that do not require action because they are not exploitable or irrelevant in the environment. When a decision to not patch a vulnerability (“Never”) is made, the risk should be documented in a risk register.

Security patches should be tested and approved prior to deployment to the production environment. Patches, updates and upgrades should originate from trusted suppliers and should be validated through the organisation’s established change-control and supply-chain security processes for OT systems.

Device configuration should be verified after maintenance and software patching, as some features may have inadvertently been reenabled, or new features installed.

An automated tool for vulnerability identification is recommended.

OT system suppliers should be consulted for advice and guidance on how to install security patches to ensure that functionality of the procured system is not impacted.

References

NIST CSF 2.0: ID-RA-08, PR-PS-02

NIST SP 800-82 Rev. 3: Clauses 5.2.5.2 and 6.2.11

IEC 62443-2-1: COMP 3

IEC 62443-2-3

2.8 CSBR 8 Change management

Control

A process for identifying, managing, controlling and implementing changes affecting the OT environment shall be in place and effective.

Objective

To ensure that all changes to OT systems or affecting the OT environment are systematically evaluated, controlled, and documented to maintain operational integrity and manage HSE and cyber security risks.

Requirements

8-1 Proposed changes shall be documented and evaluated for their potential impact to HSE risks and cyber security risks prior to implementation. The evaluation shall be performed by competent individuals knowledgeable about the operation, the specific OT system and the associated risks.

8-2 Changes shall be approved prior to start of implementation. The approval state, approvers and scope of work shall be documented for each change. Any deviations that arise during implementation shall be documented and re-approved.

8-3 An implementation plan shall be defined and approved prior to start of implementation. Competence required to carry out the implementation shall be evaluated and reflected in the implementation plan.

8-4 Following implementation of change, all relevant documentation shall be updated.

8-5 After the changes are implemented, the security controls shall be verified to be functioning correctly, and operating as intended.

8-6 After the changes are implemented, OT system functions shall be verified to be operating as intended.

Supplementary Guidance

The change management process should include identification of the change requestor, change implementer, change approvers and stakeholders. Separation of duty principle should be applied to approval of change.

An evaluation of the information needs for the users of the system, or individuals relying on the integrity of the system, should be considered. The evaluation should include informing the users of the intended changes to the system, and risks identified to apply during or after the implementation. An evaluation of the information needs for the users of the system, or individuals relying on the integrity of the system, should be considered. Relevant end users, operators and maintenance personnel should, where appropriate, be involved in the assessment of changes to identify unintended operational and safety consequences before implementation.

The process should clearly justify the need for change and review the potential of deviations and changes to scope during implementation. Risk factors and mitigating actions to be considered should include:

- Validation of product integrity before installation.
- Validation of product integrity after the installation.
- Pre-evaluation of network and computing capacities.
- Verification activities proving that the changes are working as intended.
- Rollback and recovery procedure associated with the change.
- Coordination activities that provide oversight of configuration changes and convene needed information to relevant stakeholders, including system operators and system responsible.

Changes to initial scope, addition of further scope or deviations that arise during implementation should be documented through revision control of the change management documentation.

Update of documentation should include:

- Hardware, software inventories
- Network topology diagrams
- Secure configuration baselines
- Firewall rules and access control list (ACL)
- As-built documentation

Proposed changes should be analysed in a separate test environment before implementation in an operational environment. The analysis should include security or safety impacts due to flaws, weaknesses, incompatibility, or intentional malice.

During assessment of impact and risk, due consideration should be given to competence required to carry out the implementation, handling of deviations and verification that the change is working as intended, without unintended impact to the safety or security functions in the system.

The implementation plan should be adapted to the level of task at hand. Competence required for backout, rollback and recovery of the change should be included. The competence evaluation should be carried out by individuals knowledgeable about the industrial operation and the specific OT system.

References

NSM ICT Security Principles: Section 2.10.1-4

NIST SP 800-53 Rev. 5: CM-4, CM-6

2.9 CSBR 9 Operation and maintenance procedures

Control

Documented operation and maintenance procedures covering cyber security for all OT systems shall be in place and be executed in a structured manner.

Objective

Ensure the required performance, availability, resilience and security of the OT systems.

Requirements

9-1 Operational routines and maintenance schedules shall be documented and specified for all systems and activities influencing OT cyber security.

9-2 Procedures for operation and maintenance of OT systems shall be described and implemented.

9-3 The maintenance of the OT systems shall be tracked in the company's Computerized Maintenance Management System (CMMS) or an equivalent system or a register.

9-4 OT systems shall be delivered with maintenance procedures for installation of security patches.

9-5 OT systems shall be delivered with maintenance procedures for backup and recovery.

Supplementary Guidance

Operation and maintenance procedures are essential to ensure that OT systems remain secure, available, and resilient throughout their operational life cycle. These procedures should establish a structured framework for how cyber security is maintained during routine operations, preventive maintenance, corrective maintenance, system upgrades, and emergency interventions. Effective procedures reduce the risk of human error, inconsistent practices, and degradation of cyber security controls over time.

Operational procedures should define how OT systems are securely operated on a day-to-day basis, including monitoring, user interaction, routine inspections, and verification of cyber security critical functions. Maintenance procedures should define how systems are securely maintained, patched, backed up, restored, tested, and returned to service without introducing unacceptable cyber security or operational risk.

Documentation should be complete, accurate, version-controlled, and readily available to relevant personnel. Relevant documentation should typically include:

- Operating procedures for normal and degraded modes
- Maintenance procedures for patching, backup, restore, hardening, and staged deployment
- Password and credential handling procedures
- Procedures for onboarding, modifying, or decommissioning systems

- Logging, monitoring, and verification procedures
- Cyber security incident response and recovery procedures

Maintenance activities should be tracked through the organisation's Computerized Maintenance Management System (CMMS) or equivalent system to ensure traceability, scheduling, accountability, and auditability. Records should include what was changed, who performed the work, approvals, verification results, and any deviations or compensating measures applied.

Operation and maintenance procedures should be periodically reviewed and updated to reflect evolving threats, technological changes, supplier recommendations, lessons learned from incidents, and organisational changes. Continuous improvement of these procedures helps maintain long-term resilience and ensures that cyber security remains effective beyond initial deployment.

References

NIST SP 800-82: Clauses 3.3.1 and 3.3.4

IEC 62443-2.1: User 1.11

2.10 CSBR 10 Training and competence

Control

An OT-specific cyber security training and competence programme shall be in place and effective.

Objective

To ensure that all personnel responsible for or working on and with OT systems have the cyber security knowledge and competence required for their tasks.

Requirements

10-1 A general OT-specific cyber security training and competence programme shall be established, documented and enforced on all employees, contractors and third parties who interact with OT systems.

10-2 Role-based training and competence aimed at individuals with specific duties and responsibilities within cyber security for OT systems shall be established.

10-3 Training programs shall be delivered at regular intervals to reinforce knowledge, address skill gaps, and maintain continuous awareness across all personnel who directly or indirectly interact with OT systems.

10-4 Training and competence programs shall be regularly reviewed and updated to keep them relevant and effective in response to changes in the threat landscape, organisation, regulatory requirements, and technology.

10-5 Required OT specific cyber security training shall be completed before any work on an OT system.

10-6 Personnel shall be trained to report cyber incidents.

Supplementary Guidance

Security training and competence is essential to ensure that personnel who interact with OT systems understand how their behaviour can impact the security of these systems. Direct interaction refers to individuals who actively operate, maintain, or configure OT systems, while indirect interaction includes those who support, manage, or otherwise influence the OT environment. Training helps establish a culture where everyone recognises their role in maintaining security. General OT security training modules could be a good start, but the training should also address the specific security policies and requirements the organisation have for OT systems.

The role-based training should ensure that all personnel (including management, employees, contractors, and third parties) are aware of their cyber security responsibilities for OT systems. This training should help personnel understand and carry out their roles, and follow the required processes, and procedures.

The security training should be added to the company competence matrix/profile to ensure they are enforced the same way as other company required training.

To ensure the training programme remains relevant and effective, it is recommended to establish a regular review schedule to assess its alignment with current threats, and organisational and regulatory changes. Incorporate feedback from participants, cyber security incidents, and lessons learned to identify gaps or outdated material.

The security training and competence programme should include a variety of e-learning courses, workshops, and physical courses to gain maximum effect.

References

NIST CSF 2.0: PR-AT

NIST SP 800-82 Rev. 3: Clause 3.3.5

IEC 62443-2-1: ORG 1.4, ORG 1.5

2.11 CSBR 11 Network segmentation

Control

The infrastructure shall implement segmentation of networks in the OT environment based on functionality, criticality, location, responsible organisation, and security needs.

Objective

To reduce complexity, enable interoperability, and reduce the exposure of cyber risk to the OT environment.

Requirements

11-1 OT networks shall be segmented from IT networks, and any interconnection shall be limited to the minimum necessary for operations. All connections between IT and OT shall be documented.

11-2 Internal OT networks shall be logically or physically segmented into zones based on functionality, criticality, location, responsible organisation, or security needs identified through risk assessments.

11-3 Safety Instrumented Systems (SIS) networks shall be physically or logically segmented from non-safety system networks.

11-4 Organisations shall segment and protect their OT network from another organisation's networks, including networks of suppliers, partners, peers, and services upstream and downstream. Organisations cannot presume that other organisations have the same cyber risk appetite, cyber hygiene and cyber security standards as their own.

11-5 Virtual networks implemented as part of the virtual infrastructure shall be segmented using the same criteria as for physical OT networks.

11-6 A separate network segment shall be established to enable inspection, cyber security configuration, and update of all equipment before being connected to other OT networks and devices. This also applies to temporary connected devices (e.g., service laptops).

11-7 Communication between network segments shall be strictly controlled, validated and monitored at zone boundaries using appropriate boundary protection devices (e.g., firewalls, gateways, or data-diodes) to ensure that only network traffic that is strictly necessary and that represents tolerable risk is allowed.

11-8 Separate network segments shall be established for segmenting management traffic (e.g., administration of network devices and virtual infrastructure) from other OT network traffic.

Supplementary Guidance

Network segmentation is a critical cyber security and operational strategy that enhances security, reliability, and compliance by compartmentalising devices into security zones and limiting the spread of threats. It is typically implemented physically using different network switches or logically using virtual local area network (VLAN) configurations.

Risk assessments should be used as a basis for segmentation by identifying and evaluating the specific threats, vulnerabilities, and potential impacts to different parts of the OT network and then segmenting the network to protect the most critical and vulnerable systems according to their risk profile. IEC 62443-3-2 provides guidance in how to define zones by identifying areas within an OT network that share common security requirements based on their risk levels.

It is recommended to use an industry-recognised model, such as the Purdue model, for segmentation of OT networks based on their functions, security needs, and criticality.

Safety systems shall be operationally independent from control systems and other networks. While it is often necessary for the safety system to be connected to control system networks for operator, engineering and administrator access, the safety system should not be connected to the control system networks in a manner that safety system functions and communications can be disrupted or otherwise compromised through the control system.

Devices that utilise wireless communication (e.g. WirelessHART, ISA100, Bluetooth, Wi-Fi, or other short- and long-range wireless technologies) should be placed in separate wireless networks segmented from wired OT networks. Communication between wireless and wired segments should be strictly controlled at defined boundaries to limit exposure and prevent unauthorised access or lateral movement of threats into wired OT networks.

Switches used for OT networks should be dedicated to OT traffic only to prevent potential crossover risks and ensure strict isolation between the OT environment and the IT environment.

References

NIST CSF 2.0: PR.IR

IEC 62443-2-1: NET 1.1, NET 1.3, NET 1.6, NET 2.2

IEC 62443-2-4: SP.05.02, SP.05.03

IEC 62443-3-3: SR 5.1, SR 5.2

NIST SP 800-82 Rev. 3: Clause 5.2.3.1, Clause 5.4, Clause 6.2.9, Appendix E.1

2.12 CSBR 12 OT DMZ

Control

An OT DMZ shall be established as a buffer zone between the enterprise IT and OT networks.

Objective

To securely control communication and restrict logical access and data flows between IT and OT networks.

Requirements

12-1 The OT DMZ shall be physically or logically separated from both IT and OT networks using firewalls or unidirectional gateways.

12-2 All network traffic between enterprise IT and OT networks shall be terminated in the OT DMZ. This is not applicable if the communication flows from OT to IT traverse hardware-enforced unidirectional gateways.

12-3 Only explicitly authorised communication flows shall be permitted between the enterprise IT and OT networks through the OT DMZ.

12-4 Components within the OT DMZ shall not initiate communication to OT systems if they have processed or relayed traffic initiated from IT to the OT DMZ. This is not applicable for traffic initiated from the secure remote access system.

12-5 Access to the OT DMZ shall be restricted to authorised users, applications, and devices.

12-6 The OT DMZ shall enforce separate user credentials from both enterprise IT and other OT segments.

12-7 Systems in the OT DMZ shall be regularly patched, hardened against vulnerabilities, and be designed to support security patching during normal operation.

12-8 The OT DMZ shall follow segmentation principles in *CSBR 11 Network segmentation*.

Supplementary Guidance

The OT DMZ is a dedicated security layer that sits between the corporate IT network and the OT network. Its purpose is to create a controlled and monitored space where necessary data exchange and services can take place without allowing direct connections between IT and OT systems. The OT DMZ consists of firewalls to separate IT and OT networks, switches for internal segmentation, and servers for services such as jump hosts for secure remote access, patch management servers, antivirus update distribution, data historians, and proxies.

Next-generation firewalls with deep packet inspection capabilities should be deployed to filter traffic between IT and OT environments. A dual-firewall architecture is recommended. Using firewalls from different suppliers can provide additional security by reducing the risk of common vulnerabilities being exploited across both firewalls but is only recommended if the organisation has the capability and competence to maintain firewalls from different suppliers. In the event dual-firewall architecture

is implemented, it is recommended that different teams manage the IT-facing and OT-facing firewalls. This approach strengthens security, enforces segregation of duties, and helps mitigate the risk of misconfigurations or insider threats.

It is highly recommended to run all OT DMZ equipment on dedicated hardware to physically segment it from both IT and other OT systems.

Administration of the OT DMZ should be from the solution or zone with highest criticality.

Purdue model drawings can be used to show where the OT DMZ should be located in the OT environment.

References

NIST SP 800-82 Rev. 3: Clauses 5.2.3.1 and 5.4

IEC-62443 3-3: FR 5, SR 5.1, SR 5.2

2.13 CSBR 13 Secure remote access

Control

The asset owner shall have policies, procedures and security capabilities, to handle remote access in a secure way.

Objective

To ensure that remote access is managed securely so that integrated operations, digitalisation, and interoperability with external parties can be performed without degrading the asset's cyber posture.

Requirements

13-1 The asset owner shall ensure that all methods of access to the OT environment via untrusted networks can be monitored and controlled.

13-2 The remote access applications shall be approved by the asset owner before use.

13-3 The asset owner shall have policies and procedures around the use of remote access to the OT environment.

13-4 The remote access solutions providing interactive remote access sessions shall, as a minimum, provide technical capabilities to:

a) Authenticate and validate users and client devices
b) Authenticate and encrypt all connections conducted over untrusted networks
c) Enforce granular access controls, based on least-privilege
d) Support time-restricted and duration-limited access sessions
e) Automatically suspend or terminate idle sessions
f) Integrate with identity and access management (IAM)
g) Support multi-factor authentication (MFA)
h) Require explicit approval and defined purpose for access (e.g., work permit)
i) Provide comprehensive monitoring, logging, and audit trails
j) Support secure file transfer with malware scanning
k) Support OT gateway termination and inspection of network traffic entering and leaving the OT environment

13-5 The asset owner shall have policies and procedures around authorising, authenticating, encrypting, documenting, logging and monitoring all interactive remote access connections. Documentation for each connection shall include, but not be limited to:

a) identity of the remote interactive user
b) its purpose
c) the remote access application used
d) encryption and authentication technologies used
e) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through an OT DMZ) with instructions, as necessary
f) the circumstances requiring the connection

g) the length of time the connection needs to be open, including expected inactivity periods
h) the location and identity of the remote client device, application and user
i) any compliance requirements that need to be met prior to establishing the connection

Supplementary Guidance

Remote access refers to any access to the OT environment from non-OT environments through one or more communication pathways, including access from enterprise IT environments, suppliers, service providers, or contractors.

Remote access applications are applications, protocols, or services that enable interaction with the OT environment from non-OT networks, including both interactive access such as remote desktop or engineering sessions, and non-interactive communication such as data exchange using protocols like Open Platform Communications (OPC).

Remote access solutions are security-controlled systems or products that enable authorised employees, contractors, or suppliers to operate, maintain, or update the OT environment remotely in a secure manner. Remote access solutions represent a subset of remote access applications and are characterised by providing interactive remote access sessions and enforcing security controls for such sessions.

Remote access solutions are considered part of the OT environment and provide enforcement functions such as authentication, authorisation, monitoring, and session control.

Remote access applications should be investigated to ensure that the version and configuration settings for the application(s) used do not have any known vulnerabilities. New remote access applications should not be used until they are carefully evaluated and tested by reputable and well-known third parties for security weaknesses.

Any use of remote access should require explicit approval and defined purpose for access to be documented along with any instructions that are needed to prepare and use connections. The documentation should indicate why the connection is needed, how long it needs to be open, if there are any expected inactivity periods, and the condition/circumstance that causes the connection to be needed.

The remote access solution should support real-time supervision of active sessions to allow production engineers to supervise and support during remote activities.

OT gateways enable termination of all remote access connections at a secure gateway to enable deep package inspection, protocol conversion, intrusion detection or prevention, and enforcement of security policies.

Secure file transfer with malware scanning should be applied for files transferred both into and out of the OT environment.

It should be ensured that monitoring, logging, and auditing capabilities contribute to real-time tracking and recording of user sessions. User activities and connections should be logged to provide visibility, accountability, and a complete audit trail for compliance and security management, and to enable monitoring and termination of sessions when required.

References

IEC 62443-2-1: SPE 3 NET 3.1, NET 3.2, NET 3.3

IEC 62443-2-4: SP.07.01 BR, SP.07.02 BR, SP.07.03 BR, SP.07.04 BR, SP.07.04 BR RE(1)

IEC 62443-3-3: SR 1.13, SR 2.6 BR

IEC 62443-4-2: CR 2.6 BR

DNV-RP-G108

2.14 CSBR 14 Identity and account management

Control

A process that secures identification of users and management of accounts in the OT environment shall be in place and effective.

Objective

To prevent unauthorised access while allowing authorised users and systems to do everything they need to do, but not more.

Requirements

14-1 A procedure for management of accounts in the OT environment shall be established, documented and enforced.

14-2 The OT environment shall use a dedicated identity and account management solution that is independent of other environments.

14-3 All accounts access shall be provisioned, changed or deprovisioned as the result of an authorisation process.

14-4 All accounts shall be configured according to the principle of least privilege.

14-5 Records shall be maintained of user accounts, and shall as a minimum contain user identity, assigned role, privileges and the approver of the authorisation.

14-6 All accounts shall be reviewed at regular intervals.

14-7 Suppliers and contractors shall notify the asset owner of any change to users and systems with accounts.

14-8 Use of strong passwords shall be mandatory where possible. Passwords shall be changed whenever there is reason to believe that they are known by users that do not have legitimate need for access.

14-9 Passwords shall not be stored or written down where they can be discovered by users without legitimate need to access the account.

14-10 Account authentication mechanism shall be proportional to the risk posed by breach of the account.

14-11 User accounts shall be suspended or removed as soon as they are no longer needed.

Supplementary Guidance

The term ‘accounts’ in this CSBR shall be widely understood as both user accounts and system accounts.

Procedures for management and authorisation of user accounts should cover provision of accounts for new users, change of privileges for existing users, and deprovision of accounts for users that no longer need access.

Requests for privileges should be put forth for approval through an access request, specifying the individual that will use the account and the requested role or privileges. Access should only be granted for users with a legitimate need, granting the specific user access only to the information, functionality and privileges needed to perform the work and limited to the time needed for the work to be completed. It is recommended that personal accounts are given or elevated to administrative privileges only for specific durations or tasks, automatically revoking them afterwards (just-in-time privileged access).

The principle of separation of duties should be followed to avoid conflicts of interest. A user who has been given privileged access, should not be allowed to further distribute privileges. The approval should be done on the appropriate level, and the implementer of account configuration should not be the same person. It's recommended that only authorised OT system administrators should be able to create, maintain, and delete accounts on OT systems and applications.

It is recommended that the account review also includes verifying that active accounts only have the minimum privileges required to carry out their job. Review and management of active and passive user accounts should be proportional to the criticality and the risk of the system. The need for availability of the system, such as in central control room should be considered. For system that are centrally managed, engineering workstations, or major safety and control systems the interval for account review should not be longer than 12 months.

Records of user accounts should include historical information, such as changes in privileges and previously used accounts that have later been deprovisioned. Wherever possible, users should identify as individuals. Where shared login/password is used to access a system, a process should be in place to document and follow up the use of such accounts through a record.

Suppliers and contractors should have a contractual obligation to the asset owner to notify of any changes in resources that have accounts. The reporting should include change of role, personnel transfers, or terminations.

Passkeys or other FIDO2-implementations should be used were reasonably practicable. Long passphrases instead of complex passwords are recommended. Longer passphrases for privileged accounts should be required. Re-use of passwords used in other domains (e.g., the IT environment) or for private purposes (e.g., social media) should be discouraged. Use of password vaults is recommended. Passwords should be screened against known breach corpuses. The authentication mechanism should be proportional to the risk posed by breach of the system. Multifactor authentication should be enforced where reasonably practicable.

For high-risk systems, Authenticator Assurance Level 2 (AAL2) or higher, as defined in NIST SP 800-63B, should be enforced outside trusted zones.

References

IEC 62443-2-1: SPE 6

IEC 62443-2-4: SP09.01-09

IEC 62443-3-3: SR1.3, SR1.4, SR 2.1

NSM ICT Security Principles: Chapter 1.3

NIST SP 800-82 Rev. 3: Clauses 5.15, 6.2.1 and 6.2.7

NIST SP 800-53 Rev. 5: AC-17, AC-20, PS-7

NIST SP 800-63B: 5.2, 6.2

2.15 CSBR 15 Security hardening

Control

Implement configuration settings and measures that enhance system security by reducing the attack surface.

Objective

To strengthen the security posture of OT systems and applications by applying rigorous configuration settings and protective measures, thereby minimising the attack surface.

Requirements

15-1 An OT hardening specification shall be in place, describing applicable hardening requirements for each relevant type of OT device and system.

15-2 Interfaces for portable media shall only be enabled when authorised for use and disabled when not authorised for use.

15-3 Software applications and services (e.g., email clients, office applications, games) shall be removed or disabled if they are not required for the operation of the OT system.

15-4 Associated communication paths (e.g., TCP/UDP ports, firewall openings) that are not required or are linked to disabled software and services shall be removed or disabled.

15-5 Wireless communications that are not required by the OT systems shall be removed or disabled.

15-6 Network ports that at not in use shall be blocked or disabled. For network devices, ports shall be “configured down”.

15-7 Physical and logical access to diagnostic and configuration ports, programming devices, and engineering workstations shall be protected from unauthorised access and use.

15-8 Default credentials shall be changed prior to deployment in the production environment.

15-9 The hardened state of the OT system shall be maintained during its lifetime through maintenance procedures.

15-10 Capabilities to ensure that devices cannot be forced to revert to default settings shall be in place.

Supplementary Guidance

Security hardening should be applied across all layers of the system, including the network, physical infrastructure, BIOS and firmware, operating system, hypervisor, virtual machines, and domain components.

Security hardening should be based on templates. A company hardening strategy may be limited in scope, in such cases, supplier-provided hardening guidelines or publicly available guidelines can be

used. CIS Benchmarks and Microsoft Security Compliance Toolkit may be used as the primary reference where applicable.

Checklists should be used as documentation of the implemented hardening and as input for verification.

Protecting physical ports can be implemented by limiting access to the room, the rack, or the physical port on device. Robustness of the physical protection measures should reflect the criticality of the system. As a minimum, the room or the cabinet where the equipment is placed should have access restrictions, such as being physically locked, with keys to locks managed through a key management system. Locks for which keys can be easily obtained should be avoided. Removable media interfaces (e.g., USB, SD cards) may need to be disabled or physically removed when not in use. Examples of diagnostic and configuration ports are iDRAC, iLO, and serial console ports.

Where possible, use centralised configuration management tools (e.g., Group Policy Objects via Active Directory) to enforce hardening policies consistently.

Security hardening of a system should be performed in a dedicated network segment where the target system is isolated from other OT systems, but at the same time has access to the necessary OT services required for the hardening operation. New systems shall be fully hardened before being connected to a live production environment.

Implement monitoring systems to verify the hardened state of components. Testing should be scheduled on a regular basis to verify that hardening over time is not degraded. Where automated monitoring is not feasible, establish manual verification procedures. The result should then be used as input to the risk assessment process and adjustment of cyber controls and measures.

References

IEC 62443-2-1: COMP 1.1

IEC 62443-2-4: SP 09.07, SP 02.03

IEC 62443-3-3: SR 7.7

IEC 62443-4-2

CIS Benchmark

2.16 CSBR 16 Malicious software

Control

Effective measures for protecting against malicious software shall be in place and effective.

Objective

To reduce the risk of malware impacting the productivity, reliability and safety of the OT systems.

Requirements

16-1 OT system devices vulnerable to malware threats shall be malware protected. For control system devices where it is not technically feasible to run anti-malware software on the device, protective measures that give a similar protection level shall be in place.

16-2 Anti-malware repositories and software shall be managed centrally. The system shall collect, monitor and show status of relayed alerts from managed OT devices.

16-3 A solution for anti-malware scanning of all removable or portable storage media, service laptops and configuration devices shall be implemented for the OT environment.

16-4 A secure access solution shall include malware scanning to ensure that files are malware free before being transferred to the OT environment.

16-5 The anti-malware system shall be maintained so that both malware signatures and the anti-malware system itself is kept up to date.

16-6 All storage media, configuration devices, nodes or control devices shall be verified free from malware before connected to the control system.

Supplementary Guidance

For devices where it is not feasible to run anti-malware software on the device, the device should be placed into a separate network zone with higher enforcement of strict network traffic control. In addition, offline scan of device software should be performed regularly and when implemented in the system.

The anti-malware scanning solutions software should be updated on a regular basis, malware signatures should be updated daily. For devices in the OT environment where automatic update of anti-malware software and signatures is not possible, e.g. devices in isolated network zones, the supplier should support to provide measures and procedures for manual update of anti-malware software and signatures.

For increasing malware detection capabilities, an anti-malware system can be implemented on the external facing firewall separating the enterprise network and OT DMZ networks to detect and block malware from entering the OT environment. For additional detection of irregular network traffic in the OT environment, an Intrusion Detection System (IDS) should be considered.

Devices connected to the centralised anti malware solution should check for updated malware signatures daily. The repository should be updated whenever new signatures are known and

approved for use. If anti-malware updates need supplier approval, the signature file should be tested and approved by the supplier before installation. Testing should preferably be done on a dedicated test system.

Alerts from anti-malware software should be sent to the central management system and in addition be available through the device user interface. If the anti-malware software on a device fails to communicate with a central management system, an alarm should be generated.

If enterprise monitoring or SOC is in place the alarms should be relayed.

A centralised management of the anti-malware systems reduces the need for manual check of individual endpoints and enables real-time monitoring and tailored endpoint protection.

Where technically feasible, scanned portable devices should be given a validity period, so that a re-scan should be done on regular basis.

The anti-malware procedure should cover update of both malware signatures and the anti-malware system itself. The procedure should cover all types of anti-malware systems used in the OT environment, including anti-malware software on endpoints (computers), network-based anti-malware systems, and anti-malware scanning solutions for removable and portable media.

A systematic approach for controlled use of delayed anti-malware signature updates (e.g. 48/72 hours) where required to maintain OT system integrity and availability is recommended. Such delays should be risk assessed, documented and approved prior to implementation. Updates should be tested and validated, preferably in a dedicated test system, with appropriate monitoring and compensating controls applied during the delay period.

References

IEC 62443-3-3: SR 3.2

NIST SP 800-82 Rev. 3: Clause 6.2.17

NIST SP-800-83 Rev. 1

NSM ICT Security Principles: Chapter 3.2

2.17 CSBR 17 Virtualisation

Control

Virtualised solutions shall maintain security measures as set forth in this guideline as well as specific measures related to virtualisation.

Objective

To enable the use of virtualisation for OT systems without compromising the cyber security of the systems.

Requirements

17-1 Decisions about which OT systems may be hosted on the same virtualisation infrastructure shall be based on a risk assessment.

17-2 On-premises OT systems shall not live in the same virtualisation infrastructure as IT systems.

17-3 Management of the virtualisation infrastructure shall be performed from the network zone with the highest criticality hosted on the virtualisation infrastructure.

17-4 The virtualisation infrastructure necessary for continued safe operations shall be able to operate and be managed in "island mode", see *CSBR 20 Island mode*.

Supplementary Guidance

When deciding which systems can live on the same virtualisation infrastructure a risk assessment should consider criticality, availability, network segmentation, and corresponding Purdue level of the systems to be hosted (virtual machines on the infrastructure).

Role-based access control (RBAC) should be used for controlling access to the virtualisation environment. Typical roles can be Administrator (full control of the virtualisation environment), Operator (allowed to access and power down/up her own virtual machines), and User (allowed to access the console of her virtual machines). It should be emphasised that the requirements in *CSBR 11 Network segmentation* and *CSBR 14 Identity and account management* also apply in virtualised environments. A directory service (typically Microsoft AD) makes the implementation and maintenance of users and roles more effective and should be implemented.

Review and validate network segmentation policies in virtual switches and firewalls to ensure they match the designed network segmentation.

When hosting OT systems with different criticality levels on a shared virtualisation platform, it is recommended to group the virtual machines according to their criticality rating and allocate these groups to separate physical hosts to gain segmentation according to the criticality rating and reduce risk.

Systems and network zones which are not required for continued safe operations can be considered for virtualisation in a cloud. This includes systems rated medium or low criticality according to Offshore Norge 123. The cloud service provider should be aligned with the Cloud Security Alliance (CSA) recommendations.

References

NIST SP 800-125

NIST SP 800-125A Rev .1

NIST SP 800-125B

Offshore Norge 123

Cloud Security Alliance (https://cloudsecurityalliance.org)

2.18 CSBR 18 Security monitoring and alerting

Control

Security monitoring and alerting capabilities tailored for OT systems shall be in place and effective.

Objective

To enable a timely and effective response to security incidents by identifying threats and anomalies in OT systems through continuous monitoring and ensuring relevant personnel are alerted.

Requirements

18-1 Cyber security event and audit logs that can be used to detect and confirm suspicious activities and/or security violations shall be identified, enabled and stored.

18-2 A centralised system shall be used to collect event and audit logs.

18-3 Collected event and audit logs that can assist in analysis and forensics shall include, but are not limited to:

a) access control logs
b) operating system audit logs
c) system startup and shutdown events
d) configuration change events
e) backup and restoration events
f) malware alerts
g) dropped firewall events

18-4 All event and audit logs shall include a date and timestamp that is synchronised and consistent across all OT systems, regardless of their local time zone settings.

18-5 Collected event and audit logs shall be retained for at least 12 months and be protected from tampering and deletion.

18-6 Traffic analysis network sensors shall be deployed to continuously monitor network traffic, enabling the detection of anomalous activity in real time. The selection of network traffic for monitoring shall be determined through a risk-based approach.

18-7 Systems used for analysis of logs and network traffic shall be continuously adapted to the evolving threat landscape.

18-8 Cyber security event and audit logs shall be continuously monitored to identify anomalies and indicators of compromise.

18-9 Alerts generated shall be reviewed and acted upon without undue delay by personnel trained in handling cyber security incidents.

18-10 Policies, procedures and processes related to capturing and analysing logs, reviewing, reporting and responding to events shall be established.

18-11 Security monitoring and alerting shall not interfere with the functionality of the OT system.

Supplementary Guidance

A Security Information and Event Management (SIEM) solution can be used to centrally collect, store, correlate, and analyse event and audit logs to enable detection, alerting, and investigation of suspicious activities. Measures should be taken to ensure that onboarded log sources are always functional.

The syslog protocol is commonly used to enable access to event logs. The supplier may also have a set of event logs which should be considered when establishing event and log collection.

It is recommended to retain logs beyond 12 months. To protect the integrity of event and audit logs, these should be encrypted when collected and stored in immutable storage solutions outside the OT environment.

Selection of network traffic data to be monitored should be based on the system in question's exposure to other systems in combination with its criticality. As an example, it is important to monitor DMZ networks and other networks where OT is connected to non-IT or external systems.

Design and implementation of security monitoring and alerting solutions should be done together with the OT system supplier to ensure optimal results and development of meaningful monitoring dashboards.

Monitoring capabilities should enable inspection of industrial protocols used in the OT environment. Where possible, 'accepted' firewall event logs are useful to collect because they reveal successful attacks or breaches. Monitoring capabilities should be periodically validated through exercises or simulated detection scenarios.

Systems used for analysis of logs and network traffic should be continuously adapted to the evolving threat landscape. The adaptation should include appropriate dimensions. Dimensions that should be considered may include integration of relevant supplier advisories, use of applicable sector-specific threat intelligence feeds, updates to detection rules based on emerging threats and observed attack patterns, and periodic review of detection logic. The detection logic should also be reviewed against recognized threat models, such as MITRE ATT&CK for OT, to account for evolving adversary techniques and tactics.

It is recommended that organisations utilise a Security Operations Centre (SOC) to assist in meeting requirements under this CSBR.

The effectiveness of security monitoring and detection capabilities should be regularly assessed to support continuous improvement of monitoring and response processes.

References

IEC 62443-2-1: SPE 7

IEC 62443-3-3: SR 2.8, SR 6.2

NIST CSF 2.0: DE.CM

2.19 CSBR 19 Incident response

Control

An incident response capability for the OT environment shall be established, assigning clear roles, responsibilities, procedures and practical measures.

Objective

To manage cyber security incidents and minimise their impact through timely and coordinated response actions.

Requirements

19-1 An OT specific incident response plan shall be established, describing goals, strategies, roles, responsibilities, procedures, and required competencies.

19-2 A documented process for performing initial assessment (triage) and classification of cyber security events and incidents affecting the OT environment shall be in place.

19-3 Clear requirements and mechanisms for reporting cyber security incidents affecting the OT environment shall be defined and available internally and externally.

19-4 A process for containment of cyber security incidents shall be in place, ensuring rapid isolation of affected systems and components.

19-5 A process for eradicating cyber security incidents shall be in place, ensuring removal of malicious artifacts, unauthorised access, or compromised components.

19-6 Criteria for declaring systems and components, as well as the OT environment as a whole, as clean and ready for operation shall be in place.

19-7 Incident response plans shall be regularly reviewed and updated to reflect changes in requirements, threats, technology, and lessons learned from exercises.

19-8 Service Level Agreement (SLA) with incident response parties shall define response time and support capabilities for responding to OT cyber security incidents.

19-9 Incident response capabilities shall be tested and verified to be effective through regular training and exercises.

Supplementary Guidance

It is recommended that organisations develop and maintain a comprehensive incident response plan for cyber security incidents affecting the OT environment. The plan should provide clarity on roles

and responsibilities, objectives, priorities, strategies, and the processes and procedures that support effective incident handling. Ensuring that these elements are documented, communicated, and understood across the organisation is the foundation for a coordinated and timely response.

The plan should include updated contact information for all relevant internal and external stakeholders, along with descriptions of the competencies needed to carry out remediation and

mitigation activities. The plan should describe interaction between stakeholders during an incident response scenario, including the emergency preparedness organisation, suppliers, specialised incident response teams, sectorial response milieus, and national response centres. It is recommended that criteria for escalation, de-escalation, and declaring an incident as handled and stakeholders informed, are described in the incident response plan. In addition, the incident response plan should require documentation of the incident timeline, including detection, analysis, containment, eradication and recovery activities, to support situational awareness, coordination, reporting, post-incident analysis, and lessons learned.

Processes, procedures and technical measures for performing triage support the organisation in evaluating and prioritising events and their criticality. The process, procedures and tools utilised in performing triage should be reviewed and evaluated periodically to ensure that they are effective and fit for purpose. Triage and containment activities should also consider impacts on key network segments, zones and conduits, and provide an overview of potential operational and safety consequences, rather than focusing solely on individual systems or components. The description of containment procedures should include methods such as system isolation, micro-segmentation, or island mode.

The incident response capability should include a defined approach for evidence and data collection, describing what types of data are required (e.g. logs, network traffic, system states), where such data is located in the OT environment, and how it can be retrieved in a safe and controlled manner.

A well-defined eradication procedure should ensure that malicious artifacts, unauthorised access points, and compromised components are verified to be eradicated following a cyber security incident. Regular review and testing of eradication procedures are recommended to be included in incident response training.

The incident response plan should also emphasize the role of backups in response and recovery, including verification of backup integrity, availability of offline or immutable backups, and procedures for restoring OT systems to a known good state following an incident.

Service Level Agreements (SLAs) with incident response parties should, as a minimum, specify expected timelines for initial response, escalation procedures, and the scope of technical and advisory assistance available. It is recommended that both internal and external providers of incident response capabilities (such as CSIRT) document that team members in relevant responder roles meet minimum competence requirements and participate in at least one incident response exercise per year.

It is recommended that incident response capabilities are exercised, reviewed, and tested for effectiveness at planned intervals. In determining an appropriate frequency, consideration should be given to relevant standards, changes in risk, threat level, systems, suppliers and organisation. As a baseline, exercises and verification of capabilities should be performed annually.

Lessons learned from exercises and incidents handled should be systematically gathered and evaluated for continuous improvement, as well as shared with all relevant personnel for learning purposes.

References

NIST-800-82 Rev. 3

NIST-800-53 Rev. 5: IR-4

NIST-800-61 Rev. 3

NSM ICT Security Principles: Chapters 2.9.3, 4.1.1, 4.1.3, 4.1.4, 4.1.5 and 4.1.6

2.20 CSBR 20 Island mode

Control

The infrastructure shall have the capability to prevent any network communication between OT networks and non-OT networks (also termed island mode).

Objective

To prevent threat movement across the IT/OT boundary when a cyber security incident is detected or suspected in either the OT environment or in non-OT environments.

Requirements

20-1 The OT environment shall be designed to support continued safe operations when communication with non-OT networks is disconnected or lost.

20-2 The operational and cyber security consequences of going into island mode shall be identified, understood, and documented.

20-3 The OT environment shall have a simple and easily executable mechanism for physically or logically disconnecting OT systems from external networks.

20-4 The asset owner shall have policies and procedures that describe the use of island mode.

20-5 Site personnel shall be trained in activating island mode through regular exercises.

Supplementary Guidance

To reduce the risk of external exposure or compromise of the OT environment, a facility may choose to temporarily disconnect all network connections between the OT environment and any non-OT networks. This is termed activating island mode and is typically done as part of a contingency plan during an actual or suspected cyber security incident to prevent spread of threats across the OT boundary.

Policies and procedures should clearly define the conditions and criteria for activating island mode, including both planned and emergency scenarios. They should outline the expected operational and cyber security impacts of network isolation, specifying how different OT systems will be affected. Additionally, they should provide alternative workflows, communication methods, and contingency measures to ensure safe and efficient operations while in island mode. Procedures should also describe how to securely restore connectivity to non-OT networks when exiting island mode.

The OT environment should be specifically designed to ensure that safe operation can continue while the connection to external networks is lost or deliberately deactivated as part of the contingency plan. That is, failure of network communications with external systems should not cause OT systems to fail. OT systems may operate in a degraded mode or less optimised way when in island mode, but, at a minimum, it should be possible to continue essential functions.

A mechanism for temporary disconnection of OT environment from non-OT networks should be specifically designed and verified to ensure disconnection can be done correctly and rapidly by site personnel also during stressful situations. Disconnection techniques could include manual

disconnection, such as pulling clearly marked ethernet cables or operating firewall operator panels. It is not recommended to base disconnection techniques on manually changing firewall rules as this can be difficult to carry out correctly in stressful situations.

References

IEC 62443-2-1: NET 1.4, NET 1.5

IEC 62443-3-3: SR 5.2 RE 2

NIST SP 800-82 Rev. 3: Clause 5.2.3.1

2.21 CSBR 21 Backup and restore

Control

Implement and maintain processes and systems for regularly backing up system configuration and data as well as ensuring the ability to restore it to maintain system integrity and availability.

Objective

To ensure the reliability and availability of critical systems by establishing robust backup procedures and efficient restoration capabilities.

Requirements

21-1 A documented process for backing up all critical OT systems shall be in place, clearly defining backup frequency, roles and responsibilities, and execution methods.

21-2 OT systems with frequent changes shall be backed up on scheduled basis.

21-3 OT systems which are rarely changed shall have initial backup and backup after changes.

21-4 All backups shall be stored securely with appropriate physical security measures and/or logical access controls to protect against unauthorised access or damage.

21-5 Backups for all OT systems shall be stored in a manner that is segregated from the local network to minimise the risk of compromise during network attacks.

21-6 All critical OT systems shall have an offline backup, and the backup integrity shall be verified to ensure it is functional for use.

21-7 An up to date restore procedure shall be maintained for all systems, ensuring that data can be effectively restored in case of data loss or system failure.

21-8 For critical OT systems, both the backup procedure and restore procedures shall be verified annually to ensure their effectiveness and reliability.

Supplementary Guidance

Define backup strategy based on system criticality and change frequency. Systems with infrequent changes may be backed up after each change, while systems with frequent changes should have scheduled backups. When scheduled backups are used, the process should be automated to ensure consistency and reduce human error.

Ensure backup and restore processes support broader disaster recovery and business continuity plans. Define acceptable recovery time objectives (RTO) and recovery point objectives (RPO) for critical systems. It is recommended to perform an annual restore test for all critical systems to verify the effectiveness of backup and recovery procedures.

Use supplier-recommended tools or validated procedures for creating backups of configurations, logic, and data. Ensure backups are complete and include all necessary files for restoration.

Store backups in a secure, access-controlled environment. All backups should be encrypted to protect data confidentiality and integrity. Evaluate the use of immutable storage to prevent unauthorised changes or deletion of backup data.

Consider maintaining a long-term backup copy for critical systems. In addition to regular backups, evaluate storing an additional copy for an extended retention period, minimum one year. This copy can serve as a recovery point in case of incidents where recent backups may be compromised or unusable.

References

IEC 62443-3-3: SR 7.3, SR 7.4

IEC 62443-2-1: SPE 8

IEC 62443-2-4: SP12

NIST CSF 2.0: PR.DS, RC.RP