IEC 62443-2-1

Edition 2.0 2024-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

HORIZONTAL PUBLICATION
PUBLICATION HORIZONTALE

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

Sécurité des systèmes d'automatisation et de commande industrielles – Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

IEC 62443-2-1:2024-08(en-fr)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC 62443-2-1

Edition 2.0 2024-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

Sécurité des systèmes d'automatisation et de commande industrielles – Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-9459-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial process measurement, control and automation, in collaboration with the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is an International Standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) revised requirement structure into SP elements (SPEs),
b) revised requirements to eliminate duplication of an information security management system (ISMS), and
c) defined a maturity model for evaluating requirements.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65/1044/FDIS	65/1053/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document is the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [1][1] describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

1 Numbers in square brackets refer to the Bibliography.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization needs and objectives, security requirements, business and work processes, as well as the organization size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

1 Scope

This part of IEC 62443 specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as wireless) or functions (such as remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

Figure 1 illustrates the roles and responsibilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [2] and technical security capabilities defined in IEC 62443-3-3 [3] and IEC 62443-4-2 [4].

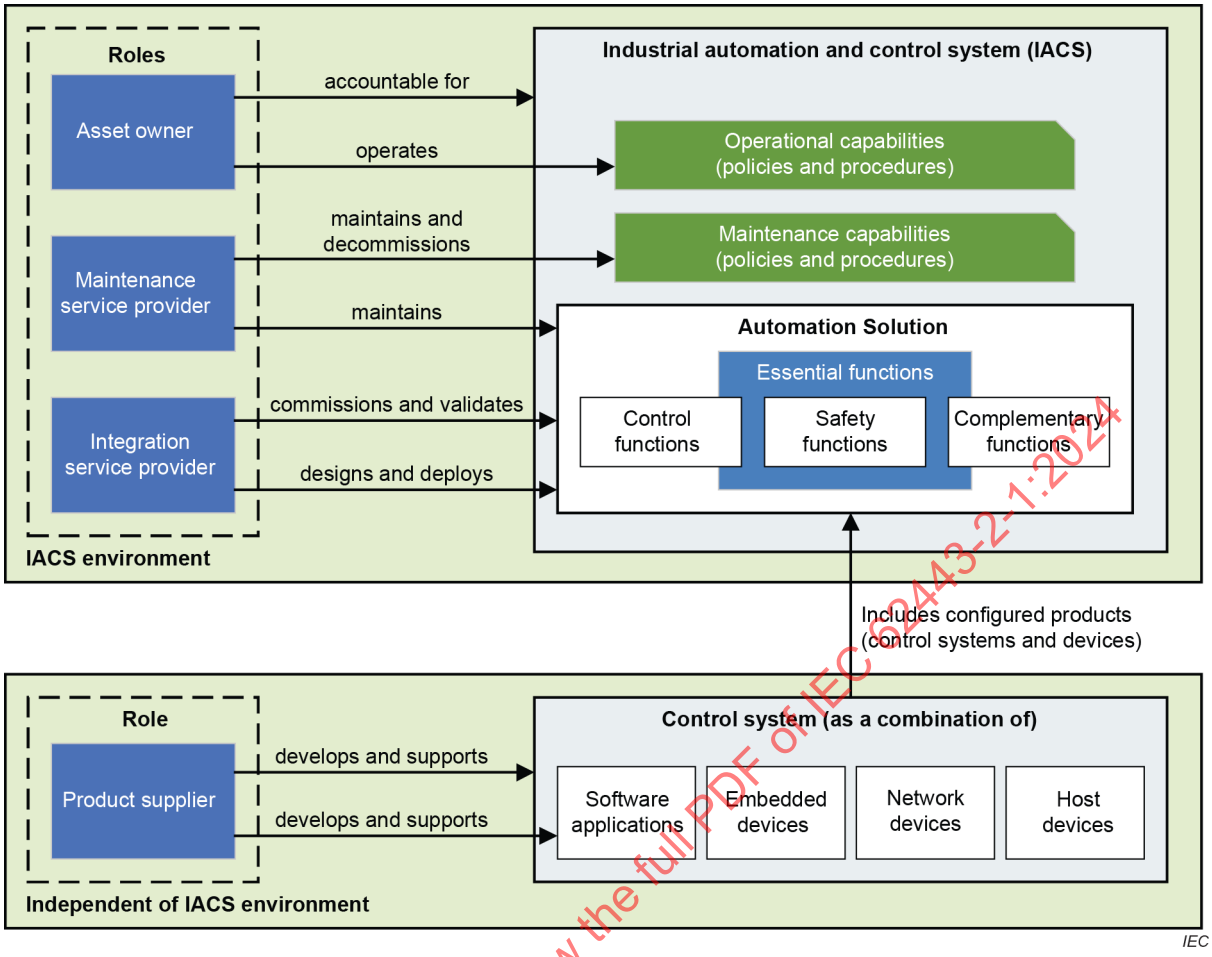

Figure 1 – Roles and responsibilities in the IEC 62443 series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62443-1-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
access right
permission to access system resources or privilege to execute system functions

Note 1 to entry: Permissions are generally rights to access resources such as data and executable files, while privileges are generally rights to execute function calls provided by the operating system (OS).

3.1.2
asset owner
organizational role ultimately accountable for one or more IACS

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: In the context of this document, asset owner also includes the operator of the IACS.

[SOURCE IEC 62443-3-3:2013, 3.1.2, modified – Changed in definition "individual or company responsible" into "organizational role ultimately accountable" to reflect role; in Note 1 to entry changed "The term "asset owner" is used" into "Used"; removed Note 2 to entry; in Note 3 to entry changed "this standard, an asset owner" into "this document, asset owner".]

3.1.3
Automation Solution
control system and any complementary hardware and software components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this document.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution can be comprised of components from multiple suppliers, including the product supplier of the control system.

3.1.4
compensating security measure
security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE 1 (Component-level) A locked cabinet around a controller that does not have sufficient cyber access control security measures.

EXAMPLE 2 (Control system/zone-level) Physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS.

EXAMPLE 3 (Component-level) A product supplier's programmable logic controller (PLC) cannot meet the access control capabilities from an asset owner, so the product supplier puts a firewall in front of the PLC and sells it as a system.

3.1.5
consultant
subcontractor that provides expert advice or guidance to their clients, such as product suppliers, integration and maintenance service providers and asset owners

3.1.6
device
asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

EXAMPLES Controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.7
maturity level
qualitative method of characterizing the capability of an organization to implement security requirements according to documented policies and procedures and their historical performance in doing so

3.1.8
portable media
portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to, compact disc (CD) / digital versatile disc (DVD) / Blu-ray media, universal serial bus (USB) memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds and portable computers.

Note 2 to entry: The term "removable media" is another term that is often used for "portable media".

3.1.9
product supplier
organizational role responsible for the manufacture and support of IACS hardware and/or software products

Note 1 to entry: This term is used in place of the generic word "vendor" to provide differentiation.

3.1.10
security capability
technology or procedural measure, feature or mechanism that can be used to provide protection against cyber and physical security attacks

Note 1 to entry: Security capabilities are typically implemented through some combination of technology and procedural means. The term "countermeasure" is often used to describe the implementation of "security capability".

Note 2 to entry: The term "control" is also used to describe this concept in some contexts. The term "security capability" has been chosen for this document to avoid confusion with the word "control" in the context of "process control".

3.1.11
security compromise
violation of the security of a system such that an unauthorized (1) disclosure or modification of information, (2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

[SOURCE IEC 62443-2-4:2023, 3.1.20, modified – Changed in definition "(2) denial of service could possibly have occurred" into "(2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred".]

3.1.12
security incident
security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term "of some significance" is relative to the environment in which the security compromise is detected. For example, the same compromise can be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

[SOURCE IEC 62443-2-4:2023, 3.1.21]

3.1.13
security management system
SMS
set of interrelated or interacting elements of an organization to establish security policies and objectives and a set of systematic processes to achieve those objectives

Note 1 to entry: This definition is based on the ISO/IEC 27000:2018, 3.41 [5] definition of "management system" and its description.

3.1.14
security patch
incremental software change in order to address a security vulnerability, a bug, reliability or operability issue (update) or add a new feature (upgrade)

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches can address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

3.1.15
security program
SP
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures and products that are applicable to the IACS

Note 1 to entry: The SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

[SOURCE IEC 62443-2-4:2023, 3.1.23, modified – Added SP; in Note 1 to entry replaced "security program" with SP, replaced "service providers" with "asset owners" and added "This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface."]

3.1.16
service provider
organizational role responsible for providing services and associated supplies for the IACS in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word "vendor" to provide differentiation.

3.1.17
software service
software program that is installed and managed by infrastructure software instead of by or on behalf of a logged-on user, typically without a user interface of its own

Note 1 to entry: Some OSs allow logged-on users with elevated privileges to start/stop software services.

3.1.18
tolerable risk
level of risk deemed acceptable to an organization

Note 1 to entry: Organizations should include consideration of legal requirements when establishing tolerable risk. Additional guidance on establishing tolerable risk can be found in ISO 31000 [6] and NIST SP 800-39 [7].

Note 2 to entry: IEC 62443-3-2 provides guidance for establishing tolerable risk.

[SOURCE IEC 62443-3-2:2020, 3.1.22, modified – Added Note 2 to entry.]

3.2 Abbreviated terms and acronyms

This subclause defines the abbreviated terms and acronyms used in this document.

ANIMA	autonomic network integrated model and approach[2]
ANSI	American National Standards Institute
API	application programming interface
BCP	business continuity plan
BOOTP	bootstrap protocol
BRSKI	bootstrapping of a remote secure key infrastructure[2]
C2M2	cybersecurity capability maturity model[3]
CD	compact disc
CDA	critical digital asset
CSF	cybersecurity framework[4]
CIS	center for Internet security
CMMI	capability maturity model integration
CMMI-SVC	CMMI for services
CONOPS	concept of operations
COTS	commercial-off-the-shelf
DA	digital asset
DES	data encryption standard
DHCP	dynamic host configuration protocol
DMZ	demilitarized zone
DOD	Department of Defense[5]
DOE	Department of Energy[5]
DoS	denial of service
DRP	disaster recovery plan
DVD	digital versatile disc
EAP	Extensible Authentication Protocol[2]
GPS	global positioning system
HMI	human-machine interface
HSE	health, safety and environment
IACS	industrial automation and control system(s)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIS	Internet information services[6]

---

2 IETF

3 US DOE

4 NIST

5 US

6 Microsoft®. This trade name is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC.

IP	Internet protocol
ISA	International Society of Automation
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
MFA	multifactor authentication
ML	maturity level
NIST	National Institute of Standards and Technology[5]
NTP	network time protocol
OPC	open platform communications
OS	operating system
PII	personally identifiable information
PIN	personal identification number
PLC	programmable logic controller
RBAC	role-based access control
RF	radio frequency
RFC	request for comment[2]
RFQ	request for quote
RTU	remote terminal unit
SI	international system of units
SL	security level
SL-T	target SL
SP	security program
SPE	SP elements
SPR	security protection rating
SPS	security protection scheme
SSID	service set identifier
TCP	transmission control protocol
UAC	user account control[6]
UDP	user datagram protocol
USB	universal serial bus
VPN	virtual private network

3.3 Conventions

A requirement without qualifier is the same as that requirement with a BR (Basic Requirement) qualifier; for example, ORG 1.1 and ORG 1.1 BR are the same requirement.

A requirement with a leading 0 in its numerical fields is the same as that requirement without a leading 0 in its numerical fields; for example, SR 2.03 and SR 2.3 are the same requirement.

The above conventions accommodate the different ways the requirements are specified in other IEC 62443 parts.

The term "Automation Solution" is used as a proper noun (and therefore capitalized) in this document to prevent confusion with other uses of this term.

4 Concepts

4.1 Use of this document

4.1.1 Applicable roles

This document primarily applies to the asset owner role, and to a lesser degree, to service provider and product supplier roles (see Figure 1). Organizations who are accountable for the IACS are considered asset owners by the IEC 62443 series. Organizations responsible for the development and support of the hardware and software used in IACS fulfil the product supplier role. Organizations that provide integration services for the IACS fulfil the integration service provider role, while those that provide maintenance services fulfil the maintenance service provider role. These roles and responsibilities are depicted in Figure 1.

It is not uncommon for the organization acting as the asset owner to perform some or all aspects of the integration or maintenance service provider roles, and also perform some or all aspects of the product supplier role for some components of the IACS. In these cases, Subclauses 4.1.2 and 4.1.3 will apply to the asset owner organization.

In other cases, the asset owner may contract with one or more product suppliers and/or service providers to deploy and maintain the IACS. In these cases, these organizations may act as one or more of the integration service providers, maintenance service provider or product supplier roles.

Similarly, part or all of a facility may be operated by an entity other than the asset owner. In all cases, the requirements specified by this document apply to the asset owner. The asset owner may have a supply chain program that contains security requirements derived from this document for product suppliers and service providers.

4.1.2 Use of this document by asset owners

4.1.2.1 Risk mitigation

This document defines requirements for IACS SPs of asset owners. In general, a SP consists of defining, implementing and maintaining process, personnel and technology-based capabilities that are intended to reduce the cybersecurity risk of an IACS.

The primary purpose for each of the SP requirements in this document is to mitigate risk. However, risk reduction can take many forms, such as reduction of the likelihood of an incident, reduction of the impact of an incident, reducing the timeline to recover from an incident, and others. In many cases, an SP requirement reduces the overall risk in multiple ways.

The requirements are specified in an implementation independent manner, allowing a variety of implementations, and allowing users of this document to select a combination of architectural approaches (for example, the use of security zones), policies, procedures and technologies that are most appropriate for their applications.

IEC 62443-3-2 [1], describes a methodology for addressing cybersecurity risks in an IACS Automation Solution design, including the use of security levels (SLs) and security zones.

An IACS SP is typically specific to an individual IACS, of which the facility can have more than one. When there is more than one, it is recommended that a single high-level, facility-level SP be defined whose requirements cascade down as needed to individual IACS SPs. Each IACS SP is dedicated to the availability, integrity and confidentiality of the specific production resources of its IACS, including controllers, field devices and other embedded devices, as well as protecting trade secrets and other confidential information of the IACS.

An IACS SP should be compatible with other IACS SPs at the facility, but this is not always practical or achievable since the technology and risks associated with one IACS can be significantly different than those of another IACS.

IACS SPs are also expected to supplement an asset owner organization's information security management system (ISMS) to provide coordinated operational and information security for the site. ISMS requirements generally do not specifically address all of the security and operational needs of an IACS. This document, along with related parts of IEC 62443 series, define the requirements needed to ensure the operational and informational security of an IACS throughout its lifecycle.

Where practical, IACS SPs should be compatible with the organization's ISMS, but complete consistency with the ISMS is typically not possible due to conflicting objectives of information technology (IT) and IACS systems, and in particular, the essential constraints associated with availability and performance of production facilities. In addition, some of the informational security requirements that apply to protection of the IACS IT aspects can be implemented differently for the IT system and an IACS.

NOTE Alignment of the ISMSs and IACS SPs can be improved by alignment of security goals and objectives between the two systems, and by formally documenting their similarities and differences.

For example, patching policies can be different between IACS SPs and ISMSs as a result of the differences in availability requirements between IACS operator stations and ISMS desktop workstations. Operational constraints, such as this, will typically result in different sets of policies and procedures for IACS SPs and ISMSs.

Since IACSs are a combination of personnel, hardware and software, and processes, SPs of asset owners compliant with this document are composed of:

a) organizational capabilities that:
   1) include an ISMS that typically defines organization-wide policies and practices for IT systems, and
   2) support coordination between the IACS and the IT infrastructure in its environment,
b) technical security capabilities implemented in hardware and software components of the Automation Solution of the IACS (see Figure 1), and
c) security-related processes, used to securely deploy, configure and operate the IACS, and to maintain its technical security capabilities.

4.1.2.2 SP implementation

This document provides IACS asset owners with a framework to develop and evolve their SPs. Implementing an effective SP for an IACS involves defining and executing comprehensive capabilities that:

a) address all aspects of security risk management, from identification of programmatic objectives to day-to-day operation, and
b) include ongoing auditing for program compliance and improvement.

Organizational commitment from top to bottom is essential for IACS SP success. Security of an IACS is a responsibility shared by all members of the organization and their contractors/consultants, and integration of security into their daily activities allows the organization to function more smoothly and succeed in protecting the IACS. SPs based on this document are expected to vary widely depending upon the asset owner's organization and industry. Application of this document to an asset owner's SP begins with determining which of the requirements defined in this document are applicable. Requirements are often determined to be applicable based on the architecture and characteristics of the IACS, the environment in which the IACS operates and the security risks associated with it (see Annex B and IEC 62443-3-2 for more information on management of IACS security risks).

For each applicable requirement, asset owners should implement the appropriate combination of technical and process-oriented capabilities. Technical capabilities are features of the IACS and its components, and process-oriented capabilities are organizational processes used to integrate/deploy the IACS, operate it and maintain it.

Cross-references are provided to IEC 62443-3-3 and IEC 62443-4-2 for technical capabilities and to IEC 62443-2-4 for integration and maintenance capabilities. These cross-referenced capabilities can be used by asset owners when determining the technical and process-oriented capabilities they will implement and for specifying security requirements for their product suppliers and service providers.

It could be impossible or impractical for an asset owner to establish and implement a SP that meets all applicable requirements at once. Therefore, asset owners may, if necessary, develop a phased approach to evolve their SP. In such cases, the initial emphasis should be on effectively managing the highest risks.

This document also recognizes that it can be desirable for asset owners to implement a SP that meets the requirements specified in this document in ways that are consistent with other security specifications. Therefore, Annex A reports cross-references to and from each requirement of this document with requirements in related external references, in particular with ISO/IEC 27001 [8] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [9]. Using these cross-references, the asset owner can harmonize with related external requirements when implementing each of its SP capabilities.

NOTE In the context of an IACS, all references in ISO/IEC 27001 to "information management" refer to the IACS.

Some legacy IACS can preclude direct implementation of specific requirements or subsets of applicable requirements. In these instances, compensating security measures should be implemented where possible.

4.1.2.3 Organizational interfaces

Although the asset owner is ultimately accountable for the operation of the IACS and processes controlled by the IACS, associated responsibilities are often fulfilled with the support of service providers and product suppliers. The respective legal, operational and technical roles and responsibilities for these entities are generally defined in contracts and procurement documents, such as request for quotes (RFQs) and purchase orders. Ideally, security requirements are included in these documents.

When the service provider or product supplier is part of the asset owner's organization, there might not be such a contract, but the security requirements for products and integration/maintenance processes are typically still specified for the IACS.

This document provides in Annex A cross-references to and from each requirement of this document with service provider and product supplier requirements specified in IEC 62443-2-4, IEC 62443-3-3 and IEC 62443-4-2. Asset owners can use these cross-references to assist in the development of security requirements for service provider and product supplier procurement documents. These referenced documents and the requirements cross-references included in Annex A of this document can assist asset owners, service providers and product suppliers to agree on a consistent set of requirements during procurement.

4.1.3 Use of this document by service providers and product suppliers

As described in 4.1.2.3, IEC 62443-2-4, IEC 62443-3-3 and IEC 62443-4-2 define security requirements for products and services procured by asset owners. Since these requirements are cross-referenced to this document's requirements in Annex A, this document can provide a useful context to service providers and product suppliers.

4.2 Maturity level (ML) definitions

The SP requirements defined in this document beginning in 5.3 have been specified to be implementation independent. This is done to allow the asset owner latitude in applying this document while meeting the needs of its organization.

To support implementation independence for process security measures that meet these requirements, a range of MLs from entry level processes to refined and improved processes is defined in Table 1. MLs apply independently to SP requirements, and the asset owner should select the most appropriate ML for a requirement based on risk management goals (see IEC 62443-3-2). While the asset owner can have policies and procedures that satisfy multiple SP requirements, each SP requirement should be evaluated independently. See Annex C for more information about evaluating MLs.

Additionally, since some asset owners could need to use a phased approach to evolve their SPs, a range of program MLs can prove helpful in the planning and scheduling of phases. Note that other parts of IEC 62443 that define requirements for process security measures, such as IEC 62443-2-4 and IEC 62443-4-1 [10], also incorporate ML.

This document's range of MLs is defined by a model that is composed of maturity benchmarks for implementation of process security measures. The benchmarks for each ML are shown in Table 1. The MLs are based on the Capability Maturity Model Integration (CMMI) for Services (CMMI-SVC) model [11]. Table 1 shows the relationship to the CMMI-SVC in the "Description/comparison to CMMI-SVC" column.

Table 1 – ML levels and descriptions

Level	CMMI-SVC	This document	Description/comparison to CMMI-SVC
1	Initial	Initial	At this level, the models are fundamentally the same. Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time can be difficult to show. NOTE "Documented" in this context refers to the procedure followed in performing this service (for example, detailed instructions to service provider personnel), not to the results of performing the process. In most IACS, changes resulting from the performance of a procedural process are often documented.
2	Managed	Managed	At this level, the models are fundamentally the same, with the exception that this document recognizes that there can be a significant delay between defining a process and executing/practicing it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, documentation exists that describes how to manage the delivery and performance of the capability. This documentation can be in the form of written procedures or written training programs for performing the capability. The discipline reflected by ML 2 helps to ensure that practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined	Defined / Practiced	At this level, the models are fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a process at Level 3 is a Level 2 process that is being practiced on the IACS. The performance of a Level 3 practice can be shown to be repeatable over time within the IACS.

Level	CMMI-SVC	This document	Description/comparison to CMMI-SVC
4	Quantitatively Managed	Improving	At this level, the "Quantitatively Managed" and "Optimizing" CMMI-SVC levels are combined. Using suitable process metrics, the effectiveness or performance improvements of the process or both can be demonstrated. This results in a SP that improves the process through technological/procedural/management changes.
	Optimizing		

Beginning with ML 2, processes are required to be documented. This includes documented policies and procedures as well as documented training for personnel. As a consequence, the SP requirements specified in this document do not state the need for documentation because the ML 2 and above require documentation.

Within this maturity model, each level is progressively more advanced than the previous level and applies independently for each requirement. MLs are a part of the conformance assessment process, so asset owners are required to identify whether they meet each requirement, and if so, the ML associated with their implementation of each requirement or group of requirements.

NOTE It is intended for evolution of a SP, that over time and for a specific requirement, a process will evolve to higher levels as the organization gains proficiency in meeting the requirement.

4.3 Security levels (SLs)

SLs for IACS represent the relative strength of security capabilities defined for the IACS Automation Solution in IEC 62443-3-3 and for components in IEC 62443-4-2.

This document does not describe the methodologies for defining zones and conduits, or determining SLs for zones, conduits and components. Instead, those methodologies are defined in IEC 62443-3-2 for zones and conduits, and IEC 62443-4-2 for components. This document defines the requirements for the overall SP within the organization to manage risk on an ongoing basis, via implementing and maintaining process, personnel and technology-based capabilities.

To correlate SP requirements in this document with target SLs (SL-Ts) for zones, conduits and components, the asset owner can use the cross-references to IEC 62443-3-3 and IEC 62443-4-2 that are provided with the SP requirement to understand the requirements/requirements enhancements associated with the SL-T from those documents.

For example, this document can state a SP should have a process to ensure proper authentication is ensured across the organization. However, to address confidence in the implementation of user authentication capabilities, the asset owner should request its product suppliers to show the product in question was developed using IEC 62443-4-1 compliant processes, and the product capabilities are compliant with relevant IEC 62443-4-2 requirements. Similarly, to address confidence in the installation, configuration and maintenance of these user authentication capabilities, the asset owner would request its service providers to use processes for these capabilities that are compliant to the cross-referenced IEC 62443-2-4 requirement, SP.03.07 RE(1).

4.4 Requirements definitions

4.4.1 Requirements organization

Subclause 5.3 and Clauses 6 through 13 define the selection methodology and individual requirements for asset owner SPs. These requirements have been specified to be implementation independent, allowing the asset owner to select the most suitable implementation for its IACS.

Requirements are organized into SPEs that represent top level activities of the SP, such as organizational security measures, configuration management, network and communications security and component security. SPEs are composed of requirements for a combination of organizational and technical security controls that can be used to implement a defense-in-depth strategy for the IACS.

4.4.2 Requirements cross-references

To aid the asset owner's use of this document, the requirements have been cross-referenced to other parts of the IEC 62443 series and other security specifications that include system and component requirements. This cross-reference is provided to support activities spanning documents in the series, such as the integration of the asset owner's SP with its ISMS and with its supply chain processes as they relate to security.

These cross-references support asset owner efforts to implement the requirements of this document consistently with the other parts of the IEC 62443 series and with the other referenced specifications. Blank entries in these cross-references mean that there is no corresponding requirement in the cross-referenced document. These cross-references are reported in Annex A.

4.4.3 Requirement conventions

Some of the requirement's definitions contain the phrase: "commonly accepted". This phrase is used when the required capability implementation is dependent on the current state of the art, and the state of the art at the time of conformance assessment is used to determine whether the requirement has been met. For example, when the Data Encryption Standard (DES) was developed, it had no known vulnerabilities, but since then vulnerabilities have been discovered and it is no longer appropriate for use in IACSs. The "Rationale and supplemental guidance" subclause of each requirement provides additional explanation of the use of this phrase.

5 Conformance and assessment

5.1 Overview

The formal definitions for terms like conformance, conformity and assessment come from other sources, such as ISO/IEC 17000 [12]. IEC 62443 series provides guidance for conformity and assessments for various roles (see 4.1.1). This guidance is intended to assist the various roles in understanding the conformance and assessment process and is not intended to supersede any of the definitions provided in ISO/IEC 17000.

Conformance or conformity with IEC 62443 series means the affected role has evaluated, and where applicable applied and documented, all methods identified in each requirement of the applicable series part thereby mitigating security risks and identifying the conformity for all identified processes with the necessary supporting evidence.

Assessment means the affected role has performed specific measurement of conformity with the requirements through use of some type of verification process or specific validation process. Those validated processes can be applied through an internal organization process or the use of a third-party identified process compliant with the IEC 62443 series, and also are verified by supplying the necessary supporting evidence.

Conformity assessments can be self-assessments performed by the asset owner, service provider or product supplier roles using internal processes, or assessments can be performed by a qualified, independent third-party. When independent third-party assessments are used, it is important to note that credentialling processes of the third-party are wide and varied and are outside the scope of this document,

Assessment processes themselves are also outside the scope of this document.

Asset owners may have their "as-deployed" control systems, IACS or Automation Solutions assessed for conformance to IEC 62443-3-3 and their "as-provided" integration and maintenance services assessed for conformance to IEC 62443-2-4. These assessments would verify conformance at the time the control system was assessed, or the services were provided. Supplementing these assessments are evaluations that combine security levels and organizational MLs to indicate the composite SP protection provided to the IACS.

Asset owners may assess their IACS and Automation Solutions for conformance to this document, to verify they have a SP in place to sustain a security posture for the IACS which includes all technical components and organizational processes. It is also desirable for the IACS or Automation Solution to use security certified products in the design that are correctly deployed and maintained by certified service providers.

Product suppliers providing products to an asset owner may have their products and development processes assessed for conformance to IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4-2.

Service providers providing services to an asset owner may have their integration and maintenance services assessed for conformance to IEC 62443-2-4.

5.2 Conformity evidence

Proof of conformity and conformance methods can be provided in many forms as shown in Table 2. Most requirements identify supporting evidence by identifying the specific methods that include, but are not limited to:

- verifying the use,
- capability and configuration of technology,
- their supporting processes, and
- validation through testing of capabilities.

Table 2 – Typical conformity evidence types

Evidence type	Description
Configuration records	Records that show configuration settings, component inventories, patch records, etc.
Legal documents	Contracts and related documents, including subcontractor agreements, signed employee statements, background checks, asset owner approvals, etc.
Organization charts, position descriptions and personnel records	Job related documentation that describes customer roles, including personnel requirements (for example, expertise/experience), job responsibilities and organizational relationships. Also, records that show who was assigned/de-assigned to these positions (for example, to Automation Solution activities).
Product documentation	Internal and external documents that describe the product, such as design documents, product data sheets, knowledge-based articles and network scanning tools.
Screen shots	Screen captures of user interfaces.
Security assessments	Reports that document security-related issues, such as risks, security incidents and vulnerabilities.
Security testing documentation	Internal and external documents that describe the security tests/results used to verify security aspects of the product or installation of the product.
Service policies and procedures	Internal customer documentation that describes policies and procedures used by customer personnel to install, configure, harden and maintain the Automation Solution.
Security-related activity documentation/checklists	Documentation, such as checklists, that records the results of security-related activities, such as risk assessments, threat models, reviews, architecture drawings, test results, spreadsheets, etc.
Automated reports	Reports generated by the IACS.

Evidence type	Description
Training materials/course descriptions	Documents that describe how training is conducted and documents that show the content of the training course, such as a syllabus or course overview.
Training records	Documents that show completion of training. These documents typically show who was trained, when they were trained and the course names. These can take the form of course rosters, course diplomas, human resource records, etc.
User documentation	User manuals, instructions, etc. that describe to the user how to configure, operate, maintain or otherwise interact with the IACS and its products and services.
Testing results	Any and all tests, performed by a qualified person having the appropriate training, on a documented configuration of components, IACS and Automation Solution that verify specifically identified requirements conformance.

5.3 Requirements evaluation and profiles

5.3.1 Overview

In preparation for a conformance assessment, asset owners need to evaluate each requirement in an applicable part of the series for its guidance in mitigating the risk addressed by the requirement.

In the event a role determines through evaluation any requirement may not apply, it is the asset owner's responsibility to justify why a requirement does not apply and provide supporting evidence stating specifically why the requirement does not apply including specifically how that security risk has been otherwise mitigated through other security measures.

5.3.2 Evaluation of risk to requirements

The determination of the cybersecurity risks to be mitigated (see 4.1.2.1 and 6.3.1, ORG 2.1: Security risk mitigation) is typically performed as part of the asset owner's risk management process in IEC 62443-3-2. This process should incorporate "risk response" activities as described in IEC TS 62443-1-1 and IEC 62443-3-2, which are responsible for identifying and dispositioning risks. Completing the risk management process in IEC 62443-3-2 is critical to the security of the IACS even if a conformance assessment is not performed.

Requirements then are applied based on risk mitigation and apply to all circumstances where identified risks need to be mitigated to a tolerable level, and conversely, if requirements may not apply where risks have evidence to prove the risk can be at a tolerable level.

Each requirement is selected based on risk mitigation and interpreted in the context of tolerable risk; that is, meeting the requirement means that the asset owner has either mitigated or accepted the risks associated with the requirement with supporting evidence.

If the asset owner is not prepared to accept the risks, then the requirement is not met.

5.3.3 Profiles

It can be necessary for some industries and verticals to align the requirements in this and other IEC 62443 documents to industry/vertical-specific concepts and terminology. In order to provide additional flexibility in the application of the standards series, IEC TS 62443-1-5 [13] describes a method for one or more organizations to create a common profile of IEC 62443 (all parts). A profile allows an interested party (organization, group, sector, conformity assessment body, etc.) to select a subset of requirements from one or more standards in IEC 62443 (all parts), provide a contextual mapping for those requirements (for example to an industry/vertical) and specify a minimum security or maturity level for selected requirements.

Published profiles can be used as a common basis of assessment against a subset or industry/vertical-specific mapping of the requirements in the IEC 62443 series. They support interested parties during conformity assessment activities, to achieve comparability of assessed IEC 62443 requirements.

5.3.4 Conformity assessment for the asset owner role

In preparation for a conformity assessment, asset owners can select the requirements that are to be assessed based on:

a) a security profile to which the asset owner claims conformance; or

b) the outcome of an IACS specific cyber security risk assessment and identification of applicable requirements necessary to reduce risks to a tolerable level.

A requirement might not be applicable because, for example, the IACS does not contain components/technology, such as wireless and safety systems addressed by the requirement.

Risk management is critical to the security of the IACS even if a conformity assessment is not performed.

6 SPE 1 – Organizational security measures

6.1 Purpose

The requirements in this SPE are defined to ensure that the organization is prepared to adequately address IACS security. It focuses on organizational policies and procedures for applying security practices and ensuring that its personnel are security aware and trained for their security responsibilities.

6.2 ORG 1 – Security related organization and policies

6.2.1 ORG 1.1: Information security management system (ISMS)

6.2.1.1 Requirement

If the asset owner has an ISMS, the asset owner shall coordinate the IACS SP with the ISMS. If the asset owner does not have an ISMS, the asset owner shall incorporate the appropriate management processes into the IACS SP.

6.2.1.2 Rationale and supplemental guidance

A formal ISMS is often employed by the asset owner organization to protect its IT system. When employed, the ISMS and the IACS SP should be coordinated to provide an integrated defense-in-depth strategy for the IACS, thereby avoiding duplication of effort and providing an efficient security interface between IT and IACS.

Requirements and recommendations for a formal ISMS can be found in ISO/IEC 27001 [8], ISO/IEC 27002 [14], the NIST CSF [9], NIST SP 800-53 [15], NIST SP 800-82 [16] as well as others. ISMS requirements and recommendations that are applicable to an IACS should be selected based on risk mitigation (see 4.1.2.1), and their implementation should be synchronized, to the greatest degree possible, with the ISMS to minimize differences and discord between the two.

Coordination between the IACS SP and the ISMS involves cooperation between security administrators, design and management of shared IACS network interfaces (for example, firewalls, demilitarized zones (DMZs) and remote access) and management of user access across those interfaces. The formal ISMS can be implemented for IT systems of the organization or for the IACS itself.

Areas of potential conflicts should be identified, examined and addressed, such as policies and practices for patch management (see also IEC TR 62443-2-3 [17]) and anti-malware updates, to prevent them from interfering with each other or opening vulnerabilities between the IACS and facility systems.

6.2.2 ORG 1.2: Background checks

6.2.2.1 Requirement

The asset owner shall have policies and procedures about performing background checks on all personnel who require access to the IACS (including employees, contractors, subcontractors, consultants, product suppliers and service providers) prior to granting them access to the IACS. Where feasible and allowed by applicable law, such background checks shall include identity verification and criminal records checks.

6.2.2.2 Rationale and supplemental guidance

Background checks are used to protect the IACS from being staffed with personnel whose integrity and trustworthiness can be questionable, including, but is not limited to, employees, contractors, subcontractors, consultants, products suppliers and service providers.

While the background check cannot guarantee these qualities, it can identify personnel who have had trouble with them. Examples of background checks include identity verification and criminal record checks.

This requirement recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities, service organizations or both. Some countries prohibit background checks; while other countries do not. Of those that allow them, some provide no support for conducting them, making it infeasible or impractical for background checks to be performed.

When background checks are possible, the asset owner should have a policy for how and how often they are performed.

6.2.3 ORG 1.3: Security roles and responsibilities

6.2.3.1 Requirement

The asset owner shall have policies and procedures around defining and assigning security roles and responsibilities to qualified personnel, including employees, contractors, subcontractors and consultants.

6.2.3.2 Rationale and supplemental guidance

Security roles, such as security administrators, security leads and security contact points, are necessary to establish/maintain the security of the IACS. Further, the personnel in those roles need to be qualified to perform their security-related tasks to ensure that they are performed appropriately. The asset owner needs to define qualification requirements, which typically consist of varying levels of education, experience and training. Some things, like facility-specific technical training, are often provided by the asset owner and are not usually included in prior experience requirements.

The organization should determine the organizational processes required to establish/maintain the security of the IACS and identify the personnel who will be responsible for managing and implementing these processes. They should also determine a base level of expertise necessary to perform these tasks, and ensure the identified personnel have this expertise. Expertise can be demonstrated through related experience, training or both.

6.2.4 ORG 1.4: Security awareness training

6.2.4.1 Requirement

The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity awareness training that is updated on a regular basis.

6.2.4.2 Rationale and supplemental guidance

Security awareness training is necessary to ensure personnel who have physical contact with or access to the IACS understand that their behaviour has the potential for impacting the security of the IACS. Maintaining security awareness is instrumental in establishing an organizational culture that recognizes that its personnel play an important role in the security of the IACS.

Physical contact with the IACS includes contact with IACS components (for example, displays and embedded devices), communications media, portable media, cabinets and all other equipment whose compromise can impact the IACS. Access to the IACS includes user interfaces, communications interfaces and local device interfaces through which access to the IACS can be gained.

Security awareness training is used to inform personnel of basic security principles that they are to apply to their daily behaviour. This training should be customized or related to the specific security policies and requirements of the IACS. Sources of these policies and requirements include this document and other parts of the IEC 62443 series that are applicable to the IACS. The asset owner should also have a policy that specifies how often its security awareness training program is to be reviewed to keep it current and relevant.

Regular review and update of training content and plans is necessary to respond to changes to the threat landscape, the vulnerability landscape and technology associated with the IACS.

6.2.5 ORG 1.5: Security responsibilities training

6.2.5.1 Requirement

The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity training that is relevant to their IACS cybersecurity responsibilities. Such training shall either be accepted or provided by the asset owner.

6.2.5.2 Rationale and supplemental guidance

Security responsibility training serves two purposes:

a) to ensure that personnel who are responsible for some aspect of the cybersecurity of the IACS understand what their responsibilities are and how their performance will be measured, and

b) to ensure that they understand the processes and procedures necessary to meet those responsibilities.

NOTE Personnel to receive security training include, but are not limited to employees, contractors, subcontractors, consultants, product suppliers and service providers.

Security responsibility training will typically be provided to personnel on a recurring basis that includes the security objectives to be met along with related job performance criteria. It is important that each person understands what is expected in the meeting of his/her security responsibilities.

Security responsibility training should also describe how to meet security responsibilities. These descriptions can include classroom/online instructions, references to manuals or written policies and procedures. When training is completed, an individual should clearly understand his/her objectives and how their job performance will be evaluated with respect to his/her security responsibilities.

6.2.6 ORG 1.6: Supply chain security

6.2.6.1 Requirement

The asset owner shall have policies and procedures that specify requirements for suppliers of products and services addressing cybersecurity risks to the IACS. The asset owner policies and procedures shall consider recursive requirements on the suppliers, where feasible.

6.2.6.2 Rationale and supplemental guidance

IACSs are typically composed of products and services integrated and tested to work together. Each of these products and services is provided to the asset owner by an organization (which can include the asset owner) that is generally referred to as a supplier. Each supplier often has suppliers of its own, and each of these second level suppliers can have suppliers of their own. This cascading of suppliers is referred to as the supply chain.

To construct an effective supply chain process, the asset owner should identify each technical and process security measure incorporated into the IACS, and then define appropriate security requirements for those that are directly or indirectly provided by product suppliers or service providers. The objective is for products to have appropriate security measures built into them and for services to include appropriate security processes.

For a product or service to meet IACS security requirements, the supplier is responsible for ensuring that components and services of the product or service are themselves assessed for risk in the context of their use and should have security requirements specified for them. This process of risk determination and security requirement definition should occur recursively along the supply chain, thus creating a formal process for addressing security in the supply chain.

6.3 ORG 2 – Security assessments and reviews

6.3.1 ORG 2.1: Security risk mitigation

6.3.1.1 Requirement

The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing IACS cybersecurity risks, including determining a tolerable risk level and responding to risks outside that tolerable risk level.

6.3.1.2 Rationale and supplemental guidance

Security risks represent the potential for loss as a result of a security compromise. The higher the risk, the greater the potential for loss. Risk management involves understanding the IACS operational environment, identifying, assessing and quantifying risks within this environment, determining which risks cannot be tolerated by the organization and mitigating them to reduce their level of risk to a tolerable level. Risks that have been mitigated to a tolerable level means that the organization is willing to "live with" or is prepared to manage the mitigated risk. See IEC 62443-3-2 for more information about risk assessments and risk tolerance. See IEC 62443-3-3 for more information about applying technical security measures to mitigate the risks outside the tolerable risk level.

Risk mitigation involves developing attack scenarios, assessing and ranking associated potential consequences and implementing security measures in response to risks that are deemed intolerable. Security measures typically include a combination of architectural, technical mechanisms, vulnerability closures and process security measures. Risk mitigation also includes activities to ensure that risks are maintained at a tolerable level, such as periodic or event-driven (for example, changes in the threat landscape and discovery of new vulnerabilities) reassessments, internal or external audits that ensure technical and process security measures are in place and applied appropriately and conformity certifications to applicable cybersecurity standards.

The requirements in this document describe capabilities that, when appropriately implemented, provide security measures for the IACS. The asset owner should select requirements from this document that are applicable for the IACS and implement them accordingly. For those requirements not selected, the asset owner should document why they are not applicable or were not selected. For example, they do not address a security risk or the risk that they address is tolerable without mitigation. When documenting the risks, desired capabilities, requirements (both selected and not) and security measures, it is preferable to collect these in a document sometimes called a security protection scheme (SPS) or concept of operations (CONOPS). The SPS should include both technical and process security measures and should discuss how each of the principal roles are involved with the IACS.

Developing attack scenarios typically involves identifying threats and known vulnerabilities that are applicable to the system. Known vulnerabilities are those that have been discovered and, in many cases, reported within the industry. Known vulnerabilities are often related to OS, open-source software and control system software; however, they can be associated with any element of the IACS. See 12.2.9, EVENT 1.9: Vulnerability handling, for more information about addressing newly discovered vulnerabilities.

6.3.2 ORG 2.2: Processes for discovery of security anomalies

6.3.2.1 Requirement

The asset owner shall have policies and procedures related to periodically discovering and addressing, through manual or automated processes:

a) undocumented and unauthorized components/software connected to or communicating within the IACS,

b) undocumented and/or unauthorized network traffic,

c) new and/or known but undocumented vulnerabilities in the IACS, and

d) other security anomalies and non-conformities.

6.3.2.2 Rationale and supplemental guidance

Security anomalies, non-conformities and undocumented/unauthorized components, software and network traffic represent potential threats to the IACS and new or known but undocumented vulnerabilities provide potential entry points to attackers.

Discovering and assessing their potential impact to the IACS is a necessary part of risk management. Using manual processes or automated tools on a regular basis limits the exposure to these threats and exploitation of vulnerabilities, allowing them to be detected and subsequently addressed.

For example, the network should be regularly probed or examined to discover unauthorized components and network accessible services. Other processes/tools should then be used to identify the software that is associated with these transmission control protocol (TCP) / internet protocol (IP) ports.

Care should be taken when using automated tools to ensure that they do not hinder or impact the operation, performance and availability of the IACS.

6.3.3 ORG 2.3: Secure development and support

6.3.3.1 Requirement

The asset owner shall have policies and procedures addressing the use of a secure development lifecycle process for the development and support of systems and components used in the IACS.

6.3.3.2 Rationale and supplemental guidance

Secure development and testing of systems and components prior to incorporating them into the IACS provides assurance that they will not allow the compromise of the integrity or availability of the IACS, or the disclosure of IACS confidential data. Secure support processes ensure that the security of systems and components is maintained throughout their lifecycle. See IEC 62443-4-1 for secure product development and support requirements.

Requiring secure development and support processes for systems and components for an IACS ensures that system and component security will be developed and tested prior to inclusion in the operational IACS, supported once operational, and managed throughout all phases of the lifecycle, including decommissioning at end-of-life and/or operational use.

6.3.4 ORG 2.4: SP reviews

6.3.4.1 Requirement

The asset owner shall have policies and procedures related to periodically reviewing the SP to:

a) verify that it is being properly applied,

b) validate that the technical and process security measures continue to meet the system security requirements,

c) address changes in the organization and its processes, technical changes in the Automation Solution and changes in the threat environment, and

d) make improvements, as appropriate.

6.3.4.2 Rationale and supplemental guidance

Regular assessments are used to verify compliance to the SP, validate that the SP meets the desired system security requirements and ensure that changes to the organization, its policies, the Automation Solution and threats to the IACS are being addressed by the SP. Such assessments are typically used to evolve the SP in terms of the requirements it meets and the ML at which they are met.

It is not uncommon for an asset owner to develop a long-term plan, referred to as a road map, for implementing requirements over a period of time. Regular assessments can then be used to monitor:

- the road map and adjust it as necessary, and
- its progress.

6.4 ORG 3 – Security of physical access

6.4.1 ORG 3.1: Physical access control

6.4.1.1 Requirement

The asset owner shall have policies and procedures around physical access to the IACS, including access to facilities, equipment and cabling, so that the physical access is controlled to meet risk targets.

6.4.1.2 Rationale and supplemental guidance

Physical access controls protect the IACS from personnel and equipment gaining unwanted physical proximity to the IACS. Physical proximity can allow connection of wired or wireless equipment to the IACS and use of IACS resources, such as workstations or surveillance (for example, cameras). In general, organizations will restrict physical access to systems, structures and components associated with the IACS, and permit access to only authorized personnel, including employees, contractors, consultants, product suppliers and service providers.

A variety of mechanisms can be used to provide physical access controls such as fences, guards, badges, locked doors, cameras and conduits for wiring.

7 SPE 2 – Configuration management

7.1 Purpose

The requirements in this SPE are defined to ensure that the asset owner documents the IACS architecture, maintains an inventory of its hardware and software components and controls changes to them.

7.2 CM 1 – Inventory management of IACS hardware/software components and network communications

7.2.1 CM 1.1: Asset inventory baseline

7.2.1.1 Requirement

The asset owner shall have policies and procedures to document, verify and maintain, throughout the full life cycle of the IACS, the inventory baseline of all devices, hardware components, software components, communications protocols and open communications ports used in the IACS including but not limited to:

a) organizational responsibilities,
b) manufacturer,
c) model,
d) version numbers,
e) serial numbers,
f) network interfaces,
g) communication addresses,
h) revision/patch levels, and
i) history.

7.2.1.2 Rationale and supplemental guidance

Having and maintaining a verified inventory baseline is necessary to validate that all devices, hardware components, software components and communications protocols/ports/endpoints are known to the asset owner, and consequently authorized and configured to meet security requirements. Maintaining the IACS inventory baseline confirms that the current implementation of the system matches the approved design. The inventory baseline should reflect the implemented system through all of the IACS life cycle phases, including design, specification, implementation, verification and validation, operations, maintenance and decommissioning.

In order to identify and manage supply chain cybersecurity risks, the inventory baseline should account for third-party assets that are part of the IACS.

Having and maintaining an inventory baseline also provides the ability for the asset owner to review the properties of components and communications paths. This helps establish the basis for managing changes to components and communications paths, including additions, deletions and updates.

Configuration baselines are normally maintained in a database that contains component and protocol properties. These properties should include information that identifies and describes the component/protocol, and its use, current state and history.

7.2.2 CM 1.2: Infrastructure drawings/documentation

7.2.2.1 Requirement

The asset owner shall have policies and procedures to verify and maintain the current baseline of drawings/documentation showing the physical and logical connectivity of all IACS devices and software components.

7.2.2.2 Rationale and supplemental guidance

Having and maintaining verified architecture drawings and descriptions provides the basis for conducting security assessments, including the identification of trust boundaries. Verifying that the drawings match the implementation is necessary to verify that unauthorized devices are not connected to the system.

Configuration baselines as described in 7.2.1, CM 1.1: Asset inventory baseline, should be supplemented by architecture drawings and descriptions. Architectural relationships should include network connectivity, communications protocols/ports and data/control flows between components.

Infrastructure drawings and documentation should be classified and protected in accordance with 10.2.1, DATA 1.1: Data classification, and 10.2.2, DATA 1.2: Data confidentiality.

Examples of documentation often used include line drawings, functional drawings, elevations and rack layouts, room layouts, security perimeter drawings (electronic and physical) and communication path protocol and endpoint information.

7.2.3 CM 1.3: Configuration settings

7.2.3.1 Requirement

The asset owner shall have policies and procedures to document the configuration settings of all IACS devices and software applications and to verify their operational compliance with the documented configuration.

7.2.3.2 Rationale and supplemental guidance

The configuration of IACS components will often change during the life cycle of the system to meet the goals and objectives of its operation through different stages including installation, deployment, maintenance, repair, and upgrades. Documenting approved configuration settings and having a means of verifying that they are applied or written correctly to components is essential to the security and operation of the system.

It is important to have accurate records of the IACS configurations to assure that a system performs as intended and that it is identified and documented in sufficient detail to support its projected life cycle.

7.2.4 CM 1.4: Change control

7.2.4.1 Requirement

The asset owner shall have policies and procedures to authorize, validate and approve changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels.

7.2.4.2 Rationale and supplemental guidance

Validating the implemented system against the configuration baseline and controlling changes are primary mechanisms for protecting against the unauthorized addition or removal of hardware, software and communications to the IACS, including substitutions, software updates and the addition of communications paths.

When combined with 7.2.1, CM 1.1: Asset inventory baseline, 7.2.2, CM 1.2: Infrastructure drawings/documentation and 7.2.3, CM 1.3: Configuration settings, asset owners are able to support forensics by inspecting components/communications and determining when they were added to the system, when they were updated, who authorized the updates and who performed the updates.

A formal process for documenting, submitting and approving change requests is necessary. This process should identify the organization roles and personnel who are responsible for these activities.

In addition, a good practice to follow is "separation of duty", in which the people implementing the change, validating the change and approving the change are different people.

8 SPE 3 – Network and communications security

8.1 Purpose

The requirements in this SPE are defined to ensure that the IACS is protected from attacks conducted through the network and through communications capabilities. These attacks can originate external to the IACS, across security zone boundaries within the IACS and from unauthorized or compromised systems or devices connected to IACS networks. See IEC 62443-3-2 for guidance on assessing risk and partitioning systems into security zones.

8.2 NET 1 – System segmentation

8.2.1 NET 1.1: Segmentation from non-IACS zones

8.2.1.1 Requirement

The asset owner shall have policies and procedures segmenting IACS from non-IACS zones and limiting any interconnections to the minimum necessary for IACS operations and within tolerable risk.

8.2.1.2 Rationale and supplemental guidance

Remote/external networks provide access to the IACS from potentially unknown sources, and consequently pose a threat to the IACS. Network segmentation provides the means for restricting traffic (data and control flows) and limiting visibility between the IACS and external systems.

Traffic between the IACS and external systems should be identified, managed, authorized and documented. Authorization and management are a typically part of policies that define the technical and process aspects of secure remote access. In addition, this traffic should be characterized by their endpoints (for example, device and software application) and by their communications protocol.

Network security devices at the boundaries between IACS and non-IACS segments are used to enforce, authorize and monitor data flows, and their configurations should be appropriate, documented and kept current. They should be configured to limit access to only those access paths that are necessary and for which the level of trust associated with their external endpoint and the associated risk is tolerable.

Based on the tolerable risks, the asset owner should determine the SL-Ts for the IACS. IEC 62443-3-2 provides a description of the process steps to partition the Automation Solution into zones and conduits. It also describes how to identify the SL-T for each zone and conduit.

See 12.2.1, EVENT 1.1: Event detection, for more information about monitoring. See 8.2.6, NET 1.6: Internal network access control, for more information about zone-to-zone segmentation within the IACS environment.

8.2.2 NET 1.2: Documentation of zones and network zone interconnections

8.2.2.1 Requirement

The asset owner shall have policies and procedures for documenting and maintaining a baseline of all IACS zones and network zone interconnections and/or conduits, the security risks associated with each, and their designation as trusted or untrusted.

8.2.2.2 Rationale and supplemental guidance

As part of the network segmentation process, or after the network has been segmented, interconnections between zones and/or conduits should be evaluated for threats and associated risks. Interconnections are typically implemented by network devices, such as routers, firewalls and data diodes, that permit network traffic to flow between segments.

Understanding which interconnections are trusted or untrusted is an essential part of determining where network access controls are required (see 8.2.3, NET 1.3: Network segmentation from safety systems, and 8.2.4, NET 1.4: Network autonomy). Untrusted interconnections should be subject to a higher degree of protection.

NOTE Zones and conduits (see IEC TS 62443-1-1 and IEC 62443-3-2) are used to represent logical partitions of the system and communications channels between them whose implementation can be supported by network segmentation and network devices.

8.2.3 NET 1.3: Network segmentation from safety systems

8.2.3.1 Requirement

If the IACS contains a safety system network, the asset owner shall have policies and procedures related to protecting the safety system from interference by non-safety system networks and their devices.

8.2.3.2 Rationale and supplemental guidance

Safety systems should be operationally independent from control systems and other networks, including both wired and wireless networks. While it is often necessary for the safety system to be connected to the IACS 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 by the control system. Therefore, the safety system should be protected from interference from applications outside the safety system.

NOTE IEC 62443-3-2 recommends giving special attention to safety systems when creating zones and conduits.

Firewalls, gateways and other methods of managing access to the safety system can be provided to implement a degree of separation between the control system and the safety system. Other mechanisms or design strategies that protect the safety system from interference can also be used.

8.2.4 NET 1.4: Network autonomy

8.2.4.1 Requirement

The asset owner shall have policies and procedures around the ability to operate the IACS as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).

8.2.4.2 Rationale and supplemental guidance

The IACS should be capable of operating as designed when communication with non-IACS systems is lost. That is, failure of network communications with external systems should not cause the IACS to fail. The IACS may operate in a degraded mode or less optimized way, but, at a minimum, it should be possible to continue essential functions.

There can be cases, such as the Industrial Internet of Things and/or Industry 4.0, where there are external connections to the IACS. In cases such as these, the IACS should be designed so that essential functions continue to operate when external connections are disconnected.

8.2.5 NET 1.5: Network disconnection from external networks

8.2.5.1 Requirement

The asset owner shall have policies and procedures around the ability to disconnect the IACS from external networks to protect itself or the external networks from actual or suspected threats.

8.2.5.2 Rationale and supplemental guidance

The IACS should be able to be disconnected, either logically or physically, from external networks in response to adverse security-related conditions (see 8.2.4, NET 1.4: Network autonomy) originating from either the IACS or the external networks. However, the asset owner should determine when such disconnection is advised to ensure that disconnection does not create a higher risk than the actual or suspected threats.

Disconnection techniques can include manual or automatic disconnection. Network devices that allow traffic flow to/from external networks to be disabled or blocked can be used for this purpose.

8.2.6 NET 1.6: Internal network access control

8.2.6.1 Requirement

The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing security risks associated with communications between internal IACS network segments, including determining a tolerable risk level and responding to risks outside that tolerable risk level.

8.2.6.2 Rationale and supplemental guidance

When analysing the risks between internal IACS network zones in 8.2.2, NET 1.2: Documentation of zones and network zone interconnections, it is important to consider the potential for disruption to essential functions by disconnecting or restricting network communications between those zones. Communications between internal IACS network zones can also present risks, such as those associated with untrusted interfaces that need mitigation. When they do, these risks can be mitigated by restricting traffic between them and allowing only those data and control flows that are necessary and have been authorized.

Communications between internal IACS network segments that were identified in 8.2.2, NET 1.2: Documentation of zones and network zone interconnections, to have tolerable risks should be authorized and allowed if they are essential. All traffic that presents intolerable risks should be blocked and reported. This can be accomplished by using network segmentation devices that inspect all traffic and block all unauthorized traffic, also called default deny.

8.2.7 NET 1.7: Network accessible services

8.2.7.1 Requirement

The asset owner shall have policies and procedures around protecting network accessible services from unauthorized network access.

8.2.7.2 Rationale and supplemental guidance

Application services accessible through the network generally provide access to IACS resources. They should be accessed only by devices, applications and users and from network segments that are authorized to do so. This will protect the IACS against unauthorized access and against probes that attempt to discover and exploit application service vulnerabilities, thus reducing the attack surface of the IACS.

Network access control mechanisms, including but not limited to managed switches, routers with access control lists and firewalls should be configured to allow access to application services only from authorized client network addresses and ports and protocols. In addition, application services should be configured to allow only authorized users to establish sessions with them, thus providing an additional layer of protection.

8.2.8 NET 1.8: User messaging

8.2.8.1 Requirement

The asset owner shall have policies and procedures around restricting the capability of user-to-user messages transferred on IACS networks from containing payloads, such as attachments, network links or scripts, that can be used to support attacks against the IACS.

8.2.8.2 Rationale and supplemental guidance

Attachments, network links to remote applications and scripts have the potential to introduce malware into the IACS.

Email, instant messaging and other mechanisms that can be used to transfer files or establish links to unknown destinations should be excluded from use in the IACS.

8.2.9 NET 1.9: Network time distribution

8.2.9.1 Requirement

The asset owner shall have policies and procedures around securely distributing and synchronizing time within the IACS.

8.2.9.2 Rationale and supplemental guidance

Accurate, system-wide time is used to timestamp events when they occur. Therefore, time needs to be distributed throughout the IACS using a protocol that provides for synchronization across devices and preferably provides some level of protection against tampering.

It is important to verify that the time distribution protocol used is commonly accepted for industrial uses and has the granularity needed for the IACS. At the time of publication of this document, the IEEE 1588 [18] standard provides finer granularity than the network time protocol (NTP) and is more cost effective than Global Positioning System (GPS) technologies. Secure versions of some of the common time synchronization protocols can be used to provide additional authentication and validation to aid in protecting against the potential for tampering.

8.3 NET 2 – Secure wireless access

8.3.1 NET 2.1: Wireless protocols

8.3.1.1 Requirement

The asset owner shall have policies and procedures about the use of wireless communications within the IACS and which industry accepted protocols are authorized for use, if any. Any wireless protocol(s) shall be documented, and this documentation maintained to include:

a) a current baseline configuration of each,

b) data exchanges with other network segments, and

c) security capabilities and features employed by each wireless network.

8.3.1.2 Rationale and supplemental guidance

Wireless networks are not restricted by physical boundaries, allowing devices outside the physical perimeter of the IACS to access it. Therefore, it is important for the asset owner to use proven wireless protocols. It is also important for the asset owner to know how they are used, the data that is transferred over them and their security capabilities, including their strengths and limitations. Wireless and radio frequency (RF) surveys and security assessments can be used to gain understanding of their capabilities. Without this knowledge, the asset owner could not be able to make security-related decisions regarding their use.

The asset owner should ensure that it has identified and documented, as part of the IACS baseline, all wireless networks used by the IACS and their data flows. The asset owner should also be aware of the security features provided by them and make all of this information available for security assessments performed on the IACS. As part of a wireless and RF survey, asset owners should also consider looking for potential unknown and/or unauthorized wireless networks within their environment as these can represent a potential attack vector for their IACS.

8.3.2 NET 2.2: Wireless network segmentation

8.3.2.1 Requirement

If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around segmenting wireless networks from other IACS network segments.

8.3.2.2 Rationale and supplemental guidance

Wireless networks are not restricted by physical boundaries, allowing devices outside the physical perimeter of the IACS to access and transfer data to/from them. Therefore, it is important for the asset owner to control/manage all access, including data flows, within and from wireless networks. Subclause 8.3.1, NET 2.1: Wireless protocols, specifies the requirement for describing security-related characteristics for accessing the IACS from wireless networks.

Access controls, such as those provided by network segmentation devices and wireless gateways, should be configured to allow only necessary communications to/from wireless networks. Those devices should be used at the interface(s) between the IACS and the wireless network.

8.3.3 NET 2.3: Wireless properties and addresses

8.3.3.1 Requirement

If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around configuring wireless networks with properties and network addresses that minimize information useful to attackers.

8.3.3.2 Rationale and supplemental guidance

Network visible properties, such as network names and service set identifiers (SSIDs), that are too descriptive can give attackers information they can use to refine their attack. Network addresses can be statically configured, or they can be automatically assigned using the dynamic host control protocol (DHCP) or bootstrap protocol (BOOTP). Unfortunately, both DHCP and BOOTP have known vulnerabilities that can be exploited by attackers. Therefore, approaches for assigning SSIDs and network addresses should follow commonly accepted industry security practices.

Commonly accepted practices for network names at the time of publication of this document are to use descriptive names that keep confusion for administrators to a minimum, but that do not provide location, ownership, function detail or other information that could be useful to attackers.

8.4 NET 3 – Secure remote access

8.4.1 NET 3.1: Remote access applications

8.4.1.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around the use of commonly accepted remote access applications in the IACS.

8.4.1.2 Rationale and supplemental guidance

Remote access applications, such as remote desktop applications, allow remote login to workstations and devices. Other remote access applications, like Open Platform Communications (OPC), provide remote connections into the IACS. In the past, many remote access applications were not developed with adequate security and were breached. Therefore, remote access applications used in the IACS should be properly vetted prior to use.

Remote access connections 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 products should not be used until carefully evaluated and tested by reputable and well-known third parties for security weaknesses.

8.4.2 NET 3.2: Remote access connections

8.4.2.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around authorizing, authenticating, encrypting, documenting, logging and monitoring all interactive remote access connections. Documentation for each connection shall include, but not be limited to:

a) its purpose,

b) the remote access application to be used,

c) encryption and authentication technologies used,

d) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions, as necessary,

e) the circumstances requiring the connection,

f) the length of time the connection needs to be open, including expected inactivity periods,

g) the location and identity of the remote client device, application and user, and

h) any compliance requirements that need to be met prior to establishing the connection.

8.4.2.2 Rationale and supplemental guidance

Interactive remote access applications, such as remote desktop applications, allow remote login to workstations and devices. Other remote access applications, like OPC, provide remote connections into the IACS. In both cases, they provide the potential for a remote computer, like a workstation or laptop, that has potentially been infected with malware to infect or attack the IACS. For example, a laptop with remote access privileges might be taken offsite, be connected to the Internet and then be infected. From the same laptop, the user might then create a VPN connection and establish a remote desktop connection over a corporate VPN to the IACS. If written with sufficient intelligence, the malware will then have direct access to the IACS.

The asset owner should have a process for documenting and authorizing all remote access connections before they can be used. This typically includes a process for requesting a remote access connection between a client and a server, a validation and approval process for the connection based on its expected use and a process to prepare for the connection for use, such as creating firewall rules, configuring VPNs and the DMZ and granting the client user access to the server application.

This should be documented along with any instructions that are needed to prepare and use the connection(s). 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. This documentation should be adequate to evaluate and approve the request, and, if approved, to authenticate the client device and user.

8.4.3 NET 3.3: Remote access termination

8.4.3.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around terminating all interactive remote access connections after a configured inactivity period.

8.4.3.2 Rationale and supplemental guidance

Leaving remote access connections open, when not in use, creates an unnecessary risk for the connection to be used inappropriately, or for attackers to attempt to take control of them, thus increasing the attack surface.

Remote access connections should be approved for use for a specific period of time or while actively being used and configured for automatic termination after a specified period of inactivity.

9 SPE 4 – Component security

9.1 Purpose

The requirements in this SPE are defined to ensure that the IACS and its components (for example, devices and software) are appropriately protected from attacks. These attacks can originate through component interfaces, both external and internal. Examples of external interfaces include network interfaces, USB interfaces and configuration ports. Examples of internal interfaces include inter-process communications interfaces and application programming interfaces (APIs).

Subclause 9.4, COMP 3 – Patch management, addresses the application of security patches to close known security vulnerabilities in IACS components. For more details on patch management, see IEC TR 62443-2-3.

9.2 COMP 1 – Components and portable media

9.2.1 COMP 1.1: Component hardening

9.2.1.1 Requirement

The asset owner shall have policies and procedures to harden components prior to their use in the IACS to protect their software and hardware features, to maintain the hardened state during the lifetime of the components and to maintain the documentation of hardening items, means and procedures of the components.

9.2.1.2 Rationale and supplemental guidance

The purpose of hardening is to reduce the attack surface of the device. Hardening a device involves removing or disabling features that are not needed for operation within the IACS, protecting the device interfaces from unauthorized physical and logical access and ensuring that maintenance processes do not cause the hardened state of the device to be compromised or degraded.

Hardening is often accomplished prior to or during installation of a device into the IACS. Security templates, such as those specified by the Center for Internet Security (CIS), define security settings that can be applied to restrict use of the device and protect it against attack. In addition, unnecessary applications, such as games, protocols and digital certificates, shipped with commercial-off-the-shelf (COTS) OSs and other infrastructure software, along with unnecessary communications ports and associated communication access services, should be removed or disabled to prevent them from being used to intentionally or unintentionally interfere with device operations or infect the device with malware.

Hardening measures are specific to each component. Examples of hardening measures include, but are not limited to:

- removing/disabling unnecessary software applications and services (for example, email, office applications and games) and their associated communication access points (for example, TCP / user datagram protocol (UDP) ports);
- enabling interfaces for portable media when authorized for use and disabling them when not authorized for use;
- removing/disabling wireless communications that are not required by the IACS;
- removing/disabling network addresses that are not authorized for use;

- protecting physical and logical access to diagnostic and configuration ports from unauthorized access and use;
- configuring unused ports on network devices (for example, switches and routers) to protect against unauthorized access to the IACS network infrastructure; and
- ensuring maintenance processes maintain the hardened state of the IACS during its lifetime.

During operation, it will often be necessary to change the configuration of components due to operational conditions. For example, a third-party organization may require the asset owner to open ports in order to perform maintenance activities on assets in the IACS. Procedures need to be defined to ensure that the hardened state of both the IACS and its components are recovered after the configuration changes.

9.2.2 COMP 1.2: Dedicated portable media

9.2.2.1 Requirement

The asset owner shall have policies and procedures related to the approved or disapproved use or functions of portable media within the IACS.

9.2.2.2 Rationale and supplemental guidance

Portable media is media that is removable and can be taken offsite to other locations where it can be infected. Dedicating portable media, such as USB memory sticks, to the IACS and to specific use within the IACS can minimize the potential for it becoming infected with malware.

Policies and procedures should be in place that

- define the portable media that can be used and the functions within the IACS for which it can be used, and
- restrict its usage to the approved functions within the IACS and only by approved devices.

In addition, technical measures can be taken to authenticate media to ensure they have been authorized for use within the IACS. For example, if portable media is authorized for use to perform an essential function, such as a safety function, the asset owner needs to ensure that the portable media used is only dedicated to that purpose and not used elsewhere.

9.3 COMP 2 – Malware protection

9.3.1 COMP 2.1: Malware free

9.3.1.1 Requirement

The asset owner shall have policies and procedures to verify that all components and portable media (if portable media is authorized for use in the IACS) are free of known malware before being used in the IACS.

9.3.1.2 Rationale and supplemental guidance

Devices and portable media can be infected prior to or during shipment. This provides a method of attack that does not require network connectivity or physical presence of the attacker. Ensuring that malware is not present in devices and portable media installed into the IACS minimizes this avenue of attack. For encrypted media, the asset owner should obtain assurances from the supplier that procedures are in place to verify the data contained on the encrypted media is free of malware.

Mechanisms used to ensure malware is not present in devices and portable media include scanning and authenticity checks, such as digital signatures. Authenticity checks can determine if software images in the device have not been modified. Scanning is used to detect known malware and is useful, in particular when authenticity checks are not supported. Further, distribution path protections, such as anti-tampering seals can also be used to support this requirement.

9.3.2 COMP 2.2: Malware protection

9.3.2.1 Requirement

The asset owner shall have policies and procedures related to the installation, functioning, and maintenance of malware protection mechanisms, where feasible.

9.3.2.2 Rationale and supplemental guidance

Mechanisms that provide protection against known malware are used to detect malware and also to prevent it from executing. These need to be verified to prevent the infection of the system with malware. These mechanisms also need to be tested for compatibility with the component, meaning that they have been tested to verify that they do not interfere with the function and operation of the component.

Malware protection software is often not available for all IACS components. Components for which malware protection software is not available should be documented and protected by compensating security measures in the IACS that are appropriate for the assessed level of risk.

Three primary methods for protecting a component against malware are antivirus, allow-listing and digital signature verification. Antivirus software is used to examine files and data entering the device and compare it to known bit-patterns called a malware signature, often called deny-listing. The malware signatures need to be kept up to date to cover all known malware. When malware is detected, it is normally quarantined, and the user is notified to take the appropriate action. Allow-listing, on the other hand, is configured to allow only authorized software to execute. Thus, allow-listing does not require updates to malware signatures and also provides protection against previously unknown malware. Digital signature verification can be considered a form of allow-listing, since it authenticates software based on its digital signature (usually a form of a secure hash) prior to allowing it to run.

9.3.3 COMP 2.3: Malware protection software validation and installation

9.3.3.1 Requirement

The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of malware protection software and any related malware signature files in a timely manner after their release.

9.3.3.2 Rationale and supplemental guidance

Anti-malware mechanisms are often integrated into OS routines, and therefore, have the potential for affecting how the system operates. In addition, because malware protection software examines files and data for predefined bit-patterns, it could be that legitimate device software or data has the same bit patterns. This is unlikely, but it has occurred. Therefore, all anti-malware software should be checked for compatibility with device software to ensure that it does not interfere with the function and operation of the device.

Testing of anti-malware software should be performed prior to its use in a device. This is generally done by the service provider or the product supplier.

Because the IACS is vulnerable to known malware until malware protection software and its malware signature files are installed, timely installation is important. Timeliness, therefore, is a factor in reducing risks to a tolerable level.

9.4 COMP 3 – Patch management

9.4.1 COMP 3.1: Security patch authenticity/integrity

9.4.1.1 Requirement

The asset owner shall have policies and procedures related to verifying the authenticity and integrity of all patches prior to installation.

9.4.1.2 Rationale and supplemental guidance

Patches are typically distributed by the product supplier using a variety of delivery mechanisms, including network transfers, CDs/DVDs and USB memory sticks. During the transfer, it is possible that the patches are intercepted and infected with malware. Therefore, verifying their integrity and authenticity is necessary.

Asset owners should verify that all patches are received directly from the patch developer, that the distribution path is protected and that support for authenticity and integrity checking is provided, such as digital signatures, or that compensating security measures are applied when digital authenticity and integrity checking is not feasible. In addition, asset owners should verify that patches have not been infected at the product supplier's site. For distribution media, such as CDs/DVDs/USB, tamperproof seals should also be used. See IEC TR 62443-2-3 for additional guidance.

9.4.2 COMP 3.2: Security patch validation and installation

9.4.2.1 Requirement

The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of security patches applicable to components in a timely manner after their release.

9.4.2.2 Rationale and supplemental guidance

Security patches are often provided for OS and infrastructure software that is developed independently from IACS software. As a result, the IACS software can be affected by these patches. Therefore, it is necessary to test security patches with the IACS prior to using them.

Testing of security patches should be performed prior to its use in a device. This is generally done by the service provider or the product supplier.

Because patches close vulnerabilities, the IACS is vulnerable to associated attacks until the patches are installed. Therefore, timely installation is important and is a factor in reducing risks to a tolerable level.

9.4.3 COMP 3.3: Security patch status

9.4.3.1 Requirement

The asset owner shall have policies and procedures related to the documentation and maintenance of the security patch status of all components.

9.4.3.2 Rationale and supplemental guidance

When troubleshooting or when performing diagnostics or forensics, it is necessary to know the software configuration, including patch status, of a device. In addition, when assessing device vulnerabilities, it is essential to know which security patches have been applied.

Security patch status should be maintained to indicate, at a minimum:

- the patch identifier,
- the applicable software that is being patched,
- the date of patch release, and
- the date of patch installation (planned or actual).

Refer to IEC TR 62443-2-3 for supplemental guidance.

9.4.4 COMP 3.4: Security patching retention of security

9.4.4.1 Requirement

The asset owner shall have policies and procedures to verify that security patch installation does not cause a reduction in the security of the component.

9.4.4.2 Rationale and supplemental guidance

In some cases, installation of patches can introduce known vulnerabilities, cause the removal of configuration settings, change the way the software handles configuration settings or change the function of the software. If the installation is not properly managed, installation can also result in loss of integrity of device contents, where some elements of the device have been removed as part of the installation process. In addition, patches can be installed that are not authenticated as part of the installation process, potentially resulting in the installation of patches that have been the subject of tampering.

Maintenance procedures should include verification that the state of a device's contents and configuration have not been degraded by patch installation. Refer to IEC TR 62443-2-3 for supplemental guidance.

9.4.5 COMP 3.5: Security patch mitigation

9.4.5.1 Requirement

The asset owner shall have policies and procedures related to assessing the risk of not installing any applicable security patches, and if the risk is not tolerable, addressing the risk and documenting the resolution.

9.4.5.2 Rationale and supplemental guidance

When security patches are not installed, for example because they failed testing, were not approved for installation or were not made available in time, their associated vulnerabilities remain. Therefore, workarounds or other compensating security measures should be used.

The asset owner should ensure that all security patches that are applicable to the device, but that were not installed, are assessed for risk(s) and addressed through workarounds or compensating security measures if the associated risks are unacceptable. Risks and resolutions should be documented. Refer to IEC TR 62443-2-3 for supplemental guidance.

10 SPE 5 – Protection of data

10.1 Purpose

The requirements in this SPE are defined to ensure that data is protected from disclosure (confidentiality) and tampering (integrity).

10.2 DATA 1 – Protection of data

10.2.1 DATA 1.1: Data classification

10.2.1.1 Requirement

The asset owner shall have policies and procedures related to identifying and classifying all IACS data requiring safeguarding according to their protection requirements.

10.2.1.2 Rationale and supplemental guidance

To protect data from disclosure and tampering, it is necessary to understand which data needs to be protected and whether it needs to be protected from disclosure, tampering, loss, loss of use or some other compromise. The risk value to the organization of compromise is also necessary and is used to determine the degree to which it needs to be protected.

A risk assessment generally is used to identify data and the risk/impact to the organization associated with its compromise, including disclosure, tampering, loss or loss of use.

The following are examples of types of IACS data that should be identified and classified:

a) user authentication and authorization information,
b) audit and security log information, including audit history,
c) test data,
d) configuration data,
e) cryptographic keys,
f) backup data,
g) control action transfers, including direction of transfer,
h) proprietary and trade secret data, and
i) any personally identifiable information (PII) collected or processed in the IACS.

10.2.2 DATA 1.2: Data confidentiality

10.2.2.1 Requirement

The asset owner shall have policies and procedures related to the confidentiality of IACS data taking into account risks to compromise of the data according to their classification.

10.2.2.2 Rationale and supplemental guidance

Confidentiality of data needs to be protected whether at rest or in motion. Failure to protect the confidentiality of the data can result in a compromise to it. Data at rest is generally considered to be data held in volatile memory (for example, computer memory) or in non-volatile memory (for example, disk, CD/DVD/USB or flash memory). Data in motion is generally considered to be data being moved between two or more locations, either electronically via some form of communication link or physically.

Data can be protected from unauthorized access via a number of mechanisms. Which mechanism is used and in which combination depends on the classification of data and its value to the organization. Generally, user access controls provide the first level of defence for data at rest, allowing only those authorized to access the data or the software using the data to access it.

Approvals for the transfer of data can be used to restrict which data is transferred.

Encryption can be used to protect data from disclosure. It can be used for data at rest when intruders have somehow defeated access controls. It is often used for data in motion to prevent anyone who is able to intercept or monitor data transmissions from being able to retrieve the original information.

When these capabilities are not feasible or when additional protection is desired, access controls that restrict physical and network access to computers and communications links allow data to be isolated from attackers.

10.2.3 DATA 1.3: Safety system configuration mode

10.2.3.1 Requirement

If safety systems are authorized for use in the IACS, the asset owner shall have policies and procedures related to:

a) updating the safety system configuration only when configuration mode is enabled, and

b) only enabling configuration mode when configuration changes are necessary.

10.2.3.2 Rationale and supplemental guidance

The safety system, like a control system, operates according to configuration parameters written or downloaded to it. Typically, the configuration is static, changing only when necessary. To protect against unauthorized changes to the safety system configuration, the safety system configuration should be updated at approved times only, and configuration changes should be allowed only for a finite duration. Such an approach is often referred to as configuration mode for the safety system. Configuration mode can be enabled using explicit actions of the safety system administrator and disabled for normal operation of the safety system once the configuration update has been completed.

A safety system configuration mode should be supported by a software, hardware or mechanical interface that is available only to authorized safety system administrators. The default should always be "disabled".

10.2.4 DATA 1.4: Data retention policy

10.2.4.1 Requirement

The asset owner shall have policies and procedures related to data retention during the entire IACS lifecycle, including purging.

10.2.4.2 Rationale and supplemental guidance

Data retention refers to keeping data values and events, such as logs, histories and backups, for a specified period of time. This also includes ensuring that data requiring safeguarding is purged when the device is decommissioned or otherwise removed from the IACS. Data retention policies, such as the length of time to keep the values, and associated capabilities should be established to support security operations, such as recovery and forensics, and control operations, such as trend analysis. These policies and capabilities should be specified to minimize risks to the organization and be documented.

Data retention policies generally include length of time to keep data values and events for runtime copies, locally accessible copies (for example, logs and historians) and archived copies. Capabilities include capacities to support the policies and the timeliness of being able to retrieve desired copies.

Confidential data in devices should be purged from memory when the device is decommissioned or otherwise removed from service. This prevents disclosure of that data to those who can subsequently have access to the device. For example, a device's memory should be purged when returning a failed board/device to the supplier for repair under a support service contract. See 10.2.2, DATA 1.2: Data confidentiality, for more information on protecting the confidentiality of IACS data.

In some situations, read-only memory should be preserved to allow the product supplier to troubleshoot the problem. To support these cases, the agreements with the supplier should include protection of asset owner data.

Devices used in the IACS should have mechanisms or documented procedures for purging confidential, non-volatile data from them. Non-volatile data media includes disks and flash memory.

10.2.5 DATA 1.5: Cryptographic mechanisms

10.2.5.1 Requirement

The asset owner shall have policies and procedures related to utilizing commonly accepted cryptographic mechanisms in the IACS.

10.2.5.2 Rationale and supplemental guidance

The IACS should use cryptographic mechanisms that are in current use by IT, as well as industrial applications, and are regarded as free of publicly known vulnerabilities and weaknesses.

10.2.6 DATA 1.6: Key management

10.2.6.1 Requirement

If cryptographic mechanisms utilizing keys are approved for use in the IACS, the asset owner shall have policies and procedures around using, protecting and enforcing the lifetime of cryptographic keys, following practices and recommendations commonly accepted by both the industrial and security communities.

10.2.6.2 Rationale and supplemental guidance

Key management is an important component for the use of cryptographic mechanisms, such as data encryption, digital signatures and authentication. Poor key management can result in the compromise of keys that can result in cryptographic failure.

Handling of expiration of certificates needs to be taken into account to avoid risks to the operations of the IACS in the event of an expired certificate.

10.2.7 DATA 1.7: Data Integrity

10.2.7.1 Requirement

The asset owner shall have policies and procedures related to data integrity protection from compromise, whether at rest or in motion (electronically or physically), that take into account applicable risks.

10.2.7.2 Rationale and supplemental guidance

Data needing integrity protection needs to be protected whether at rest or in motion. Failure to protect the integrity of the data can result in a compromise that can impact the industrial process.

Approvals for the transfer of data can be used to restrict which data is transferred, and data/parameter validation can be used to determine if it has been changed in transit or whether invalid values are being transmitted.

Digital signatures can be used to protect data at rest or in motion from tampering. They provide a secure checksum that allows authentication and detection of changes.

When these capabilities are not feasible or when additional protection is desired, access controls that restrict physical and network access to computers and communications links allow data to be isolated from attackers.

11 SPE 6 – User access control

11.1 Purpose

The requirements in this SPE are defined to ensure that users (human users, software processes and devices) are assigned accounts that are used to control access to the IACS and its resources and commands. Access control involves identification, authentication and authorization in order to assign and enforce access rights as well as the control of user sessions. IACS human users include, but are not limited to, engineers, operators, administrators and support personnel.

OS and control system access rights grant users' permission to use IACS resources and issue commands. Typical access rights include read, write and execute; however, others are possible. Sessions are user connections to the system established as a result of successful identification and authentication.

In general, user account management policies should be defined to provide consistency across user accounts that meet the requirements of Clause 11. Such policies will typically be formally documented and provide a framework for creating and maintaining user accounts.

11.2 USER 1 – Identification and authentication

11.2.1 USER 1.1: User identity assignment

11.2.1.1 Requirement

The asset owner shall have policies and procedures for assigning IACS-specific identifiers, authenticators and roles to users (human users, software processes and devices).

11.2.1.2 Rationale and supplemental guidance

User accounts are digital representations of users. Identifiers relate users to accounts and authenticators, such as passwords, give human users, software processes and devices permission to use their associated account. Human users are authenticated during login and are granted access to run programs under the account used to login. Software processes are authenticated when they are started automatically by the OS and run under the account used to start them.

For devices, the account management system is configured with an account that is used to verify a device’s identity during device connection to the system. This capability verifies that devices are authorized to participate in system operations and complements network device authentication (see 11.2.19, USER 1.19: Component authentication), which is used to prevent unauthenticated devices from transmitting or receiving on the network.

Human users and software processes can also be authenticated when they establish a communications connection with another software process, typically referred to as a server. In these cases, the server process determines whether it will use the account under which it is running or the account of the user or software process that was authenticated.

Roles, such as operator, process engineer, maintenance engineer and administrator, represent groups/sets of access rights that can be assigned to human users. The use of identifiers, authenticators and roles, simplifies management of user access controls and reduces the potential for errors and omissions in the associated processes. See 11.2.4, USER 1.4: Access rights assignment, for the assignment of access rights to user accounts and roles.

Roles should be defined for the IACS based on how users will use the system. When a user account is added to the system, an identifier, an authenticator (for example, password or smart card) and one or more roles should be assigned to the account. Accounts may be created for individual users (human users, software processes and devices) or for a logical user, which is typically done for software (the software executable is the logical user while the instantiated process is the individual user). Logical users, however, can also be created for human users, such as "third shift operator", provided that the account will be used by a uniquely identified individual. Individual accounts for human users are preferred.

11.2.2 USER 1.2: User identity removal

11.2.2.1 Requirement

The asset owner shall have policies and procedures for removing/disabling IACS-specific identifiers, authenticators, roles and access rights for human users, software processes and devices that do not or no longer need access.

11.2.2.2 Rationale and supplemental guidance

When a user no longer needs access to the IACS, even for a temporary period, the user's access to all accounts assigned to it should be removed or disabled. Keeping access to accounts associated with the user provides an unnecessary access path into the system.

A process should exist for reporting when a user will no longer need access to the system and for removing/disabling access by that user. This process should be coordinated with human resources to ensure that any employee action (for example, transfers, resignations or terminations) requiring user identity actions is immediately addressed.

Removing/disabling access can involve removing/disabling accounts assigned to the user, changing passwords for password-protected shared accounts, retrieving smart cards from the human user and disabling them or some similar action for other types of authenticators.

11.2.3 USER 1.3: User identity persistence

11.2.3.1 Requirement

The asset owner shall have policies and procedures to verify that IACS-specific user identifiers, authenticators, roles and their associated access rights that are used to support essential IACS operations, including operator accounts, are configured so they are not disabled automatically.

11.2.3.2 Rationale and supplemental guidance

Automatic expiration and other types of automatic disabling of accounts, groups and authenticators have the potential for causing DoS for essential operations whose software runs under those identities. Essential operations are those that are required to maintain health, safety, the environment and availability for the equipment under control.

A threat or risk assessment should identify essential operations and their software dependencies, as well as the user accounts under which that software runs. Policies should be established and enforced (for example, through verification) for those accounts, groups and authenticators to ensure that they are not configured for automatic expiration or termination.

11.2.4 USER 1.4: Access rights assignment

11.2.4.1 Requirement

The asset owner shall have policies and procedures for assigning, reviewing and removing access rights to/from IACS-specific roles and users.

11.2.4.2 Rationale and supplemental guidance

User identification and authentication authorizes the user to access the system, and access rights grant the user permission to use OS and IACS resources and commands within the system. Typical rights include read, write and execute. Access rights are generally assigned to roles, which users then inherit from the roles that have been assigned to them.

Access rights are usually administered separately for those enforced by the OS and for those enforced by the control system software. OS resources/commands generally include files, OS configuration data and OS administrator data and functions. Control system resources/commands generally include parameters (for example, setpoints and alarm limits) and calibration and maintenance functions.

11.2.5 USER 1.5: Least privilege

11.2.5.1 Requirement

The asset owner shall have policies and procedures to verify that IACS users are only granted the access rights that they require to perform their assigned tasks.

11.2.5.2 Rationale and supplemental guidance

Granting IACS users more access rights than they need means that they will have capabilities that they should not have to view data, make changes to the system or both. It also means that if software running under their account becomes infected with malware, that malware will also have those additional rights. IACS users include all users who have IACS accounts, including operators, engineers, administrators, maintenance personnel and product supplier/service provider personnel.

Role-based access control (RBAC) is typically used to grant roles only the rights they need, and then assign those roles only to users who need them. Of particular concern are rights assigned to software accounts. They are often given elevated privileges that they do not need. Therefore, least privilege requirements should be provided to developers and software accounts.

11.2.6 USER 1.6: Software service authentication

11.2.6.1 Requirement

The asset owner shall have policies and procedures related to identifying and authenticating software services prior to their execution.

11.2.6.2 Rationale and supplemental guidance

Two commonly used software identification and authentication techniques are described below; however, there can be others that meet this requirement.

Software services are typically run under an account assigned to them. This account may be shared by two or more software services, or it can be an account created specifically for the software service. Therefore, these services should not be allowed to start without first being identified and authenticated for that account by the infrastructure (for example, a service control management application).

Digital signatures and allow-listing provide a supplemental or alternative way to verify the identity and authenticity of software and to authorize its execution. For them, infrastructure software is also involved in verifying the identity and authorizing the execution prior to starting the service.

11.2.7 USER 1.7: Software services interactive login rights

11.2.7.1 Requirement

The asset owner shall have policies and procedures related to denying software services interactive login capabilities.

11.2.7.2 Rationale and supplemental guidance

Software services that run under an account that has interactive login privileges provide the potential for attackers to use those accounts to login to the system, thus expanding the attack surface.

Generally, accounts have properties that control how they are used. Typically, a property is defined that allows/disallows the account to be used for interactive logins. For accounts used to start service control programs, that property should be set to "disallow" when this is supported by the software service.

11.2.8 USER 1.8: Human user authentication

11.2.8.1 Requirement

The asset owner shall have policies and procedures related to identifying and authenticating all human users on all IACS interfaces that can be used by human users to access the IACS. This includes, but is not limited to:

a) device interactive human user login interfaces,

b) application interfaces such as web services, file transfers and OPC servers, and

c) remote desktop interfaces that provide human users login access to IACS devices over the network.

NOTE Some OSs manage the conveyance of the authenticated user identity transparently to the application and make the user identity available to the application.

11.2.8.2 Rationale and supplemental guidance

Human users who access the IACS but who are not identified and authenticated pose a risk to the IACS. These users are often granted access using "guest" accounts for desktop access and "anonymous" accounts for web server access. Both of these account types have restricted privileges, but they still allow the user to launch attacks that attempt to discover or exploit internal vulnerabilities of the system. Guest and anonymous accounts should not be used in the IACS. All users should be properly identified and authenticated prior to granting them access.

In addition, client applications, such as tunnelers, that do not securely convey the authenticated IACS human user identity to the server can pose a larger problem by connecting to the server with an account that has higher privileges than the human user. The human users then operate with elevated privileges that they should not have.

11.2.9 USER 1.9: Multifactor authentication (MFA)

11.2.9.1 Requirement

The asset owner shall have policies and procedures related to using MFA by devices that support interactive human user login for remote access or when they are located in public access areas.

11.2.9.2 Rationale and supplemental guidance

MFA is used to provide a more secure method of identification and authentication. It is generally composed of a combination of something a user knows (for example, password or personal identification number (PIN)), something a user has (for example, a smart card or security token) and something a person is (for example, fingerprint or retinal scan). Using MFA for workstations that can be accessed by non-IACS users makes it more difficult for these users to defeat a single-factor authentication mechanism, such as a password-only scheme.

All devices that support interactive user login, such as workstations, and that are granted access to the IACS should be evaluated to determine if they face the risk of access by unauthorized personnel. Those that do should be protected by an MFA scheme. Where the use of MFA is not feasible, compensating security measures, such as physical access control, in combination with single-factor authentication, can be used when the risk of access by unauthorized personnel needs to be reduced. In addition to this information, the asset owner's policies and procedures should indicate whether or not MFA is approved for use in the IACS and where it is approved for use.

11.2.10 USER 1.10: Mutual authentication

11.2.10.1 Requirement

The asset owner shall have policies and procedures related to using mutual authentication for access to all server applications hosted on IACS devices, including web technology-based servers.

11.2.10.2 Rationale and supplemental guidance

Mutual authentication is used to verify to the login process that the user is known and authorized. It is also used to verify to the user that the login process is known and authorized and not spoofing (pretending to be) a legitimate login process. Login processes that spoof legitimate login processes typically ask users for their credentials and steal them. The same spoofing technique can be used by attackers to mislead an operator to configure the wrong device, which poses a risk to the availability and integrity of the IACS.

Server applications should be installed to use mutual authentication. Web server managers, such as Apache and Microsoft Internet Information Services (IIS), usually have the option for using mutual authentication. Some protocols, like mTLS, establish a process to encrypt connections in which both parties, client and server, use digital certificates to authenticate each other using trusted third-party services.

11.2.11 USER 1.11: Password protection

11.2.11.1 Requirement

When passwords are used in the IACS, the asset owner shall have policies and procedures to increase the degree of difficulty to compromise passwords, including complexity, lifetime and reuse.

11.2.11.2 Rationale and supplemental guidance

Password policies are used to make it more difficult to compromise and use compromised passwords.

Policies for password length and complexity can be used to make compromise more difficult. Password lifetimes (expiration times) and reuse properties limit the time period that a compromised password can be used to gain access the system. NIST SP800 63B [19] provides guidance on password complexity, lifetimes and reuse.

11.2.12 USER 1.12: Shared and disclosed/compromised passwords

11.2.12.1 Requirement

The asset owner shall have policies and procedures for managing shared and disclosed/compromised passwords.

11.2.12.2 Rationale and supplemental guidance

Passwords for maintenance and other accounts, such as operator accounts, are often shared to simplify account and password administration to fit operational requirements. However, without appropriate controls, knowledge of who has access to the system can be lost. In these cases, personnel who no longer need access can still be able to use shared passwords.

Policies and procedures for the use of shared passwords, including approvals and records, should be defined and used. These policies and procedures should identify the accounts for which passwords can be shared, who may use a shared password, how long a shared password is valid and rules for revoking shared passwords. Other policies and procedures may be defined as needed, typically as a result of assessing risks associated with their use. Exceptions to these policies should be documented.

Note that password patterns are sometimes used to simplify sharing of passwords. However, it is often better to have a managed and secure written password sharing system than to use password patterns that can be known by people who no longer are assigned to a work area.

11.2.13 USER 1.13: User login display information

11.2.13.1 Requirement

The asset owner shall have policies and procedures to display login information to the user to assist in the detection of fraudulent logins.

11.2.13.2 Rationale and supplemental guidance

Users should participate in the security of the system by being able to review historical login information about their account. For example, users could use this information to determine whether someone else was or is using their account to access the system.

Login screens should be set to provide information to users appropriate to the level of risk. Information will normally be provided about user login histories, such as date, time and workstation of their last login and logout and date, time and workstation of login sessions that are still open. Other information can be useful, such as information about the most recent failed login attempts.

11.2.14 USER 1.14: User login failure displays

11.2.14.1 Requirement

The asset owner shall have policies and procedures related to displaying information following a login failure to limit the information useful to attackers.

11.2.14.2 Rationale and supplemental guidance

Login failure information, such as "invalid username" or "password should be composed of …" messages can be used by attackers to refine their attempts to break into the system. Any information released to unauthenticated entities can be used for side-channel attacks. Therefore, failure information should be kept to a minimum, informing the user only that the login failed.

11.2.15 USER 1.15: Consecutive login failures

11.2.15.1 Requirement

The asset owner shall have policies and procedures related to denying login access to user accounts for a specified length of time or until unlocked by an authorized administrator after the configured number of consecutive unsuccessful login attempts have occurred.

11.2.15.2 Rationale and supplemental guidance

Enforcing a maximum number of consecutive login failures prevents attackers from continuously trying to login, protecting against password exhaustion attempts. However, locking out an account after consecutive login failures makes the account vulnerable to a denial-of-service attack. As a result, a risk assessment needs to be conducted to identify any accounts or devices that need to be exempted from the locking policy as the failure to login represents a bigger risk for the IACS.

Account policies should be defined to manage the process to lock and unlock a user after a specified number of consecutive login failures has been reached.

11.2.16 USER 1.16: Session integrity

11.2.16.1 Requirement

The asset owner shall have policies and procedures related to protecting sessions from unauthorized access and modification.

11.2.16.2 Rationale and supplemental guidance

Sessions are user connections to the system established by the login process. They are system resources and should be protected from misuse and hijacking to protect against attackers interfering with user activity and to protect against attackers gaining access through them.

As critical system resources, sessions should be protected by authentication, encryption and access control lists that require administrative privileges to access them.

11.2.17 USER 1.17: Concurrent sessions

11.2.17.1 Requirement

The asset owner shall have policies and procedures related to limiting the number of concurrent sessions per interface for any given human user, software process or device.

11.2.17.2 Rationale and supplemental guidance

Users often have the need to have multiple sessions open at the same time for the operation of the IACS. However, allowing the system to accept an unlimited number of concurrent sessions exposes the IACS to a higher degree of risk related to session hijacking and to denial-of-service attacks.

User activities should be assessed, and if a user needs to login multiple times concurrently, then a practical upper limit should be determined, and the system configured accordingly.

11.2.18 USER 1.18: Screen lock

11.2.18.1 Requirement

The asset owner shall have policies and procedures related to locking user screens upon user request or automatically after a configured period of inactivity unless failure to access the screen can result in a greater risk to the IACS. Re-authentication shall be required of an authorized user to unlock it.

11.2.18.2 Rationale and supplemental guidance

User screens that are inactive for a period of time are often left unattended by the user. In these cases, the screen should be locked to prevent unauthorized use of the session. Operator screens are screens used to control operations of the physical process, such as viewing and responding to alarms, viewing faceplates and changing setpoints. These screens need to be available to monitor the process, therefore, they normally remain unlocked. The asset owner should consider the risks associated with using or not using screen locks on operator screens.

OSs typically have a screen lock function that can be configured to lock the screen after a period of inactivity. The period of time to use is dependent on a number of factors related to the physical environment in which the workstation exists and the work practices of the user. An appropriate value should be selected that allows the user to be productive but does not leave the screen exposed and vulnerable.

11.2.19 USER 1.19: Component authentication

11.2.19.1 Requirement

The asset owner shall have policies and procedures related to identifying and authenticating all components connected to the IACS.

11.2.19.2 Rationale and supplemental guidance

This requirement addresses the component's ability to be authenticated using the identification credentials associated with 11.2.1, USER 1.1: User identity assignment. However, some devices, such as legacy devices and field devices, do not always support identification and authentication protocols, thus requiring compensating security measures to be applied to them to meet this requirement, such as stringent physical access controls.

At the time of publication of this document, some examples of different authentication mechanisms include, but are not limited to, the Institute for Electrical and Electronics Engineers (IEEE) 802.1AR [20], the Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP) (request for comment (RFC) 3748 [21], RFC 7057 [22]), IETF Autonomic Networking Integrated Model and Approach (ANIMA) / bootstrapping of a remote secure key infrastructure (BRSKI) and IEEE 802.1X [23] define protocols that support device identification and authentication. For wireless instrumentation and control networks, IEC 62591 WirelessHART™ [24] and IEC 62734 ISA-100.11a [25] both provide for secure connection of devices to wireless networks.

11.3 USER 2 – Authorization and access control

11.3.1 USER 2.1: Authorization

11.3.1.1 Requirement

The asset owner shall have policies and procedures related to enforcing assigned access rights for all users.

11.3.1.2 Rationale and supplemental guidance

Access rights to execute commands and access resources, such as files, should be assigned to users based on their job descriptions. Access rights are used to protect IACS commands from unauthorized execution and IACS data from unauthorized disclosure and modification.

These access rights need to be enforced to prevent users from bypassing them, for example, through backdoors and direct connections to devices. Such bypassing can provide access by users who do not have the appropriate access rights, thus allowing uncontrolled access to IACS commands and data and to physical resources that they represent. Client applications that connect to IACS servers using accounts with read and write privileges to protected parameters (for example, setpoints and alarm limits) can also be used to circumvent access controls. This can happen when the client application does not verify user privileges and users who do not have access privileges for the protected parameters are allowed to run the client application.

Security assessments should be conducted to identify all access paths through the IACS and verify that all are subject to access controls. See IEC 62443-3-2 for more detail on the use of security assessments within an IACS.

11.3.2 USER 2.2: Separation of duties

11.3.2.1 Requirement

The asset owner shall have policies and procedures related to separation of duties, reducing the privileges assigned to IACS users to the minimum needed.

11.3.2.2 Rationale and supplemental guidance

The separation of duties policies and procedures should use the least privilege principle that states that no user should be given enough privileges to misuse the system on their own. This principle protects the IACS against sabotage, fraud or unintentional mistakes that can damage the system.

IACS users who are logged onto the OS with administrator accounts should not be allowed to access IACS control commands and resources. If such a user does have access to the IACS, then if that user's device becomes infected with malware, the malware will have complete control of the device (for example, engineering workstations or operator stations), and hence access to all control system functions accessible through that device. Therefore, IACS users who require access to the IACS should be logged on to the OS with non-administrative privileges.

11.3.3 USER 2.3: Multiple approvals

11.3.3.1 Requirement

The asset owner shall have policies and procedures to verify that approval by two or more users are required for actions that can result in serious impact to the industrial process, unless failure to perform the action can result in a greater impact to the industrial process.

11.3.3.2 Rationale and supplemental guidance

Certain commands or data changes within the IACS can have significant consequences, including some with HSE implications. In these cases, a risk assessment needs to be conducted to evaluate if the consequences of the changes are serious enough to require authorization of two or more users and to identify if the enforcement of multiple approvals can introduce bigger risk by increasing the probabilities of failure in the timely execution of the operation. See IEC 62443-3-2 for more detail on the use of security assessments within an IACS.

Many IACS components do not always have the capability of enforcing multiple approvals to perform an action. In these cases, compliance with this requirement would need to be policy-driven or enforced via a network management system capable of requiring multiple approvals utilizing different system accounts to perform an action. This ensures verification by a second party (or more) prior to execution of these commands or changes to this data.

Security and HSE assessments should be conducted to identify all commands and data changes that have serious consequences on the IACS. For those that do, ensure that approval by more than one user is required and that this capability is supported by the IACS.

11.3.4 USER 2.4: Manual elevation of privileges

11.3.4.1 Requirement

The asset owner shall have policies and procedures related to requiring explicit elevation of privileges, including supervisor overrides, for all operations that require elevated privileges.

11.3.4.2 Rationale and supplemental guidance

Users who are logged on without administrative privileges perform many operations that do not require elevated privileges. However, there are cases in which they could need to perform operations that require elevated privileges. When they do, it should be noted that they have requested an elevated privilege operation and the operation should be authorized.

Users without the necessary elevated privileges should have a supervisor or another user with the appropriate privileges authorize the operation. This protects against inadvertent execution of privileged operations.

System administrators should ensure that elevated privilege operations are known, and that the system has been configured to notify the user prior to their execution. For example, Microsoft Windows OS employs user account control (UAC) to enforce such controls.

12 SPE 7 – Event and incident management

12.1 Purpose

The requirements in this SPE are defined to support detection, logging and analysis of security-related events and compromises. Such activities are used to identify security-related issues and ensure their non-repudiation.

12.2 EVENT 1 – Event and incident management

12.2.1 EVENT 1.1: Event detection

12.2.1.1 Requirement

The asset owner shall have policies and procedures related to the reporting, logging, analysis and response (immediate or delayed) of IACS security-related events that are detected to support security management activities.

12.2.1.2 Rationale and supplemental guidance

Detecting IACS security-related events allows them to be reported (see 12.2.2, EVENT 1.2: Event reporting), logged (see 12.2.4, EVENT 1.4: Logging) and subsequently analysed (see 12.2.7, EVENT 1.7: Event analysis). It also provides for immediate response, either automatic or manual. Detection can occur through monitoring or through active mechanisms that identify specific security event conditions as they occur. Examples of such conditions include, but are not limited to:

a) valid and invalid login attempts,

b) access to controlled commands and data,

c) OS events,

d) IACS events,

e) backup and restore events,

f) configuration changes, and

g) potential reconnaissance activity and audit log events.

12.2.2 EVENT 1.2: Event reporting

12.2.2.1 Requirement

The asset owner shall have policies and procedures related to reporting IACS security-related events in a timely manner.

12.2.2.2 Rationale and supplemental guidance

Once detected, events should be reported to the appropriate personnel and assigned the appropriate priority for handling to ensure security risk targets are met. Reporting provides awareness of event occurrences and ensures that action can be taken as needed in a timely manner. Timeliness, therefore, is important and is a factor in reducing risks to a tolerable level.

Events should be evaluated to determine who should receive notification, and if supported, their priority. Once that determination is made, the system should be configured to have the events reported appropriately.

12.2.3 EVENT 1.3: Event reporting interfaces

12.2.3.1 Requirement

The asset owner shall have policies and procedures around utilizing interfaces commonly accepted by the industrial and security communities for reporting IACS security-related events.

12.2.3.2 Rationale and supplemental guidance

Using commonly used interfaces to report events, such as OPC alarms and events, allows widespread distribution to a variety of client applications. Such applications are often specialized to provide a richer display, processing, logging and analysis capabilities, making it possible to better understand and respond to events. Using interfaces that are free of known vulnerabilities reduce the attack surface of the IACS.

The event reporting interfaces supported by the IACS should be identified and the appropriate client applications selected for receiving event reports.

12.2.4 EVENT 1.4: Logging

12.2.4.1 Requirement

The asset owner shall have policies and procedures related to writing IACS security-related events to one or more protected event/audit logs and retaining them for an adequate time period.

12.2.4.2 Rationale and supplemental guidance

Logging events is a primary means for reviewing and analysing events. Reviewing events can be used to detect and identify suspicious activities and security violations and to prioritize them. Event analysis, and having an appropriate history of events, can be used to correlate events and to better understand circumstances surrounding event occurrences. All these activities support event response, including determining root causes, and actions taken to minimize impacts and better protect the system from suspicious activities and security violations in the future.

Events should be analysed to determine which events need to be logged, the logs in which they are to be recorded and how long they need to be retained. As part of this exercise, the protections (for example, access controls) provided for the various logs should be determined.

Retaining event/audit logs provides support for forensics. Performing forensic analyses supports identification of root causes and can also identify technical and behavioural vulnerabilities. Therefore, the retention period becomes a factor in reducing risk to a tolerable level and should be selected accordingly.

12.2.5 EVENT 1.5: Log entries

12.2.5.1 Requirement

The asset owner shall have policies and procedures about the information contained in IACS security-related audit and event log entries to support non-repudiation and time-correlated analysis of events.

12.2.5.2 Rationale and supplemental guidance

Having the appropriate information about log entries supports review and analysis. Inadequate information can make it impossible to correctly determine who was associated with event occurrences, the time and order in which events occurred and how to respond to events.

Event analysis needs of the system and organization should be assessed, and a determination made regarding which properties of events should be recorded. Examples of properties include event type, location, time, users (for example, human, software, device) and other event specific parameters and their values.

12.2.6 EVENT 1.6: Log access

12.2.6.1 Requirement

The asset owner shall have policies and procedures around utilizing interfaces commonly accepted by the industrial and security communities to access IACS security-related audit and event logs.

12.2.6.2 Rationale and supplemental guidance

Using commonly used interfaces to access event logs, such as the syslog protocol, allows access by a variety of client applications. Such applications are often specialized to provide a richer display, processing and analysis capabilities, making it possible to better understand and respond to events.

The event log interfaces supported by the IACS should be identified and the appropriate client applications selected for accessing and processing them. Using interfaces that are free of known vulnerabilities reduce the attack surface of the IACS.

NOTE Subclause 12.2.3, EVENT 1.3: Event reporting interfaces, is for reporting events as they occur, such as through OPC alarms and events, while this requirement is for access to logs.

12.2.7 EVENT 1.7: Event analysis

12.2.7.1 Requirement

The asset owner shall have policies and procedures around the analysis of IACS security-related events to identify and characterize attacks, security compromises and security incidents in a timely manner.

12.2.7.2 Rationale and supplemental guidance

Events are analysed for a number of reasons. Two primary reasons are:

a) to identify compromises and suspicious conditions, often achieved by correlation of related events, and

b) to prioritize or rank them with respect to the risk that they pose.

Once IACS security-related events are identified, they are also analysed, often in priority order, to identify conditions surrounding event occurrences with attempts to discover root causes, and to decide how to handle them, including how to protect against their reoccurrence. Event analysis should identify all events that have the potential to support security management activities, such as suspicious activity identification, forensic analysis and immediate response.

Events should be actively reviewed to identify those that represent security violations, and regularly reviewed to detect event patterns that can indicate security violations or suspicious activity. The objective is to be able to identify all actual and potential violations so that appropriate actions can be taken. Once identified, the actual and potential violations should be ranked or prioritized to allow them to be evaluated in priority order.

12.2.8 EVENT 1.8: Incident handling and response

12.2.8.1 Requirement

The asset owner shall have policies and procedures for employing and keeping current a process for evaluating and responding to IACS security-related incidents.

12.2.8.2 Rationale and supplemental guidance

Evaluation of IACS security-related incidents allows the asset owner to determine their impact so that an appropriate response can be developed and implemented. Such evaluations can be performed as a result of a facility event, and evaluations of facility events can determine that the root cause of the facility event was a security incident.

A process for evaluating security incidents should be used that identifies the potential impacts and the threats and vulnerabilities that allowed the incident to occur. Appropriate responses should be developed to reduce the impacts and to apply security measures to close the vulnerabilities and protect the IACS against future threats.

12.2.9 EVENT 1.9: Vulnerability handling

12.2.9.1 Requirement

The asset owner shall have policies and procedures related to identifying, addressing and resolving existing and newly identified IACS vulnerabilities in a timely manner.

12.2.9.2 Rationale and supplemental guidance

Vulnerabilities represent flaws or weaknesses in the IACS architecture, its components and its organizational processes. Subclause 6.3.1, ORG 2.1: Security risk mitigation, addresses handling of known vulnerabilities, while this requirement addresses handling of newly discovered vulnerabilities.

A process for reporting and responding to newly discovered vulnerabilities, both within the IACS and by external means, is a necessary component of risk management. Having a process for addressing and resolving newly discovered vulnerabilities allows them to be factored into the risk management process.

The asset owner should establish a process for reporting and monitoring newly discovered vulnerabilities, whether they are discovered within the organization or by parties external to the organization. This process should route newly identified vulnerabilities to appropriate third parties, such as product suppliers or service providers, as well as responsible entities within the asset owner's organization. The asset owner should also have processes in place for:

a) incorporating the vulnerabilities into its risk management process,

b) determining and ranking potential impacts, and

c) determining an appropriate resolution for newly discovered vulnerabilities.

Resolutions may include fixing the vulnerability, providing mitigating or compensating security measures, deferring the fix or accepting the associated risk and leaving the vulnerability unresolved. Finally, newly identified vulnerabilities should be monitored until the appropriate resolution has been determined.

13 SPE 8 – System integrity and availability

13.1 Purpose

The requirements in this SPE are defined to ensure that the integrity and availability of the IACS are protected, and that the appropriate capabilities are present to recover the system to a previous state when necessary.

13.2 AVAIL 1 – System availability and intended functionality

13.2.1 AVAIL 1.1: Continuity management

13.2.1.1 Requirement

The asset owner shall have policies and procedures related to employing and keeping current a site disaster recovery plan (DRP), business continuity plan (BCP) or both, that includes disaster scenarios, failure handling procedures and processes for maintaining the required level of operational continuity.

13.2.1.2 Rationale and supplemental guidance

Site DRPs and BCPs are developed by asset owners to prepare them to respond appropriately to significant disruptions in their operations. Since cybersecurity attacks have the potential for creating significant disruptions, DRPs and BCPs should be created or updated to address them.

13.2.2 AVAIL 1.2: Resource availability management

13.2.2.1 Requirement

The asset owner shall have policies and procedures related to protecting the IACS from resource/equipment failures due to power disruptions, unintentional capacity/processing overloads, hardware failures and intentional DoS attacks. These policies and procedures shall also consider remediation actions, such as device replacement.

13.2.2.2 Rationale and supplemental guidance

Unintentional power disruptions, capacity/processing overloads and hardware failures can lead to loss or degradation of processing capabilities, resulting in a reduction of availability of the IACS and its components. Likewise, intentional attacks such as DoS have the potential of diminishing usable network bandwidth, processing capabilities and memory resources to a level that can degrade operation of the IACS below tolerable levels. Such DoS attacks can be launched internal to the device or through the network, utilizing malware that consumes processing capabilities, filling up memory, flooding the network (including wireless) with multicast/broadcast traffic, or unicast to a specific target, all of which can degrade or entirely prevent an IACS from operating.

Many techniques, such as redundancy and alarms, can be used in a comprehensive program to limit the impacts of these disruptions, overloads, DoS attacks and ultimately, failure. Segmentation and filtering can limit the impact of such events, and firewalls can be used to prevent unnecessary traffic. Further, protection of the equipment itself from physical tampering and local security attacks should be included in this comprehensive program.

13.2.3 AVAIL 1.3: Failure-state

13.2.3.1 Requirement

The asset owner shall have policies and procedures related to bringing the IACS to a predetermined state if normal operation cannot be maintained as a result of a detected security compromise.

13.2.3.2 Rationale and supplemental guidance

Similar to safety's "fail safe", the IACS should "fail-secure" if a security incident results in a situation where normal operations cannot be maintained. Predetermined state represents a default state that the system enters to protect itself from the compromise. This state is IACS specific and should be determined based on risk to the organization.

Fail-secure should cause the IACS to enter a state that limits further IACS risks, including health, safety and environmental risks.

This could be a manual or automated process.

13.3 AVAIL 2 – Backup/restore/archive

13.3.1 AVAIL 2.1: Backup

13.3.1.1 Requirement

The asset owner shall have policies and procedures related to backing up the IACS at regular intervals to support recovery to a stable state.

13.3.1.2 Rationale and supplemental guidance

Backups taken at regular intervals provide a stored copy of the state of devices, configuration files, recipes and other control system data. Having regular backups allows recovery to a stable, recent state, thus reducing the amount of downtime to make the system operational again. System backups should be stored in a secure location, separated from the location of the original system, and can be done in immutable storage mediums or offline copies to ensure retention.

13.3.2 AVAIL 2.2: Backup non-interference

13.3.2.1 Requirement

The asset owner shall have policies and procedures validating that backup processes do not adversely affect normal operations of the IACS.

13.3.2.2 Rationale and supplemental guidance

Backing up a system or a component has the potential to adversely affect availability. Therefore, their effect on system operation should be considered when developing a backup strategy. Adjusting the backup schedule or selecting different backup software are ways to avoid unacceptable impacts.

13.3.3 AVAIL 2.3: Backup verification

13.3.3.1 Requirement

The asset owner shall have policies and procedures to verify the integrity of backup data at the completion of the backup and periodically after the backup.

13.3.3.2 Rationale and supplemental guidance

Backup data integrity refers to the validity and subsequent usefulness of the backup data to restore the system. Therefore, it is important to know that the backup data is valid and can be used to restore the system. Typically, backup software has an option to validate the backup data at the end of the backup process. When performing a test restoration is not possible, using features within the backup software to validate the backup, reviewing log files for any warnings or errors, or other available means to confirm the health of the backup is required. Subsequent verification is then used to ensure that the backup data has not been corrupted.

13.3.4 AVAIL 2.4: Backup media

13.3.4.1 Requirement

The asset owner shall have policies and procedures around handling and storing backup media in a safe and secure manner to ensure its integrity, authenticity and availability when needed and the confidentiality of the data is maintained.

13.3.4.2 Rationale and supplemental guidance

Backup media are the storage media that contain backup data. They can be kept onsite or offsite. In both cases, they need to be protected against tampering and destruction to ensure that they can be used when needed. Backup media needs to be protected from unauthorized access, as the information contained can provide valuable information for attackers (such as configuration information or potentially also authentication information). The asset owner should also ensure that the backup media can be accessed when needed, and if offsite, transferred back to the site when needed.

13.3.5 AVAIL 2.5: Backup restoration

13.3.5.1 Requirement

The asset owner shall have policies and procedures related to restoring the IACS from a backup to a stable state in a timely manner.

13.3.5.2 Rationale and supplemental guidance

The primary purpose of having backup data is to be prepared to restore the system if necessary. Ensuring that the restore process works as intended is an important part of the SP. Tests should be run periodically to ensure that system changes and changes to the backup/recovery software have not impacted the ability to restore the system. This helps the asset owner be better prepared for situations of widespread outages that require restoration of many systems in a short amount of time.

Timely restoration to a stable state reduces downtime. Timeliness, therefore, is important and is a factor in reducing risks associated with downtime to a tolerable level.

Annex A
(informative)

Cross-references to other standards

A.1 Requirements relationship to IEC 62443-2-4

Table A.1 identifies the requirements in this document that relate to the IEC 62443-2-4 requirements. Where more than one requirement in this document is related to a single IEC 62443-2-4 requirement, multiple rows for that IEC 62443-2-4 requirement are used.

Table A.1 – IEC 62443-2-4 cross-references

IEC 62443-2-4	IEC 62443-2-1
SP.01.01 BR	ORG 1.5
SP.01.01 RE(1)	ORG 1.5
SP.01.02 BR	ORG 1.5
SP.01.02 RE(1)	ORG 1.5
SP.01.03 BR	ORG 1.5
SP.01.03 RE(1)	ORG 1.5
SP.01.04 BR	ORG 1.2
SP.01.04 RE(1)	ORG 1.2
SP.01.05 BR	ORG 1.3
SP.01.06 BR	ORG 1.3
SP.01.07 BR	ORG 1.3
SP.01.07 BR	USER 1.2
SP.02.01 BR	ORG 1.6
SP.02.01 BR	ORG 2.1
SP.02.01BR	ORG 2.3
SP.02.02 BR	ORG 2.2
SP.02.02 RE(1)	ORG 2.2
SP.02.02 RE(2)	ORG 2.2
SP.02.02 RE(3)	ORG 2.2
SP.02.03 BR	COMP 1.1
SP.02.03 RE(1)	COMP 1.1
SP.03.01 BR	ORG 2.1
SP.03.01 RE(1)	ORG 2.1
SP.03.01 RE(2)	ORG 2.1
SP.03.01BR	ORG 2.4
SP.03.02 BR	CM 1.4
SP.03.02 BR	NET 1.1
SP.03.02 BR	NET 1.6
SP.03.02 RE(1)	NET 1.2
SP.03.02 RE(2)	NET 1.1
SP.03.02 RE(2)	NET 1.2
SP.03.02 RE(2)	NET 1.6
SP.03.03 BR	EVENT 1.9
SP.03.03 RE(1)	NET 1.1
SP.03.03 RE(1)	NET 1.2
SP.03.04 BR	NET 1.9
SP.03.05 BR	CM 1.4
SP.03.05 BR	COMP 1.1
SP.03.06 BR	USER 1.18
SP.03.07 BR	NET 1.6
SP.03.07 BR	USER 2.1
SP.03.07 RE(1)	USER 1.9
SP.03.08 BR	USER 1.5
SP.03.08 RE(1)	USER 1.1
SP.03.08 RE(2)	DATA 1.2
SP.03.08 RE(3)	USER 1.10
SP.03.09 BR	CM 1.4
SP.03.10 RE(2)	DATA 1.4
SP.03.10 RE(2)	DATA 1.6
SP.03.10 RE(2)	EVENT 1.4
SP.03.10 RE(3)	DATA 1.5
SP.03.10 RE(3)	DATA 1.6
SP.03.10 RE(4)	COMP 1.1
SP.04.01 BR	NET 2.1
SP.04.02 BR	NET 2.2
SP.04.02 RE(1)	NET 2.2
SP.04.03 BR	NET 2.1
SP.04.03 RE(1)	NET 2.3
SP.04.03 RE(2)	NET 2.3
SP.05.01 BR	NET 1.3
SP.05.02 BR	NET 1.3
SP.05.03 BR	NET 1.3
SP.05.05 BR	NET 1.3
SP.05.05 RE(1)	NET 1.3
SP.05.06 BR	NET 1.3
SP.05.07 BR	NET 1.3
SP.05.08 BR	NET 1.3
SP.05.09 BR	DATA 1.3
SP.05.09 RE(1)	DATA 1.3
SP.05.09 RE(2)	DATA 1.3
SP.06.01 BR	CM 1.2
SP.06.01 RE(1)	CM 1.2
SP.06.02 BR	CM 1.1
SP.06.03	DATA 1.7
SP.06.03 BR	CM 1.3
SP.07.01 BR	NET 3.1
SP.07.02 BR	NET 3.2
SP.07.03 BR	NET 3.2
SP.07.04 BR	CM 1.4
SP.07.04 BR	NET 3.2
SP.08.01 BR	EVENT 1.1
SP.08.01 BR	EVENT 1.2
SP.08.01 BR	EVENT 1.7
SP.08.01 BR	EVENT 1.8
SP.08.01 RE(1)	EVENT 1.3
SP.08.02 BR	EVENT 1.4
SP.08.02 RE(1)	EVENT 1.3
SP.08.02 RE(1)	EVENT 1.6
SP.08.02 RE(2)	EVENT 1.4
SP.08.02 RE(2)	CM 1.4
SP.08.03 BR	EVENT 1.1
SP.08.03 RE(1)	EVENT 1.3
SP.08.04 BR	AVAIL 1.2
SP.09.01 BR	USER 1.1
SP.09.02 BR	USER 1.1
SP.09.02 RE(2)	USER 1.1

IEC 62443-2-4	IEC 62443-2-1
SP.09.02 RE(3)	USER 1.3
SP.09.02 RE(4)	USER 1.2
SP.09.03 BR	USER 1.2
SP.09.04 RE(1)	USER 1.4
SP.09.05 BR	USER 1.11
SP.09.06 BR	USER 1.11
SP.09.06 RE(1)	USER 1.11
SP.09.08 BR	USER 1.11
SP.09.08 RE(1)	USER 1.11
SP.09.09 BR	CM 1.4
SP.09.09 BR	USER 1.12
SP.09.09 RE(1)	USER 1.12
SP.10.01 BR	COMP 2.2
SP.10.02 BR	CM 1.4
SP.10.02 BR	COMP 2.3

IEC 62443-2-4	IEC 62443-2-1
SP.10.02 RE(1)	COMP 2.2
SP.10.03 BR	COMP 2.2
SP.10.05 BR	COMP 2.1
SP.10.05 RE(1)	COMP 1.2
SP.10.05 RE(2)	COMP 2.1
SP.11.01 BR	COMP 3.2
SP.11.01 RE(1)	COMP 3.2
SP.11.02 BR	COMP 3.2
SP.11.02 RE(2)	CM 1.4
SP.11.02 RE(2)	COMP 3.5
SP.11.03 BR	CM 1.4
SP.11.03 BR	COMP 3.1
SP.11.04 BR	COMP 3.2
SP.11.05 BR	COMP 3.2
SP.11.06	DATA 1.7

IEC 62443-2-4	IEC 62443-2-1
SP.11.06 BR	CM 1.4
SP.11.06 RE(1)	COMP 3.4
SP.11.06 RE(2)	COMP 3.1
SP.11.06 RE(3)	COMP 3.3
SP.12.01 BR	AVAIL 2.1
SP.12.02 BR	AVAIL 2.5
SP.12.03 BR	AVAIL 2.4
SP.12.04 BR	AVAIL 2.3
SP.12.05 BR	AVAIL 2.1
SP.12.05 BR	AVAIL 2.5
SP.12.06 BR	AVAIL 2.1
SP.12.07 BR	AVAIL 2.2
SP.12.09 BR	AVAIL 1.1

Table A.2 identifies the requirements in this document that relate to the IEC 62443-2-4 requirements. Where more than one requirement in IEC 62443-2-4 is related to a single IEC 62443-2-1 requirement, multiple rows for that IEC 62443-2-1 requirement are used. If there is no appropriate mapping, the requirement will be followed by a blank entry.

Table A.2 – Cross-reference of IEC 62443-2-1 to IEC 62443-2-4

IEC 62443-2-1	IEC 62443-2-4
ORG 1.1	
ORG 1.2	SP.01.04 BR
ORG 1.2	SP.01.04 RE(1)
ORG 1.3	SP.01.05 BR
ORG 1.3	SP.01.06 BR
ORG 1.3	SP.01.07 BR
ORG 1.4	
ORG 1.5	SP.01.01 BR
ORG 1.5	SP.01.01 RE(1)
ORG 1.5	SP.01.02 BR
ORG 1.5	SP.01.02 RE(1)
ORG 1.5	SP.01.03 BR
ORG 1.5	SP.01.03 RE(1)
ORG 1.6	SP.02.01 BR
ORG 2.1	SP.02.01 BR
ORG 2.1	SP.03.01 BR
ORG 2.1	SP.03.01 RE(1)
ORG 2.1	SP.03.01 RE(2)
ORG 2.2	SP.02.02 BR

IEC 62443-2-1	IEC 62443-2-4
ORG 2.2	SP.02.02 RE(1)
ORG 2.2	SP.02.02 RE(2)
ORG 2.2	SP.02.02 RE(3)
ORG 2.3	SP.02.01BR
ORG 2.4	SP.03.01BR
ORG 3.1	
CM 1.1	SP.06.02 BR
CM 1.2	SP.06.01 BR
CM 1.2	SP.06.01 RE(1)
CM 1.3	SP.06.03 BR
CM 1.4	SP.03.02 BR
CM 1.4	SP.03.05 BR
CM 1.4	SP.03.09 BR
CM 1.4	SP.07.04 BR
CM 1.4	SP.08.02 RE(2)
CM 1.4	SP.09.09 BR
CM 1.4	SP.10.02 BR
CM 1.4	SP.11.02 RE(2)
CM 1.4	SP.11.03 BR

IEC 62443-2-1	IEC 62443-2-4
CM 1.4	SP.11.06 BR
NET 1.1	SP.03.02 BR
NET 1.1	SP.03.02 RE(2)
NET 1.1	SP.03.03 RE(1)
NET 1.2	SP.03.02 RE(1)
NET 1.2	SP.03.02 RE(2)
NET 1.2	SP.03.03 RE(1)
NET 1.3	SP.05.01 BR
NET 1.3	SP.05.02 BR
NET 1.3	SP.05.03 BR
NET 1.3	SP.05.05 BR
NET 1.3	SP.05.05 RE(1)
NET 1.3	SP.05.06 BR
NET 1.3	SP.05.07 BR
NET 1.3	SP.05.08 BR
NET 1.4	
NET 1.5	
NET 1.6	SP.03.02 BR
NET 1.6	SP.03.02 RE(2)

IEC 62443-2-1	IEC 62443-2-4
NET 1.6	SP.03.07 BR
NET 1.7	
NET 1.8	
NET 1.9	SP.03.04 BR
NET 2.1	SP.04.01 BR
NET 2.1	SP.04.03 BR
NET 2.2	SP.04.02 BR
NET 2.2	SP.04.02 RE(1)
NET 2.3	SP.04.03 RE(1)
NET 2.3	SP.04.03 RE(2)
NET 3.1	SP.07.01 BR
NET 3.2	SP.07.02 BR
NET 3.2	SP.07.03 BR
NET 3.2	SP.07.04 BR
NET 3.3	
COMP 1.1	SP.02.03 BR
COMP 1.1	SP.02.03 RE(1)
COMP 1.1	SP.03.05 BR
COMP 1.1	SP.03.10 RE(4)
COMP 1.2	SP.10.05 RE(1)
COMP 2.1	SP.10.05 BR
COMP 2.1	SP.10.05 RE(2)
COMP 2.2	SP.10.01 BR
COMP 2.2	SP.10.02 RE(1)
COMP 2.2	SP.10.03 BR
COMP 2.3	SP.10.02 BR
COMP 3.1	SP.11.03 BR
COMP 3.1	SP.11.06 RE(2)
COMP 3.2	SP.11.01 BR
COMP 3.2	SP.11.01 RE(1)
COMP 3.2	SP.11.02 BR
COMP 3.2	SP.11.04 BR
COMP 3.2	SP.11.05 BR
COMP 3.3	SP.11.06 RE(3)
COMP 3.4	SP.11.06 RE(1)
COMP 3.5	SP.11.02 RE(2)
DATA 1.1	
DATA 1.2	SP.03.08 RE(2)
DATA 1.3	SP.05.09 BR
DATA 1.3	SP.05.09 RE(1)
DATA 1.3	SP.05.09 RE(2)
DATA 1.4	SP.03.10 RE(2)
DATA 1.5	SP.03.10 RE(3)

IEC 62443-2-1	IEC 62443-2-4
DATA 1.6	SP.03.10 RE(2)
DATA 1.6	SP.03.10 RE(3)
DATA 1.7	SP.06.03
DATA 1.7	SP.11.06
USER 1.1	SP.03.08 RE(1)
USER 1.1	SP.09.01 BR
USER 1.1	SP.09.02 BR
USER 1.1	SP.09.02 RE(2)
USER 1.2	SP.01.07 BR
USER 1.2	SP.09.02 RE(4)
USER 1.2	SP.09.03 BR
USER 1.3	SP.09.02 RE(3)
USER 1.4	SP.09.04 RE(1)
USER 1.5	SP.03.08 BR
USER 1.6	
USER 1.7	
USER 1.8	
USER 1.9	SP.03.07 RE(1)
USER 1.10	SP.03.08 RE(3)
USER 1.11	SP.09.05 BR
USER 1.11	SP.09.06 BR
USER 1.11	SP.09.06 RE(1)
USER 1.11	SP.09.08 BR
USER 1.11	SP.09.08 RE(1)
USER 1.12	SP.09.09 BR
USER 1.12	SP.09.09 RE(1)
USER 1.13	
USER 1.14	
USER 1.15	
USER 1.16	
USER 1.17	
USER 1.18	SP.03.06 BR
USER 1.19	
USER 2.1	SP.03.07 BR
USER 2.2	
USER 2.3	
USER 2.4	
EVENT 1.1	SP.08.01 BR
EVENT 1.1	SP.08.03 BR
EVENT 1.2	SP.08.01 BR
EVENT 1.3	SP.08.01 RE(1)
EVENT 1.3	SP.08.02 RE(1)
EVENT 1.3	SP.08.03 RE(1)

IEC 62443-2-1	IEC 62443-2-4
EVENT 1.4	SP.03.10 RE(2)
EVENT 1.4	SP.08.02 BR
EVENT 1.4	SP.08.02 RE(2
EVENT 1.5	
EVENT 1.6	SP.08.02 RE(1)
EVENT 1.7	SP.08.01 BR
EVENT 1.8	SP.08.01 BR
EVENT 1.9	SP.03.03 BR
AVAIL 1.1	SP.12.09 BR
AVAIL 1.2	SP.08.04 BR
AVAIL 1.3	
AVAIL 2.1	SP.12.01 BR
AVAIL 2.1	SP.12.05 BR
AVAIL 2.1	SP.12.06 BR
AVAIL 2.2	SP.12.07 BR
AVAIL 2.3	SP.12.04 BR
AVAIL 2.4	SP.12.03 BR
AVAIL 2.5	SP.12.02 BR
AVAIL 2.5	SP.12.05 BR
EVENT 1.2	SP.08.01 BR
EVENT 1.3	SP.08.01 RE(1)
EVENT 1.3	SP.08.02 RE(1)
EVENT 1.3	SP.08.03 RE(1)
EVENT 1.4	SP.03.10 RE(2)
EVENT 1.4	SP.08.02 BR
EVENT 1.4	SP.08.02 RE(2)
EVENT 1.5	
EVENT 1.6	SP.08.02 RE(1)
EVENT 1.7	SP.08.01 BR
EVENT 1.8	SP.08.01 BR
EVENT 1.9	SP.03.03 BR
AVAIL 1.1	SP.12.09 BR
AVAIL 1.2	SP.08.04 BR
AVAIL 1.3	
AVAIL 2.1	SP.12.01 BR
AVAIL 2.1	SP.12.05 BR
AVAIL 2.1	SP.12.06 BR
AVAIL 2.2	SP.12.07 BR
AVAIL 2.3	SP.12.04 BR
AVAIL 2.4	SP.12.03 BR
AVAIL 2.5	SP.12.02 BR
AVAIL 2.5	SP.12.05 BR

A.2 Requirements relationship to IEC 62443-3-3

Table A.3 identifies the requirements in this document that relate to the IEC 62443-3-3 requirements. Where more than one requirement in this document is related to a single IEC 62443-3-3 requirement, multiple rows for that IEC 62443-3-3 requirement are used.

Table A.3 – IEC 62443-3-3 cross-references

IEC 62443-3-3	IEC 62443-2-1
SR 1.1 BR	USER 1.8
SR 1.1 RE(1)	USER 1.1
SR 1.1 RE(2)	USER 1.9
SR 1.2 BR	USER 1.6
SR 1.2 BR	USER 1.19
SR 1.2 BR	NET 1.7
SR 1.3 BR	USER 1.2
SR 1.4 BR	USER 1.1
SR 1.5 BR	DATA 1.6
SR 1.5 BR	USER 1.1
SR 1.6 BR	USER 1.8
SR 1.6 RE(1)	USER 1.1
SR 1.7 BR	USER 1.11
SR 1.7 RE(1)	USER 1.11
SR 1.7 RE(2)	USER 1.11
SR 1.11 BR	USER 1.15
SR 1.13 BR	NET 1.6
SR 1.13 BR	NET 3.1
SR 1.13 BR	NET 3.2
SR 2.1 BR	USER 1.4
SR 2.1 BR	USER 2.1
SR 2.1 BR	USER 2.2
SR 2.1 RE(1)	USER 2.1
SR 2.1 RE(2)	USER 1.5
SR 2.1 RE(3)	USER 2.4
SR 2.1 RE(4)	USER 2.3
SR 2.2 BR	NET 2.2
SR 2.3 BR	NET 1.7
SR 2.3 BR	USER 1.19
SR 2.3 BR	USER 2.1
SR 2.3 RE(1)	NET 1.7
SR 2.3 RE(1)	USER 1.19
SR 2.3 RE(1)	USER 2.1
SR 2.4 BR	USER 1.5
SR 2.4 RE(1)	USER 1.6
SR 2.5 BR	USER 1.18
SR 2.6 BR	NET 3.3
SR 2.7 BR	USER 1.17
SR 2.8 BR	EVENT 1.1
SR 2.8 BR	EVENT 1.4
SR 2.8 BR	EVENT 1.5
SR 2.8 RE(1)	EVENT 1.4
SR 2.8 RE(1)	EVENT 1.6
SR 2.9 BR	EVENT 1.4
SR 2.9 RE(1)	EVENT 1.1
SR 2.9 RE(1)	EVENT 1.2
SR 2.10 BR	EVENT 1.1
SR 2.11 BR	NET 1.9
SR 2.11 RE(1)	NET 1.9
SR 2.11 RE(2)	NET 1.9
SR 2.12 BR	EVENT 1.5
SR 2.12 RE(1)	EVENT 1.5
SR 3.1 BR	DATA 1.7
SR 3.1 RE(1)	DATA 1.7
SR 3.2 BR	COMP 2.2
SR 3.2 RE(1)	COMP 2.2
SR 3.2 RE(2)	COMP 2.2
SR 3.3 BR	ORG 2.2
SR 3.3 RE(1)	ORG 2.2
SR 3.3 RE(2)	ORG 2.2
SR 3.4 BR	DATA 1.7
SR 3.4 BR	CM 1.4
SR 3.4 RE(1)	ORG 2.2
SR 3.6 BR	AVAIL 1.3
SR 3.8 BR	USER 1.16
SR 3.8 RE(1)	USER 1.16
SR 3.8 RE(2)	USER 1.16
SR 3.8 RE(3)	USER 1.16
SR 3.9 BR	DATA 1.1
SR 3.9 BR	DATA 1.7
SR 3.9 RE(1)	DATA 1.1
SR 3.9 RE(1)	DATA 1.7
SR 4.1 BR	DATA 1.2
SR 4.1 RE(1)	DATA 1.2
SR 4.1 RE(2)	DATA 1.2
SR 4.2 BR	DATA 1.4
SR 4.2 RE(1)	DATA 1.4
SR 4.3 BR	DATA 1.5
SR 5.1 BR	NET 1.1
SR 5.1 RE(1)	NET 1.1
SR 5.1 RE(2)	NET 1.1
SR 5.1 RE(3)	NET 1.1
SR 5.2 BR	NET 1.1
SR 5.2 BR	NET 1.6
SR 5.2 BR	NET 2.2
SR 5.2 RE(1)	NET 1.1
SR 5.2 RE(1)	NET 1.6
SR 5.2 RE(2)	NET 1.4
SR 5.2 RE(3)	NET 1.5
SR 5.3 BR	NET 1.8
SR 5.3 RE(1)	NET 1.8
SR 5.4 BR	NET 1.1
SR 6.1 BR	EVENT 1.6
SR 6.1 RE(1)	EVENT 1.6
SR 6.2 BR	EVENT 1.1
SR 6.2 BR	EVENT 1.2
SR 6.2 BR	EVENT 1.3
SR 6.2 BR	EVENT 1.4
SR 7.1 BR	AVAIL 1.2
SR 7.1 RE(1)	AVAIL 1.2
SR 7.1 RE(2)	AVAIL 1.2
SR 7.2 BR	AVAIL 1.2
SR 7.3 BR	AVAIL 2.1
SR 7.3 BR	AVAIL 2.2
SR 7.3 RE(1)	AVAIL 2.1
SR 7.3 RE(1)	AVAIL 2.3
SR 7.3 RE(2)	AVAIL 2.1
SR 7.4 BR	DATA 1.4
SR 7.4 BR	AVAIL 2.5
SR 7.5 BR	AVAIL 1.2
SR 7.6 BR	CM 1.3

IEC 62443-3-3	IEC 62443-2-1
SR 7.6 RE(1)	CM 1.3
SR 7.7 BR	COMP 1.1

IEC 62443-3-3	IEC 62443-2-1
SR 7.8 BR	CM 1.1

Table A.4 identifies the requirements in this document that relate to the IEC 62443-3-3 requirements. Where more than one requirement in IEC 62443-3-3 is related to a single IEC 62443-2-1 requirement, multiple rows for that IEC 62443-2-1 requirement are used. If there is no appropriate mapping, the requirement will be followed by a blank entry.

Table A.4 – Cross-reference of IEC 62443-2-1 to IEC 62443-3-3

IEC-62443-2-1	IEC-62443-3-3
ORG 1.1	
ORG 1.2	
ORG 1.3	
ORG 1.4	
ORG 1.5	
ORG 1.6	
ORG 2.1	
ORG 2.2	SR 3.3 BR
ORG 2.2	SR 3.3 RE(1)
ORG 2.2	SR 3.3 RE(2)
ORG 2.2	SR 3.4 RE(1)
ORG 2.3	
ORG 2.4	
ORG 3.1	
CM 1.1	SR 7.8 BR
CM 1.2	
CM 1.3	SR 7.6 BR
CM 1.3	SR 7.6 RE(1)
CM 1.4	SR 3.4 BR
NET 1.1	SR 5.1 BR
NET 1.1	SR 5.1 RE(1)
NET 1.1	SR 5.1 RE(2)
NET 1.1	SR 5.1 RE(3)
NET 1.1	SR 5.2 BR
NET 1.1	SR 5.2 RE(1)
NET 1.1	SR 5.4 BR
NET 1.2	
NET 1.3	
NET 1.4	SR 5.2 RE(2)
NET 1.5	SR 5.2 RE(3)
NET 1.6	SR 1.13 BR
NET 1.6	SR 1.13 RE(1)
NET 1.6	SR 5.2 BR
NET 1.6	SR 5.2 RE(1)

IEC-62443-2-1	IEC-62443-3-3
NET 1.7	SR 1.2
NET 1.7	SR 1.2 RE (1)
NET 1.7	SR 2.3
NET 1.7	SR 2.3 RE (1)
NET 1.8	SR 5.3 BR
NET 1.8	SR 5.3 RE(1)
NET 1.9	SR 2.11 BR
NET 1.9	SR 2.11 RE(1)
NET 1.9	SR 2.11 RE(2)
NET 2.1	
NET 2.2	SR 2.2 BR
NET 2.2	SR 5.2 BR
NET 2.3	
NET 3.1	SR 1.13
NET 3.2	SR 1.13
NET 3.3	SR 2.6 BR
COMP 1.1	SR 7.7 BR
COMP 1.2	
COMP 2.1	
COMP 2.2	SR 3.2 BR
COMP 2.2	SR 3.2 RE(1)
COMP 2.2	SR 3.2 RE(2)
COMP 2.3	
COMP 3.1	
COMP 3.2	
COMP 3.3	
COMP 3.4	
COMP 3.5	
DATA 1.1	SR 3.9 BR
DATA 1.1	SR 3.9 RE(1)
DATA 1.2	SR 4.1 BR
DATA 1.2	SR 4.1 RE(1)
DATA 1.2	SR 4.1 RE(2)
DATA 1.3	

IEC-62443-2-1	IEC-62443-3-3
DATA 1.4	SR 4.2 BR
DATA 1.4	SR 4.2 RE(1)
DATA 1.4	SR 7.4
DATA 1.5	SR 4.3 BR
DATA 1.6	SR 1.5 BR
DATA 1.7	SR 3.1 BR
DATA 1.7	SR 3.1 RE(1)
DATA 1.7	SR 3.4 BR
DATA 1.7	SR 3.9 BR
DATA 1.7	SR 3.9 RE(1)
USER 1.1	SR 1.1 RE(1)
USER 1.1	SR 1.2 RE(1)
USER 1.1	SR 1.3 BR
USER 1.1	SR 1.3 RE(1)
USER 1.1	SR 1.4 BR
USER 1.1	SR 1.5 BR
USER 1.1	SR 1.6 RE(1)
USER 1.2	SR 1.3 BR
USER 1.3	
USER 1.4	SR 2.1 BR
USER 1.5	SR 2.1 RE(2)
USER 1.5	SR 2.4 BR
USER 1.6	SR 1.2 BR
USER 1.6	SR 2.4 RE(1)
USER 1.7	
USER 1.8	SR 1.1 BR
USER 1.8	SR 1.6 BR
USER 1.9	SR 1.1 RE(2)
USER 1.9	SR 1.1 RE(3)
USER 1.10	
USER 1.11	SR 1.7 BR
USER 1.11	SR 1.7 RE(1)
USER 1.11	SR 1.7 RE(2)
USER 1.12	

IEC-62443-2-1	IEC-62443-3-3
USER 1.13	
USER 1.14	
USER 1.15	SR 1.11 BR
USER 1.16	SR 3.8 BR
USER 1.16	SR 3.8 RE(1)
USER 1.16	SR 3.8 RE(2)
USER 1.16	SR 3.8 RE(3)
USER 1.17	SR 2.7 BR
USER 1.18	SR 2.5 BR
USER 1.19	SR 1.2 BR
USER 1.19	SR 1.2 RE(1)
USER 1.19	SR 2.3 BR
USER 1.19	SR 2.3 RE(1)
USER 2.1	SR 2.1 BR
USER 2.1	SR 2.1 RE(1)
USER 2.1	SR 2.3
USER 2.1	SR 2.3 RE(1)
USER 2.2	SR 2.1 BR
USER 2.3	SR 2.1 RE(4)

IEC-62443-2-1	IEC-62443-3-3
USER 2.4	SR 2.1 RE(3)
EVENT 1.1	SR 2.8 BR
EVENT 1.1	SR 2.9 RE(1)
EVENT 1.1	SR 2.10 BR
EVENT 1.1	SR 6.2 BR
EVENT 1.2	SR 2.9 RE(1)
EVENT 1.2	SR 6.2 BR
EVENT 1.3	SR 6.2 BR
EVENT 1.4	SR 2.8 BR
EVENT 1.4	SR 2.8 RE(1)
EVENT 1.4	SR 2.9
EVENT 1.4	SR 6.2 BR
EVENT 1.5	SR 2.8 BR
EVENT 1.5	SR 2.12 BR
EVENT 1.5	SR 2.12 RE(1)
EVENT 1.6	SR 2.8 RE(1)
EVENT 1.6	SR 6.1 RE(1)
EVENT 1.7	
EVENT 1.8	

IEC-62443-2-1	IEC-62443-3-3
EVENT 1.9	
AVAIL 1.1	
AVAIL 1.2	SR 7.1 BR
AVAIL 1.2	SR 7.1 RE(1)
AVAIL 1.2	SR 7.1 RE(2)
AVAIL 1.2	SR 7.2 BR
AVAIL 1.2	SR 7.5 BR
AVAIL 1.3	SR 3.6 BR
AVAIL 2.1	SR 7.3
AVAIL 2.1	SR 7.3 RE(1)
AVAIL 2.1	SR 7.3 RE(2)
AVAIL 2.2	SR 7.3 BR
AVAIL 2.3	SR 7.3 RE(1)
AVAIL 2.4	
AVAIL 2.5	SR 7.4 BR

A.3 Requirements relationship to IEC 62443-4-2

Table A.5 identifies the requirements in this document that relate to the IEC 62443-4-2 requirements. Where more than one requirement in this document is related to a single IEC 62443-4-2 requirement, multiple rows for that IEC 62443-4-2 requirement are used.

Table A.5 – IEC 62443-4-2 cross-references

IEC 62443-4-2	IEC 62443-2-1
CCSC 1	USER 1.3
CCSC 3	USER 1.5
CCSC 4	ORG 2.3
CR 1.1 BR	USER 1.8
CR 1.1 RE(1)	USER 1.1
CR 1.1 RE(2)	USER 1.9
CR 1.2 BR	USER 1.6
CR 1.2 BR	USER 1.19
CR 1.2 RE(1)	USER 1.1
CR 1.2 RE(1)	USER 1.19
CR 1.3 BR	USER 1.1
CR 1.3 BR	USER 1.2
CR 1.4 BR	USER 1.1
CR 1.5 BR	DATA 1.6
CR 1.5 BR	USER 1.1
CR 1.7 BR	USER 1.11

IEC 62443-4-2	IEC 62443-2-1
CR 1.7 RE(1)	USER 1.11
CR 1.7 RE(2)	USER 1.11
CR 1.11 BR	USER 1.15
CR 1.14 BR	DATA 1.1
CR 1.14 BR	DATA 1.2
CR 1.14 BR	DATA 1.5
CR 1.14 RE(1)	DATA 1.1
CR 1.14 RE(1)	DATA 1.2
CR 2.1 BR	USER 1.4
CR 2.1 BR	USER 2.1
CR 2.1 RE(1)	USER 2.1
CR 2.1 RE(2)	USER 1.5
CR 2.1 RE(3)	USER 2.4
CR 2.1 RE(4)	USER 2.3
CR 2.2 BR	NET 2.2
CR 2.5 BR	USER 1.18

IEC 62443-4-2	IEC 62443-2-1
CR 2.6 BR	NET 3.3
CR 2.7 BR	USER 1.17
CR 2.8 BR	EVENT 1.1
CR 2.8 BR	EVENT 1.4
CR 2.8 BR	EVENT 1.5
CR 2.9 BR	EVENT 1.4
CR 2.9 RE(1)	EVENT 1.1
CR 2.10 BR	EVENT 1.1
CR 2.11 BR	NET 1.9
CR 2.11 RE(1)	NET 1.9
CR 2.11 RE(2)	NET 1.9
CR 2.12 BR	EVENT 1.5
CR 2.12 RE(1)	EVENT 1.5
CR 3.1 BR	DATA 1.7
CR 3.1 RE(1)	DATA 1.7
CR 3.3 BR	ORG 2.2

IEC 62443-4-2	IEC 62443-2-1
CR 3.3 RE(1)	ORG 2.2
CR 3.4 BR	CM 1.4
CR 3.4 BR	DATA 1.7
CR 3.4 RE(1)	ORG 2.2
CR 3.6 BR	AVAIL 1.3
CR 3.8 BR	USER 1.16
CR 3.9 BR	DATA 1.1
CR 3.9 BR	DATA 1.7
CR 3.9 RE(1)	DATA 1.1
CR 3.9 RE(1)	DATA 1.7
CR 4.1 BR	DATA 1.2
CR 4.2 BR	DATA 1.4
CR 4.2 RE(1)	DATA 1.4
CR 4.3 BR	DATA 1.5
CR 5.1 BR	NET 1.1
CR 6.1 BR	EVENT 1.6
CR 6.1 RE(1)	EVENT 1.6
CR 6.2 BR	EVENT 1.1
CR 6.2 BR	EVENT 1.2
CR 6.2 BR	EVENT 1.3
CR 6.2 BR	EVENT 1.4
CR 7.1 BR	AVAIL 1.2
CR 7.1 RE(1)	AVAIL 1.2
CR 7.2 BR	AVAIL 1.2
CR 7.3	AVAIL 2.1
CR 7.3 BR	AVAIL 2.2
CR 7.3 RE(1)	AVAIL 2.1
CR 7.3 RE(1)	AVAIL 2.3
CR 7.4	DATA 1.4
CR 7.4 BR	AVAIL 2.5
CR 7.6 BR	CM 1.3
CR 7.6 RE(1)	CM 1.3
CR 7.7 BR	COMP 1.1
CR 7.8 BR	CM 1.1
EDR 2.4 BR	USER 1.5
EDR 2.4 RE(1)	USER 1.6
EDR 2.13 BR	COMP 1.1
EDR 2.13 RE(1)	EVENT 1.1

IEC 62443-4-2	IEC 62443-2-1
EDR 3.2 BR	COMP 2.2
EDR 3.10 BR	COMP 1.1
EDR 3.10 RE(1)	CM 1.4
EDR 3.10 RE(1)	COMP 3.1
EDR 3.11 BR	COMP 1.1
EDR 3.11 BR	ORG 3.1
EDR 3.11 RE(1)	ORG 3.1
EDR 3.11 RE(1)	EVENT 1.2
EDR 3.11 RE(1)	EVENT 1.4
EDR 3.12 BR	DATA 1.1
EDR 3.12 BR	DATA 1.7
EDR 3.13 BR	DATA 1.1
EDR 3.13 BR	DATA 1.7
EDR 3.14 BR	DATA 1.1
EDR 3.14 BR	DATA 1.7
EDR 3.14 RE(1)	DATA 1.7
HDR 2.4 BR	USER 1.5
HDR 2.4 RE(1)	USER 1.6
HDR 2.13 BR	COMP 1.1
HDR 2.13 RE(1)	EVENT 1.1
HDR 3.2 BR	COMP 2.2
HDR 3.2 RE(1)	COMP 2.2
HDR 3.10 BR	COMP 1.1
HDR 3.10 RE(1)	CM 1.4
HDR 3.10 RE(1)	COMP 3.1
HDR 3.11 BR	COMP 1.1
HDR 3.11 BR	ORG 3.1
HDR 3.11 RE(1)	EVENT 1.2
HDR 3.11 RE(1)	EVENT 1.4
HDR 3.11 RE(1)	ORG 3.1
HDR 3.12 BR	DATA 1.1
HDR 3.12 BR	DATA 1.7
HDR 3.13 BR	DATA 1.1
HDR 3.13 BR	DATA 1.7
HDR 3.14 BR	DATA 1.1
HDR 3.14 BR	DATA 1.7
HDR 3.14 RE(1)	DATA 1.7
NDR 1.6 BR	USER 1.8

IEC 62443-4-2	IEC 62443-2-1
NDR 1.6 RE(1)	USER 1.1
NDR 1.13 BR	NET 1.1
NDR 1.13 BR	NET 1.6
NDR 1.13 RE(1)	NET 1.1
NDR 1.13 RE(1)	NET 1.6
NDR 2.4 BR	USER 1.5
NDR 2.4 RE(1)	USER 1.6
NDR 2.13 BR	COMP 1.1
NDR 2.13 RE(1)	EVENT 1.2
NDR 3.2 BR	COMP 2.2
NDR 3.10 BR	COMP 1.1
NDR 3.10 RE(1)	CM 1.4
NDR 3.10 RE(1)	COMP 3.1
NDR 3.11 BR	COMP 1.1
NDR 3.11 BR	ORG 3.1
NDR 3.11 RE(1)	EVENT 1.2
NDR 3.11 RE(1)	EVENT 1.4
NDR 3.11 RE (1)	ORG 3.1
NDR 3.12 BR	DATA 1.1
NDR 3.12 BR	DATA 1.7
NDR 3.13 BR	DATA 1.1
NDR 3.13 BR	DATA 1.7
NDR 3.14 BR	DATA 1.1
NDR 3.14 BR	DATA 1.7
NDR 3.14 RE(1)	DATA 1.7
NDR 5.2 BR	NET 1.1
NDR 5.2 BR	NET 1.6
NDR 5.2 RE(1)	NET 1.1
NDR 5.2 RE(1)	NET 1.6
NDR 5.2 RE(2)	NET 1.4
NDR 5.2 RE(3)	NET 1.5
NDR 5.3 BR	NET 1.8
SAR 2.4 BR	USER 1.5
SAR 2.4 RE(1)	USER 1.6
SAR 3.2 BR	COMP 2.2

Table A.6 identifies the requirements in this document that relate to the IEC 62443-4-2 requirements. Where more than one requirement in IEC 62443-4-2 is related to a single IEC 62443-2-1 requirement, multiple rows for that IEC 62443-2-1 requirement are used. If there is no appropriate mapping, the requirement will be followed by a blank entry.

Table A.6 – Cross-reference of IEC 62443-2-1 to IEC 62443-4-2

IEC 62443-2-1	IEC 62443-4-2
ORG 1.1	
ORG 1.2	
ORG 1.3	
ORG 1.4	
ORG 1.5	
ORG 1.6	
ORG 2.1	
ORG 2.2	CR 3.3 BR
ORG 2.2	CR 3.3 RE(1)
ORG 2.2	CR 3.4 RE(1)
ORG 2.3	CCSC 4
ORG 2.4	
ORG 3.1	EDR 3.11 BR
ORG 3.1	EDR 3.11 RE(1)
ORG 3.1	HDR 3.11 BR
ORG 3.1	HDR 3.11 RE(1)
ORG 3.1	NDR 3.11
ORG 3.1	NDR 3.11 RE(1)
CM 1.1	CR 7.8 BR
CM 1.2	
CM 1.3	CR 7.6 BR
CM 1.3	CR 7.6 RE(1)
CM 1.4	CR 3.4 BR
CM 1.4	EDR 3.10 RE(1)
CM 1.4	HDR 3.10 RE(1)
CM 1.4	NDR 3.10 RE(1)
NET 1.1	CR 5.1 BR
NET 1.1	NDR 1.13 BR
NET 1.1	NDR 1.13 RE(1)
NET 1.1	NDR 5.2 BR
NET 1.1	NDR 5.2 RE(1)
NET 1.2	
NET 1.3	
NET 1.4	NDR 5.2 RE(2)
NET 1.5	NDR 5.2 RE(3)
NET 1.6	NDR 1.13
NET 1.6	NDR 1.13 RE(1)
NET 1.6	NDR 5.2 BR
NET 1.6	NDR 5.2 RE(1)
NET 1.7	
NET 1.8	NDR 5.3 BR
NET 1.9	CR 2.11 BR
NET 1.9	CR 2.11 RE(1)
NET 1.9	CR 2.11 RE(2)
NET 2.1	
NET 2.2	CR 2.2 BR
NET 2.3	
NET 3.1	
NET 3.2	
NET 3.3	
COMP 1.1	CR 7.7 BR
COMP 1.1	EDR 2.13 BR
COMP 1.1	EDR 3.10 BR
COMP 1.1	EDR 3.11 BR
COMP 1.1	HDR 2.13 BR
COMP 1.1	HDR 3.10 BR
COMP 1.1	HDR 3.11 BR
COMP 1.1	NDR 2.13 BR
COMP 1.1	NDR 3.10 BR
COMP 1.1	NDR 3.11 BR
COMP 1.2	
COMP 2.1	
COMP 2.2	SAR 3.2 BR
COMP 2.2	EDR 3.2 BR
COMP 2.2	HDR 3.2 BR
COMP 2.2	HDR 3.2 RE(1)
COMP 2.2	NDR 3.2 BR
COMP 2.3	
COMP 3.1	EDR 3.10 RE(1)
COMP 3.1	HDR 3.10 RE(1)
COMP 3.1	NDR 3.10 RE(1)
COMP 3.2	
COMP 3.3	
COMP 3.4	
COMP 3.5	
DATA 1.1	CR 1.14 BR
DATA 1.1	CR 1.14 RE(1)
DATA 1.1	CR 3.9 BR
DATA 1.1	CR 3.9 RE(1)
DATA 1.1	EDR 3.12 BR
DATA 1.1	EDR 3.13 BR
DATA 1.1	EDR 3.14 BR
DATA 1.1	HDR 3.12 BR
DATA 1.1	HDR 3.13 BR
DATA 1.1	HDR 3.14 BR
DATA 1.1	NDR 3.12 BR
DATA 1.1	NDR 3.13 BR
DATA 1.1	NDR 3.14 BR
DATA 1.2	CR 1.14 BR
DATA 1.2	CR 1.14 RE(1)
DATA 1.2	CR 4.1 BR
DATA 1.3	
DATA 1.4	CR 4.2 BR
DATA 1.4	CR 4.2 RE(1)
DATA 1.4	CR 7.4 BR
DATA 1.5	CR 1.14 BR
DATA 1.5	CR 4.3 BR
DATA 1.6	CR 1.5 BR
DATA 1.7	CR 3.1 BR
DATA 1.7	CR 3.1 RE(1)
DATA 1.7	CR 3.4 BR
DATA 1.7	CR 3.9 BR
DATA 1.7	CR 3.9 RE(1)
DATA 1.7	EDR 3.12 BR
DATA 1.7	EDR 3.13 BR
DATA 1.7	EDR 3.14 BR
DATA 1.7	EDR 3.14 RE(1)
DATA 1.7	HDR 3.12 BR
DATA 1.7	HDR 3.13 BR
DATA 1.7	HDR 3.14 BR
DATA 1.7	HDR 3.14 RE(1)
DATA 1.7	NDR 3.12 BR
DATA 1.7	NDR 3.13 BR
DATA 1.7	NDR 3.14 BR
DATA 1.7	NDR 3.14 RE(1)
USER 1.1	CR 1.1 RE(1)
USER 1.1	CR 1.2 RE(1)
USER 1.1	CR 1.3 BR
USER 1.1	CR 1.4 BR
USER 1.1	CR 1.5 BR
USER 1.1	NDR 1.6 RE(1)
USER 1.2	CR 1.3 BR
USER 1.3	CCSC 1
USER 1.4	CR 2.1 BR
USER 1.5	CCSC 3
USER 1.5	CR 2.1 RE(2)

IEC 62443-2-1	IEC 62443-4-2
USER 1.5	SAR 2.4 BR
USER 1.5	EDR 2.4 BR
USER 1.5	HDR 2.4 BR
USER 1.5	NDR 2.4 BR
USER 1.6	CR 1.2 BR
USER 1.6	SAR 2.4 RE(1)
USER 1.6	EDR 2.4 RE(1)
USER 1.6	HDR 2.4 RE(1)
USER 1.6	NDR 2.4 RE(1)
USER 1.7	
USER 1.8	CR 1.1 BR
USER 1.8	NDR 1.6 BR
USER 1.9	CR 1.1 RE(2)
USER 1.10	
USER 1.11	CR 1.7 BR
USER 1.11	CR 1.7 RE(1)
USER 1.11	CR 1.7 RE(2)
USER 1.12	
USER 1.13	
USER 1.14	
USER 1.15	CR 1.11 BR
USER 1.16	CR 3.8 BR
USER 1.17	CR 2.7 BR

IEC 62443-2-1	IEC 62443-4-2
USER 1.18	CR 2.5 BR
USER 1.19	CR 1.2 BR
USER 1.19	CR 1.2 RE(1)
USER 2.1	CR 2.1 BR
USER 2.1	CR 2.1 RE(1)
USER 2.2	
USER 2.3	CR 2.1 RE(4)
USER 2.4	CR 2.1 RE(3)
EVENT 1.1	CR 2.8 BR
EVENT 1.1	CR 2.9 RE(1)
EVENT 1.1	CR 2.10 BR
EVENT 1.1	CR 6.2 BR
EVENT 1.1	EDR 2.13 RE(1)
EVENT 1.1	HDR 2.13 RE(1)
EVENT 1.2	NDR 2.13 RE(1)
EVENT 1.2	CR 6.2 BR
EVENT 1.2	EDR 3.11 RE(1)
EVENT 1.2	HDR 3.11 RE(1)
EVENT 1.2	NDR 3.11 RE(1)
EVENT 1.3	CR 6.2 BR
EVENT 1.4	CR 2.8 BR
EVENT 1.4	CR 2.9 BR
EVENT 1.4	CR 6.2 BR

IEC 62443-2-1	IEC 62443-4-2
EVENT 1.4	EDR 3.11 RE(1)
EVENT 1.4	HDR 3.11 RE(1)
EVENT 1.4	NDR 3.11 RE(1)
EVENT 1.5	CR 2.8 BR
EVENT 1.5	CR 2.12 BR
EVENT 1.5	CR 2.12 RE(1)
EVENT 1.6	CR 6.1 RE(1)
EVENT 1.7	
EVENT 1.8	
EVENT 1.9	
AVAIL 1.1	
AVAIL 1.2	CR 7.1 BR
AVAIL 1.2	CR 7.1 RE(1)
AVAIL 1.2	CR 7.2 BR
AVAIL 1.3	CR 3.6 BR
AVAIL 2.1	CR 7.3
AVAIL 2.1	CR 7.3 RE(1)
AVAIL 2.2	CR 7.3 BR
AVAIL 2.3	CR 7.3 RE(1)
AVAIL 2.4	
AVAIL 2.5	CR 7.4 BR

A.4 Requirements relationship to ISO/IEC 27001:2013

Table A.7 identifies the requirements in this document that relate to the ISO/IEC 27001 requirements. Where more than one requirement in this document is related to a single ISO/IEC 27001 requirement, multiple rows for that requirement are used.

Table A.7 – ISO/IEC 27001:2013 cross-references

ISO/IEC 27001	IEC 62443-2-1
4.1	ORG 1.1
4.2	ORG 1.1
4.3	ORG 1.1
4.4	ORG 2.4
5.1	ORG 1.1
5.1	ORG 1.3
5.1	ORG 2.4
5.2	ORG 1.1
5.2	ORG 2.4
5.3	ORG 1.3
6.1.1	ORG 1.1
6.1.1	ORG 2.1

ISO/IEC 27001	IEC 62443-2-1
6.1.2	ORG 2.1
6.1.3	ORG 2.1
6.2	ORG 1.1
6.2	ORG 2.4
7.1	ORG 1.1
7.2	ORG 1.3
7.2	ORG 1.5
7.3	ORG 1.4
7.4	ORG 1.1
7.5.1	ORG 1.1
7.5.2	CM 1.1
7.5.2	CM 1.2

ISO/IEC 27001	IEC 62443-2-1
7.5.2	CM 1.3
7.5.2	COMP 3.3
7.5.2	NET 1.1
7.5.2	NET 1.2
7.5.2	NET 2.1
7.5.2	NET 3.2
7.5.2	ORG 1.1
7.5.2	ORG 2.1
7.5.3	CM 1.1
7.5.3	CM 1.2
7.5.3	CM 1.4
7.5.3	COMP 3.3

ISO/IEC 27001	IEC 62443-2-1
7.5.3	DATA 1.2
7.5.3	DATA 1.4
7.5.3	DATA 1.7
7.5.3	NET 1.1
7.5.3	NET 1.2
7.5.3	NET 2.1
7.5.3	NET 3.2
7.5.3	ORG 1.1
7.5.3	ORG 2.1
8.1	ORG 1.1
8.2	ORG 2.1
8.3	ORG 2.1
9.1	ORG 2.4
9.2	ORG 2.4
9.3	ORG 2.4
10.1	ORG 1.1
10.2	ORG 2.4
12.1.1	CM 1.3
12.3	AVAIL 2.1
A.5.1.1	ORG 1.1
A.5.1.2	ORG 2.4
A.6.1.1	ORG 1.3
A.6.1.1	ORG 2.1
A.6.1.2	ORG 2.2
A.6.1.2	USER 1.5
A.6.1.3	ORG 1.1
A.6.1.4	ORG 1.1
A.6.1.5	ORG 1.1
A.6.1.5	ORG 2.3
A.6.2.1	COMP 1.1
A.6.2.2	DATA 1.2
A.7.1.1	ORG 1.2
A.7.1.2	ORG 1.1
A.7.2.1	ORG 1.3
A.7.2.2	ORG 1.4
A 7.2.2	ORG 1.5
A.7.2.3	ORG 1.1
A.7.3.1	USER 1.2
A.8.1.1	CM 1.1
A.8.1.1	CM 1.3
A.8.1.2	CM 1.1
A.8.1.3	USER 1.4
A.8.1.4	ORG 1.1
A.8.2.1	DATA 1.1

ISO/IEC 27001	IEC 62443-2-1
A.8.2.2	DATA 1.1
A.8.2.3	DATA 1.2
A.8.3.1	DATA 1.1
A.8.3.2	DATA 1.4
A.8.3.3	DATA 1.1
A.9.1.1	USER 1.4
A.9.1.2	USER 1.4
A.9.1.2	USER 1.5
A.9.2.1	USER 1.2
A.9.2.2	USER 1.4
A.9.2.3	USER 1.5
A.9.2.4	DATA 1.1
A.9.2.5	USER 1.4
A.9.2.6	USER 1.4
A.9.3.1	DATA 1.1
A.9.4.1	USER 1.5
A.9.4.2	USER 1.8
A.9.4.3	USER 1.11
A.9.4.4	USER 1.5
A.9.4.5	USER 1.4
A.10.1.1	DATA 1.5
A.10.1.2	DATA 1.6
A.11.1.1	ORG 3.1
A.11.1.2	ORG 3.1
A.11.1.3	ORG 3.1
A.11.1.4	ORG 3.1
A.11.1.5	ORG 3.1
A.11.1.6	ORG 3.1
A.11.2.1	ORG 3.1
A.11.2.2	AVAIL 1.2
A.11.2.3	ORG 3.1
A.11.2.4	AVAIL 1.2
A.11.2.5	ORG 3.1
A.11.2.6	ORG 1.1
A.11.2.7	COMP 1.1
A.11.2.8	ORG 3.1
A.11.2.9	ORG 1.3
A.12.1.1	ORG 1.1
A.12.1.2	CM 1.4
A.12.1.3	AVAIL 1.2
A.12.1.4	ORG 3.1
A.12.2.1	COMP 2.1
A.12.2.1	COMP 2.2
A.12.2.1	COMP 2.3

ISO/IEC 27001	IEC 62443-2-1
A.12.3.1	AVAIL 2.3
A.12.4.1	EVENT 1.4
A.12.4.2	DATA 1.1
A.12.4.3	EVENT 1.4
A.12.4.4	NET 1.9
A.12.5.1	CM 1.4
A.12.6.1	COMP 3.1
A.12.6.1	COMP 3.2
A.12.6.1	COMP 3.3
A.12.6.1	COMP 3.4
A.12.6.1	COMP 3.5
A.12.6.1	EVENT 1.9
A.12.6.2	CM 1.4
A.12.7.1	EVENT 1.4
A.13.1.1	NET 1.1
A.13.1.2	ORG 1.1
A.13.1.3	NET 1.1
A.13.2.1	NET 1.1
A.13.2.2	ORG 1.1
A.13.2.3	DATA 1.1
A.13.2.4	DATA 1.1
A.14.1.1	ORG 2.3
A.14.1.2	NET 1.7
A.14.1.3	DATA 1.2
A.14.1.3	DATA 1.7
A.14.2.1	ORG 2.3
A.14.2.2	CM 1.4
A.14.2.3	CM 1.4
A.14.2.4	CM 1.4
A.14.2.5	ORG 2.3
A.14.2.6	ORG 2.3
A.14.2.7	ORG 1.1
A.14.2.8	ORG 2.3
A.14.2.9	CM 1.4
A.14.3.1	DATA 1.1
A.15.1.1	USER 1.4
A.15.1.2	ORG 1.1
A.15.1.3	ORG 1.6
A.15.2.1	ORG 1.6
A.15.2.2	ORG 1.6
A.16.1.1	EVENT 1.8
A.16.1.2	EVENT 1.2
A.16.1.3	EVENT 1.9
A.16.1.4	EVENT 1.7

ISO/IEC 27001	IEC 62443-2-1
A.16.1.5	EVENT 1.8
A.16.1.6	EVENT 1.8
A.16.1.6	ORG 1.1
A.16.1.7	EVENT 1.4
A.17.1.1	AVAIL 1.1
A.17.1.2	AVAIL 1.1
A.17.1.3	AVAIL 1.1
A.17.2.1	AVAIL 1.2

ISO/IEC 27001	IEC 62443-2-1
A.18.1.1	ORG 1.1
A.18.1.2	ORG 1.1
A.18.1.3	DATA 1.1
A.18.1.3	DATA 1.2
A.18.1.3	DATA 1.7
A.18.1.4	DATA 1.1
A.18.1.4	DATA 1.2
A.18.1.5	DATA 1.5

ISO/IEC 27001	IEC 62443-2-1
A.18.2.1	ORG 1.1
A.18.2.1	ORG 2.4
A.18.2.2	ORG 1.1
A.18.2.2	ORG 2.4
A.18.2.3	ORG 2.4

Table A.8 identifies the requirements in this document that relate to the ISO/IEC 27001 requirements. Where more than one requirement in ISO/IEC 27001 is related to a single IEC 62443-2-1 requirement, multiple rows for that IEC 62443-2-1 requirement are used. If there is no appropriate mapping, the requirement will be followed by a blank entry.

Table A.8 – Cross-reference of IEC 62443-2-1 to ISO/IEC 27001:2013

IEC 62443-2-1	ISO/IEC 27001
ORG 1.1	4.1
ORG 1.1	4.2
ORG 1.1	4.3
ORG 1.1	5.1
ORG 1.1	5.2
ORG 1.1	6.1.1
ORG 1.1	6.2
ORG 1.1	7.1
ORG 1.1	7.4
ORG 1.1	7.5.1
ORG 1.1	7.5.2
ORG 1.1	7.5.3
ORG 1.1	8.1
ORG 1.1	10.1
ORG 1.1	A.5.1.1
ORG 1.1	A.6.1.3
ORG 1.1	A.6.1.4
ORG 1.1	A.6.1.5
ORG 1.1	A.7.1.2
ORG 1.1	A.7.2.3
ORG 1.1	A.8.1.4
ORG 1.1	A.11.2.6
ORG 1.1	A.12.1.1
ORG 1.1	A.13.1.2
ORG 1.1	A.13.2.2
ORG 1.1	A.14.2.7
ORG 1.1	A.15.1.2
ORG 1.1	A.16.1.6

IEC 62443-2-1	ISO/IEC 27001
ORG 1.1	A.18.1.1
ORG 1.1	A.18.1.2
ORG 1.1	A.18.2.1
ORG 1.1	A.18.2.2
ORG 1.2	A.7.1.1
ORG 1.3	5.1
ORG 1.3	7.2
ORG 1.3	5.3
ORG 1.3	A.6.1.1
ORG 1.3	A.7.2.1
ORG 1.3	A.11.2.9
ORG 1.4	7.3
ORG 1.4	A.7.2.2
ORG 1.5	7.2
ORG 1.5	A 7.2.2
ORG 1.6	A.15.1.3
ORG 1.6	A.15.2.1
ORG 1.6	A.15.2.2
ORG 2.1	6.1.1
ORG 2.1	6.1.2
ORG 2.1	6.1.3
ORG 2.1	7.5.2
ORG 2.1	7.5.3
ORG 2.1	8.2
ORG 2.1	8.3
ORG 2.1	A.6.1.1
ORG 2.2	A.6.1.2
ORG 2.3	A.6.1.5

IEC 62443-2-1	ISO/IEC 27001
ORG 2.3	A.14.1.1
ORG 2.3	A.14.2.1
ORG 2.3	A.14.2.5
ORG 2.3	A.14.2.6
ORG 2.3	A.14.2.8
ORG 2.4	10.2
ORG 2.4	9.1
ORG 2.4	9.2
ORG 2.4	9.3
ORG 2.4	4.4
ORG 2.4	5.1
ORG 2.4	5.2
ORG 2.4	6.2
ORG 2.4	A.5.1.2
ORG 2.4	A.18.2.1
ORG 2.4	A.18.2.2
ORG 2.4	A.18.2.3
ORG 3.1	A.11.1.1
ORG 3.1	A.11.1.2
ORG 3.1	A.11.1.3
ORG 3.1	A.11.1.4
ORG 3.1	A.11.1.5
ORG 3.1	A.11.1.6
ORG 3.1	A.11.2.1
ORG 3.1	A.11.2.3
ORG 3.1	A.11.2.5
ORG 3.1	A.11.2.8
ORG 3.1	A.12.1.4

IEC 62443-2-1	ISO/IEC 27001
CM 1.1	7.5.2
CM 1.1	7.5.3
CM 1.1	A.8.1.1
CM 1.1	A.8.1.2
CM 1.2	7.5.2
CM 1.2	7.5.3
CM 1.3	7.5.2
CM 1.3	A.8.1.1
CM 1.3	12.1.1
CM 1.4	7.5.3
CM 1.4	A.12.1.2
CM 1.4	A.12.5.1
CM 1.4	A.12.6.2
CM 1.4	A.14.2.2
CM 1.4	A.14.2.3
CM 1.4	A.14.2.4
CM 1.4	A.14.2.9
NET 1.1	7.5.2
NET 1.1	7.5.3
NET 1.1	A.13.1.1
NET 1.1	A.13.1.3
NET 1.1	A.13.2.1
NET 1.2	7.5.2
NET 1.2	7.5.3
NET 1.3	
NET 1.4	
NET 1.5	
NET 1.6	
NET 1.7	A.14.1.2
NET 1.8	
NET 1.9	A.12.4.4
NET 2.1	7.5.2
NET 2.1	7.5.3
NET 2.2	
NET 2.3	
NET 3.1	
NET 3.2	7.5.2
NET 3.2	7.5.3
NET 3.3	CR 2.6 BR
COMP 1.1	A.6.2.1
COMP 1.1	A.11.2.7
COMP 1.2	
COMP 2.1	A.12.2.1
COMP 2.2	A.12.2.1

IEC 62443-2-1	ISO/IEC 27001
COMP 2.3	A.12.2.1
COMP 3.1	A.12.6.1
COMP 3.2	A.12.6.1
COMP 3.3	07.5.2
COMP 3.3	07.5.3
COMP 3.3	A.12.6.1
COMP 3.4	A.12.6.1
COMP 3.5	A.12.6.1
DATA 1.1	A.8.2.1
DATA 1.1	A.8.2.2
DATA 1.1	A.8.3.1
DATA 1.1	A.8.3.3
DATA 1.1	A.9.2.4
DATA 1.1	A.9.3.1
DATA 1.1	A.12.4.2
DATA 1.1	A.13.2.3
DATA 1.1	A.13.2.4
DATA 1.1	A.14.3.1
DATA 1.1	A.18.1.3
DATA 1.1	A.18.1.4
DATA 1.2	7.5.3
DATA 1.2	A.6.2.2
DATA 1.2	A.8.2.3
DATA 1.2	A.14.1.3
DATA 1.2	A.18.1.3
DATA 1.2	A.18.1.4
DATA 1.3	
DATA 1.4	A.8.3.2
DATA 1.4	7.5.3
DATA 1.5	A.10.1.1
DATA 1.5	A.18.1.5
DATA 1.6	A.10.1.2
DATA 1.7	7.5.3
DATA 1.7	A.14.1.3
DATA 1.7	A.18.1.3
USER 1.1	
USER 1.2	A.7.3.1
USER 1.2	A.9.2.1
USER 1.3	
USER 1.4	A.8.1.3
USER 1.4	A.9.1.1
USER 1.4	A.9.1.2
USER 1.4	A.9.2.2
USER 1.4	A.9.2.5

IEC 62443-2-1	ISO/IEC 27001
USER 1.4	A.9.2.6
USER 1.4	A.9.4.5
USER 1.4	A.15.1.1
USER 1.5	A.6.1.2
USER 1.5	A.9.1.2
USER 1.5	A.9.2.3
USER 1.5	A.9.4.1
USER 1.5	A.9.4.4
USER 1.6	
USER 1.7	
USER 1.8	A.9.4.2
USER 1.9	
USER 1.10	
USER 1.11	A.9.4.3
USER 1.12	
USER 1.13	
USER 1.14	
USER 1.15	
USER 1.16	
USER 1.17	
USER 1.18	
USER 1.19	
USER 2.1	
USER 2.2	
USER 2.3	
USER 2.4	
EVENT 1.1	
EVENT 1.2	A.16.1.2
EVENT 1.3	
EVENT 1.4	A.12.4.1
EVENT 1.4	A.12.4.3
EVENT 1.4	A.12.7.1
EVENT 1.4	A.16.1.7
EVENT 1.5	
EVENT 1.6	
EVENT 1.7	A.16.1.4
EVENT 1.8	A.16.1.1
EVENT 1.8	A.16.1.5
EVENT 1.8	A.16.1.6
EVENT 1.9	A.12.6.1
EVENT 1.9	A.16.1.3
AVAIL 1.1	A.17.1.1
AVAIL 1.1	A.17.1.2
AVAIL 1.1	A.17.1.3

IEC 62443-2-1	ISO/IEC 27001
AVAIL 1.2	A.11.2.2
AVAIL 1.2	A.11.2.4
AVAIL 1.2	A.12.1.3
AVAIL 1.2	A.17.2.1

IEC 62443-2-1	ISO/IEC 27001
AVAIL 1.3	
AVAIL 2.1	12.3
AVAIL 2.2	
AVAIL 2.3	A.12.3.1

IEC 62443-2-1	ISO/IEC 27001
AVAIL 2.4	
AVAIL 2.5	

A.5 Requirements relationship to the NIST CSF

Table A.9 identifies the requirements in this document that relate to elements in NIST CSF. Where more than one requirement in this document is related to a single NIST CSF element, multiple rows for that NIST CSF element are used.

Table A.9 – NIST CSF cross-references

NIST CSF	IEC 62443-2-1
DE.AE-1	NET 1.1
DE.AE-2	EVENT 1.7
DE.AE-3	EVENT 1.7
DE.AE-4	EVENT 1.7
DE.AE-4	EVENT 1.8
DE.AE-5	EVENT 1.1
DE.AE-5	EVENT 1.7
DE.CM-1	EVENT 1.1
DE.CM-2	EVENT 1.1
DE.CM-3	EVENT 1.1
DE.CM-4	COMP 2.2
DE.CM-5	USER 1.6
DE.CM-5	EVENT 1.1
DE.CM-6	ORG 1.1
DE.CM-6	ORG 1.3
DE.CM-7	ORG 2.2
DE.CM-7	EVENT 1.1
DE.CM-8	ORG 2.2
DE.DP-1	ORG 1.3
DE.DP-2	EVENT 1.1
DE.DP-3	ORG 2.2
DE.DP-3	ORG 2.3
DE.DP-3	EVENT 1.1
DE.DP-4	EVENT 1.2
DE.DP-5	ORG 1.1
ID.AM-1	CM 1.1
ID.AM-2	CM 1.1
ID.AM-3	NET 1.1
ID.AM-3	CM 1.2
ID.AM-4	ORG 1.1
ID.AM-5	DATA 1.1
ID.AM-6	ORG 1.3

NIST CSF	IEC 62443-2-1
ID.BE-1	ORG 1.6
ID.BE-5	AVAIL 1.1
ID.GV-1	ORG 1.1
ID.GV-2	ORG 1.3
ID.GV-3	ORG 1.1
ID.GV-4	ORG 2.1
ID.RA-1	EVENT 1.9
ID.RA-2	ORG 1.1
ID.RA-4	ORG 2.1
ID.RA-5	ORG 2.1
ID.RA-6	ORG 2.1
ID.RM-1	ORG 2.1
ID.RM-2	ORG 2.1
ID.RM-3	ORG 2.1
PR.AC-1	DATA 1.1
PR.AC-1	DATA 1.6
PR.AC-1	USER 1.1
PR.AC-1	USER 1.2
PR.AC-1	USER 1.4
PR.AC-1	USER 1.6
PR.AC-1	USER 1.8
PR.AC-1	USER 1.9
PR.AC-1	USER 1.11
PR.AC-1	USER 1.19
PR.AC-2	ORG 3.1
PR.AC-2	AVAIL 1.1
PR.AC-2	AVAIL 1.2
PR.AC-3	NET 1.1
PR.AC-3	NET 1.6
PR.AC-3	NET 3.2
PR.AC-3	NET 3.3
PR.AC-4	USER 1.4

NIST CSF	IEC 62443-2-1
PR.AC-4	USER 1.5
PR.AC-4	USER 1.7
PR.AC-4	USER 2.1
PR.AC-4	USER 2.2
PR.AC-5	NET 1.1
PR.AC-5	NET 1.6
PR.AC-5	USER 1.16
PR.AT-1	ORG 1.4
PR.AT-2	ORG 1.3
PR.AT-2	ORG 1.5
PR.AT-3	ORG 1.3
PR.AT-3	ORG 1.4
PR.AT-3	ORG 1.5
PR.AT-4	ORG 1.3
PR.AT-4	ORG 1.4
PR.AT-4	ORG 1.5
PR.AT-5	ORG 1.3
PR.AT-5	ORG 1.4
PR.AT-5	ORG 1.5
PR.DS-1	CM 1.3
PR.DS-1	DATA 1.2
PR.DS-2	NET 1.1
PR.DS-2	NET 1.6
PR.DS-2	NET 1.7
PR.DS-2	DATA 1.2
PR.DS-2	DATA 1.4
PR.DS-2	USER 1.16
PR.DS-3	COMP 1.1
PR.DS-3	USER 1.4
PR.DS-3	USER 1.5
PR.DS-5	ORG 1.1
PR.DS-5	ORG 1.2

NIST CSF	IEC 62443-2-1
PR.DS-5	NET 1.1
PR.DS-5	NET 1.6
PR.DS-5	NET 1.7
PR.DS-5	DATA 1.1
PR.DS-5	DATA 1.2
PR.DS-6	ORG 2.2
PR.DS-6	DATA 1.7
PR.DS-6	USER 1.16
PR.DS-7	NET 1.1
PR.IP-1	CM 1.3
PR.IP-1	CM 1.4
PR.IP-2	ORG 1.1
PR.IP-2	ORG 2.3
PR.IP-3	CM 1.3
PR.IP-3	CM 1.4
PR.IP-4	AVAIL 2.1
PR.IP-5	ORG 3.1
PR.IP-5	AVAIL 1.2
PR.IP-6	DATA 1.4
PR.IP-7	ORG 1.1
PR.IP-8	ORG 1.1
PR.IP-9	EVENT 1.8
PR.IP-9	AVAIL 1.1
PR.IP-10	EVENT 1.8
PR.IP-10	AVAIL 1.1
PR.IP-11	ORG 1.1
PR.IP-11	ORG 1.2
PR.IP-12	EVENT 1.9
PR.MA-1	AVAIL 1.2
PR.MA-2	ORG 3.1
PR.MA-2	AVAIL 1.2
PR.PT-1	NET 1.9
PR.PT-1	DATA 1.1
PR.PT-1	EVENT 1.4

NIST CSF	IEC 62443-2-1
PR.PT-1	EVENT 1.7
PR.PT-2	ORG 1.3
PR.PT-2	DATA 1.1
PR.PT-2	DATA 1.2
PR.PT-3	NET 1.1
PR.PT-3	NET 1.6
PR.PT-3	NET 2.2
PR.PT-3	COMP 1.1
PR.PT-3	DATA 1.1
PR.PT-3	DATA 1.2
PR.PT-3	DATA 1.6
PR.PT-3	USER 1.4
PR.PT-3	USER 1.5
PR.PT-3	USER 1.6
PR.PT-3	USER 1.8
PR.PT-3	USER 1.9
PR.PT-3	USER 1.11
PR.PT-3	USER 1.15
PR.PT-3	USER 1.17
PR.PT-3	USER 1.18
PR.PT-3	USER 1.19
PR.PT-3	USER 2.1
PR.PT-3	USER 2.2
PR.PT-3	USER 2.3
PR.PT-3	USER 2.4
PR.PT-4	CM 1.3
PR.PT-4	NET 1.1
PR.PT-4	NET 1.2
PR.PT-4	NET 1.4
PR.PT-4	NET 1.5
PR.PT-4	NET 1.6
PR.PT-4	NET 1.8
PR.PT-4	USER 1.16
RC.IM-1	EVENT 1.8

NIST CSF	IEC 62443-2-1
RC.IM-1	AVAIL 1.1
RC.IM-2	EVENT 1.8
RC.IM-2	AVAIL 1.2
RC.RP-1	EVENT 1.8
RC.RP-1	AVAIL 1.1
RS.AN-1	ORG 1.1
RS.AN-1	EVENT 1.7
RS.AN-1	EVENT 1.8
RS.AN-2	ORG 1.1
RS.AN-2	EVENT 1.7
RS.AN-3	EVENT 1.7
RS.AN-4	EVENT 1.7
RS.CO-1	ORG 1.3
RS.CO-1	EVENT 1.8
RS.CO-2	ORG 1.1
RS.CO-2	EVENT 1.2
RS.CO-3	EVENT 1.2
RS.CO-4	EVENT 1.2
RS.IM-1	EVENT 1.8
RS.IM-2	EVENT 1.8
RS.MI-1	NET 1.1
RS.MI-1	NET 1.4
RS.MI-1	NET 1.5
RS.MI-1	NET 1.6
RS.MI-1	EVENT 1.8
RS.MI-2	NET 1.1
RS.MI-2	NET 1.5
RS.MI-2	NET 1.6
RS.MI-2	COMP 2.2
RS.MI-3	EVENT 1.9
RS.RP-1	EVENT 1.8

Table A.10 identifies the requirements in this document that relate to the NIST CSF elements. Where more than one NIST CSF element is related to a single IEC 62443-2-1 requirement, multiple rows for that IEC 62443-2-1 requirement are used. If there is no appropriate mapping, the requirement will be followed by a blank entry.

Table A.10 – Cross-reference of IEC 62443-2-1 to NIST CSF

IEC 62443-2-1	NIST CSF
ORG 1.1	DE.DP-5
ORG 1.1	ID.GV-1
ORG 1.1	ID.GV-3
ORG 1.1	ID.AM-4
ORG 1.1	ID.RA-2
ORG 1.1	PR.DS-5
ORG 1.1	PR.IP-2
ORG 1.1	PR.IP-7
ORG 1.1	PR.IP-8
ORG 1.1	PR.IP-11
ORG 1.1	DE.CM-6
ORG 1.1	RS.CO-2
ORG 1.1	RS.AN-1
ORG 1.1	RS.AN-2
ORG 1.2	PR.DS-5
ORG 1.2	PR.IP-11
ORG 1.3	ID.AM-6
ORG 1.3	ID.GV-2
ORG 1.3	PR.AT-2
ORG 1.3	PR.AT-3
ORG 1.3	PR.AT-4
ORG 1.3	PR.AT-5
ORG 1.3	PR.PT-2
ORG 1.3	DE.CM-6
ORG 1.3	DE.DP-1
ORG 1.3	RS.CO-1
ORG 1.4	PR.AT-1
ORG 1.4	PR.AT-3
ORG 1.4	PR.AT-4
ORG 1.4	PR.AT-5
ORG 1.5	PR.AT-2
ORG 1.5	PR.AT-3
ORG 1.5	PR.AT-4
ORG 1.5	PR.AT-5
ORG 1.6	ID.BE-1
ORG 2.1	ID.GV-4
ORG 2.1	ID.RA-4
ORG 2.1	ID.RA-5
ORG 2.1	ID.RA-6
ORG 2.1	ID.RM-1
ORG 2.1	ID.RM-2
ORG 2.1	ID.RM-3
ORG 2.2	PR.DS-6
ORG 2.2	DE.CM-7
ORG 2.2	DE.CM-8
ORG 2.2	DE.DP-3
ORG 2.3	PR.IP-2
ORG 2.3	DE.DP-3
ORG 2.4	
ORG 3.1	PR.AC-2
ORG 3.1	PR.IP-5
ORG 3.1	PR.MA-2
CM 1.1	ID.AM-1
CM 1.1	ID.AM-2
CM 1.2	ID.AM-3
CM 1.3	PR.DS-1
CM 1.3	PR.IP-1
CM 1.3	PR.IP-3
CM 1.3	PR.PT-4
CM 1.4	PR.IP-1
CM 1.4	PR.IP-3
NET 1.1	ID.AM-3
NET 1.1	PR.AC-3
NET 1.1	PR.AC-5
NET 1.1	PR.DS-2
NET 1.1	PR.DS-5
NET 1.1	PR.DS-7
NET 1.1	PR.PT-3
NET 1.1	PR.PT-4
NET 1.1	DE.AE-1
NET 1.1	RS.MI-1
NET 1.1	RS.MI-2
NET 1.2	PR.PT-4
NET 1.3	
NET 1.4	PR.PT-4
NET 1.4	RS.MI-1
NET 1.5	PR.PT-4
NET 1.5	RS.MI-1
NET 1.5	RS.MI-2
NET 1.6	PR.AC-3
NET 1.6	PR.AC-5
NET 1.6	PR.DS-2
NET 1.6	PR.DS-5
NET 1.6	PR.PT-3
NET 1.6	PR.PT-4
NET 1.6	RS.MI-1
NET 1.6	RS.MI-2
NET 1.7	PR.DS-2
NET 1.7	PR.DS-5
NET 1.8	PR.PT-4
NET 1.9	PR.PT-1
NET 2.1	
NET 2.2	PR.PT-3
NET 2.3	
NET 3.1	
NET 3.2	PR.AC-3
NET 3.3	PR.AC-3
COMP 1.1	PR.DS-3
COMP 1.1	PR.PT-3
COMP 1.2	
COMP 2.1	
COMP 2.2	DE.CM-4
COMP 2.2	RS.MI-2
COMP 2.3	
COMP 3.1	
COMP 3.2	
COMP 3.3	
COMP 3.4	
COMP 3.5	
DATA 1.1	ID.AM-5
DATA 1.1	PR.AC-1
DATA 1.1	PR.DS-5
DATA 1.1	PR.PT-1
DATA 1.1	PR.PT-2
DATA 1.1	PR.PT-3
DATA 1.2	PR.DS-1
DATA 1.2	PR.DS-2

IEC 62443-2-1	NIST CSF
DATA 1.2	PR.DS-5
DATA 1.2	PR.PT-2
DATA 1.2	PR.PT-3
DATA 1.3	
DATA 1.4	PR.DS-2
DATA 1.4	PR.IP-6
DATA 1.5	
DATA 1.6	PR.AC-1
DATA 1.6	PR.PT-3
DATA 1.7	PR.DS-6
USER 1.1	PR.AC-1
USER 1.2	PR.AC-1
USER 1.3	
USER 1.4	PR.AC-1
USER 1.4	PR.AC-4
USER 1.4	PR.DS-3
USER 1.4	PR.PT-3
USER 1.5	PR.AC-4
USER 1.5	PR.DS-3
USER 1.5	PR.PT-3
USER 1.6	PR.AC-1
USER 1.6	PR.PT-3
USER 1.6	DE.CM-5
USER 1.7	PR.AC-4
USER 1.8	PR.AC-1
USER 1.8	PR.PT-3
USER 1.9	PR.AC-1
USER 1.9	PR.PT-3
USER 1.10	
USER 1.11	PR.AC-1
USER 1.11	PR.PT-3
USER 1.12	
USER 1.13	
USER 1.14	
USER 1.15	PR.PT-3
USER 1.16	PR.AC-5
USER 1.16	PR.DS-2

IEC 62443-2-1	NIST CSF
USER 1.16	PR.DS-6
USER 1.16	PR.PT-4
USER 1.17	PR.PT-3
USER 1.18	PR.PT-3
USER 1.19	PR.AC-1
USER 1.19	PR.PT-3
USER 2.1	PR.AC-4
USER 2.1	PR.PT-3
USER 2.2	PR.AC-4
USER 2.2	PR.PT-3
USER 2.3	PR.PT-3
USER 2.4	PR.PT-3
EVENT 1.1	DE.AE-5
EVENT 1.1	DE.CM-1
EVENT 1.1	DE.CM-2
EVENT 1.1	DE.CM-3
EVENT 1.1	DE.CM-5
EVENT 1.1	DE.CM-7
EVENT 1.1	DE.DP-2
EVENT 1.1	DE.DP-3
EVENT 1.2	DE.DP-4
EVENT 1.2	RS.CO-2
EVENT 1.2	RS.CO-3
EVENT 1.2	RS.CO-4
EVENT 1.3	
EVENT 1.4	PR.PT-1
EVENT 1.5	
EVENT 1.6	
EVENT 1.7	PR.PT-1
EVENT 1.7	DE.AE-2
EVENT 1.7	DE.AE-3
EVENT 1.7	DE.AE-4
EVENT 1.7	DE.AE-5
EVENT 1.7	RS.AN-1
EVENT 1.7	RS.AN-2
EVENT 1.7	RS.AN-3
EVENT 1.7	RS.AN-4

IEC 62443-2-1	NIST CSF
EVENT 1.8	PR.IP-9
EVENT 1.8	PR.IP-10
EVENT 1.8	DE.AE-4
EVENT 1.8	RS.RP-1
EVENT 1.8	RS.CO-1
EVENT 1.8	RS.AN-1
EVENT 1.8	RS.MI-1
EVENT 1.8	RS.IM-1
EVENT 1.8	RS.IM-2
EVENT 1.8	RC.RP-1
EVENT 1.8	RC.IM-1
EVENT 1.8	RC.IM-2
EVENT 1.9	ID.RA-1
EVENT 1.9	PR.IP-12
EVENT 1.9	RS.MI-3
AVAIL 1.1	ID.BE-5
AVAIL 1.1	PR.AC-2
AVAIL 1.1	PR.IP-9
AVAIL 1.1	PR.IP-10
AVAIL 1.1	RC.RP-1
AVAIL 1.1	RC.IM-1
AVAIL 1.2	RC.IM-2
AVAIL 1.2	PR.AC-2
AVAIL 1.2	PR.IP-5
AVAIL 1.2	PR.MA-1
AVAIL 1.2	PR.MA-2
AVAIL 1.3	
AVAIL 2.1	PR.IP-4
AVAIL 2.2	
AVAIL 2.3	
AVAIL 2.4	
AVAIL 2.5	

Annex B
(informative)

Establishing and maintaining an IACS SP

B.1 General

Business risk is the possibility that an organization will not achieve its business goals. Business goals vary for different organizations and can include abstract goals such as goodwill and intellectual property goals, and tangible goals such as production and HSE goals. Business risk management is fundamental for assuring that an organization protects itself from conditions and events that can cause damage or that can be costly and time consuming to repair based on their business goals. Therefore, business risk management should be an integrated and formalized program within the organization.

This annex summarizes considerations for assessing and managing IACS cybersecurity risks that contribute to the overall business risk of an organization. Notably, the causes of these risks are related to cybersecurity threats as opposed to other factors such as fire, flood, vandalism and safety hazards threats. These threats can originate from a variety of sources, including the Internet, corporate networks, maintenance activities, software upgrades and unauthorized IACS access with the potential to result in incidents with HSE consequences, financial/economic consequences or both.

This annex discusses the management of cybersecurity risks and the associated reduction of risk through the direct application of cybersecurity measures. The process of managing these risks and applying/maintaining appropriate cybersecurity measures throughout the life cycle of the IACS and based on the asset owner's business objectives is referred to as a SP. Utilizing a SP has the main benefit of optimizing the asset owner's expenditures such that:

a) security measures and requirements necessary to provide an appropriate level of protection from and mitigation of cyber-attacks for a facility's current risk profile are identified, and

b) potential security measures or requirements are prioritized in a manner that provides cost-effective protection from and mitigation of cyber-attacks for a facility's current risk profile.

Either consciously or unconsciously, the asset owner manages risk every day in pursuing their business objectives. Organizations typically evaluate risks associated with their specific businesses and decide how to manage those risks based on organizational priorities, as well as internal and external constraints such as budget and regulatory requirements. This risk management process should be systematic and iterative and be an ongoing part of the organization's normal operations.

Historically, organizations with IACS have managed risk through engineering and safety practices and through the use of safety assessments, which are generally well-established in most industrial sectors. However, cybersecurity is a relatively new and rapidly evolving problem facing organizations, and associated risk assessment and management practices to counter cybersecurity risks are equally new and evolving.

Therefore, the asset owner's risk management program should be extended to address cybersecurity risks and supported by a cybersecurity assessment process that is used to assist with the development, improvement and evaluation of an IACS SP.

In summary, an effective and comprehensive risk management process that includes cybersecurity should be employed seamlessly throughout the organization with overall objectives of continuous improvement in the organization's risk-related activities and effective communication among all stakeholders having a shared interest in the mission/business success of the organization.

This annex summarizes some of the key factors IACS asset owners should consider in assessing and managing their organization's cyber risk. A detailed presentation of a risk management framework, process and requirements, as well as implementation guidance, are provided in IEC 62443-3-2.

B.2 Managing cybersecurity risk

B.2.1 Understanding cybersecurity risk

An effective cybersecurity risk management program should ensure that an asset's level of protection is commensurate to the impact of a compromise caused by a cybersecurity related attack. Traditional elements of business risk include:

a) the likelihood of an event, and

b) the impact resulting from occurrence of the event.

Likelihood, however, is not generally appropriate for cybersecurity risks for a variety of reasons. First, there is little or no historical data to support likelihood estimates. Second, the threat landscape is rapidly changing, and for intentional attacks, that threat landscape is related to the often-unpredictable behaviour of attackers, which is also based on a number of non-quantifiable factors.

Therefore, the traditional business risk equation has to be re-evaluated for cybersecurity with respect to the likelihood of an event. An IACS's vulnerability to attack can be characterized by the combination of exposure to attack and the degree of difficulty/cost/effort required for an attack to succeed. This provides greater insights into cybersecurity risks than attempts to estimate the likelihood of a cyber event. This concept for cybersecurity risk is discussed in more detail in B.2.3.

B.2.2 Impacts of cybersecurity compromises

Focusing initially on impact, many consider the impact of concern to be the successful cyber-attack on an IACS asset or system of interest. Although this approach has some value, obtaining the most value for the organization's "cybersecurity expenditure" is achieved by focusing on the potential impact or business consequence of a cyber-attack rather than the cyber compromise itself. After all, if a cyber-attack on an asset or system produces an impact or consequence that is acceptable to the organization, then why spend limited resources protecting that asset or system from cyber threats? Thus, when assessing and managing cyber risks, it is equally, and perhaps more, important to understand the impact or business consequence of a cyber-attack on an asset as it is to understand the asset's robustness to protect against a cyber-attack.

B.2.3 Risk ranking

Asset owners already manage risks, and those risks can be categorized by their impact/consequence to the business. The impact of a cyber-attack needs to be included within the asset owner's risk matrix. In order to properly prioritize the business risks by the impact of a cyber-attack, it is important to understand the organization's risk environment within which the IACS assets exist.

For example, maintaining production requirements based on a daily output that can be compromised due to a cyber-attack on an asset within the IACS can be defined by the business as a commercial risk with a "serious" impact. Many companies have formally defined "risk" levels for use in their decision making regarding discretionary expenditures and investments.

Examples of an organization's risks and risk levels are provided in Table B.1. This table is a representative example intended to illustrate different types of risk levels. This table does not represent recommended or suggested risk levels.

The format and content of this example table varies greatly by industry and organization. Nonetheless, it does provide a sense for how organizations may formally define their risk levels for use in their decision making. It is important for the asset owner to understand its organizational risk levels in order to effectively incorporate this information into the assessment and management of cyber risk.

Table B.1 – Example risk levels

Risk level	Worker safety	Public safety	Environment	Commercial
Very low	Minor injury, first aid	N/A	Small release, limited onsite clean-up	$50,000
Low	Lost time injury, no extended hospitalization	N/A	Limited onsite damage, moderate clean-up	$500,000
Moderate	Lost time injury, requires extended hospitalization	Notification of offsite emergency agencies	Limited offsite impact, large onsite clean-up	$5 million
High	Single fatality	Shelter in place required	Large offsite release and clean-up required	$50 million
Very high	Multiple fatalities	Evacuation required	Extensive offsite clean-up, some permanent damage	$500 million
Serious	Multiple fatalities	Offsite injuries, medical treatment required	Extensive multi-year offsite clean-up and remediation	$1 billion

B.2.4 Cybersecurity attack exposure versus likelihood

Given the diversity of potential cyber threats ranging from unintentional internal events to malicious acts by nation-states, the ability to estimate a realistic value for likelihood for a specific type of a cyber-attack is at best arguable. Human factors engineering can enable a level of quantification for unintentional internal incidents. However, this is not the case for the other types of potential cyber threats.

A more practical alternative is to replace the likelihood of a cyber-attack with a combination of the exposure to attack and the degree of difficulty to carry out the attack. Exposure can be estimated based on the number of exposed interfaces through which an attack can be launched. The degree of difficulty is proportional to the level of protection provided by cybersecurity measures. The more effective the security measure, the greater the degree of difficulty.

IEC 62443-3-3 and IEC 62443-4-2 define requirements for technical security measures and specify SLs for them that indicate their strength against attack. IEC 62443-2-4 defines requirements for process security measures and specifies MLs for them that indicate how well evolved/mature they are. The asset owner can use any combination of these in its IACS, and each requirement in this document is supported by references to these IEC 62443 parts to assist the asset owner in selecting appropriate technical and process security measures to meet the requirements in this document.

B.3 Elements of a cybersecurity risk assessment/management process

An effective risk assessment/management process should contain a risk assessment portion that produces graded results that align the level of security protections directly with the significance of an asset's potential compromise. A summary of the objectives of the risk assessment portion is as follows:

a) Review and identify the critical systems and networks

Identify IACS critical process systems and networks, based on the risk level to the business so that they may be reviewed with regards to appropriate security measures and requirements to protect the assets within these per this document. For example, if loss of production is a major risk to the business, then identify all IACS process systems and networks that are required to maintain production as essential systems.

b) Identify assets within the essential systems

Develop a documented listing of all assets within the essential systems. Identify the assets that are digital assets (DAs) and are potential sources of undesired cyber impacts. Review the listing of these assets to identify and document which ones are "critical" digital assets (CDAs) and either directly or indirectly perform functions supporting the areas for which risk levels have been defined (for example, worker protection, production, HSE protection, etc.) as described in B.2.2.

c) Assessing the cyber compromise impact

For each of the DAs and CDAs, determine/document the impact of a cyber compromise within each of the areas for which risk levels are defined (for example, worker protection, production, HSE protection, etc.). Then, determine the highest impact for each of the assets by using the risk level table. An asset's impact can vary by risk area. For example, a CDA can have a "serious" financial commercial impact and a "low" impact with regards to worker safety with little or no HSE impact. Thus, it is important that the CDA be assessed for each of the risk areas.

d) Identify existing cybersecurity controls

For each DA and CDA, determine/document the existing cybersecurity measures (both technical and administrative) in place and functioning that protect the asset from compromise.

e) Conduct cybersecurity controls gap analysis

For each DA and CDA, conduct/document a cybersecurity measures gap analysis between those in place and functioning for the "as is" risk acceptance condition and those required to achieve a tolerable risk level.

f) Identify additional cybersecurity measures

For each DA CDA and their identified zone, conduit or both, evaluate the cybersecurity measures gaps and determine what (if any) additional security measures per this document are required to result in a tolerable risk.

Admittedly, the level of work required to perform this process will vary by industry, the complexity of IACS and the process it governs. Additionally, implementing these steps is not necessarily as easy as it can appear. Figure B.1 presents a detailed example of how the asset owner can implement the above process utilizing a risk-informed approach per this annex. A more formal discussion on risk management is provided in IEC 62443-3-2.

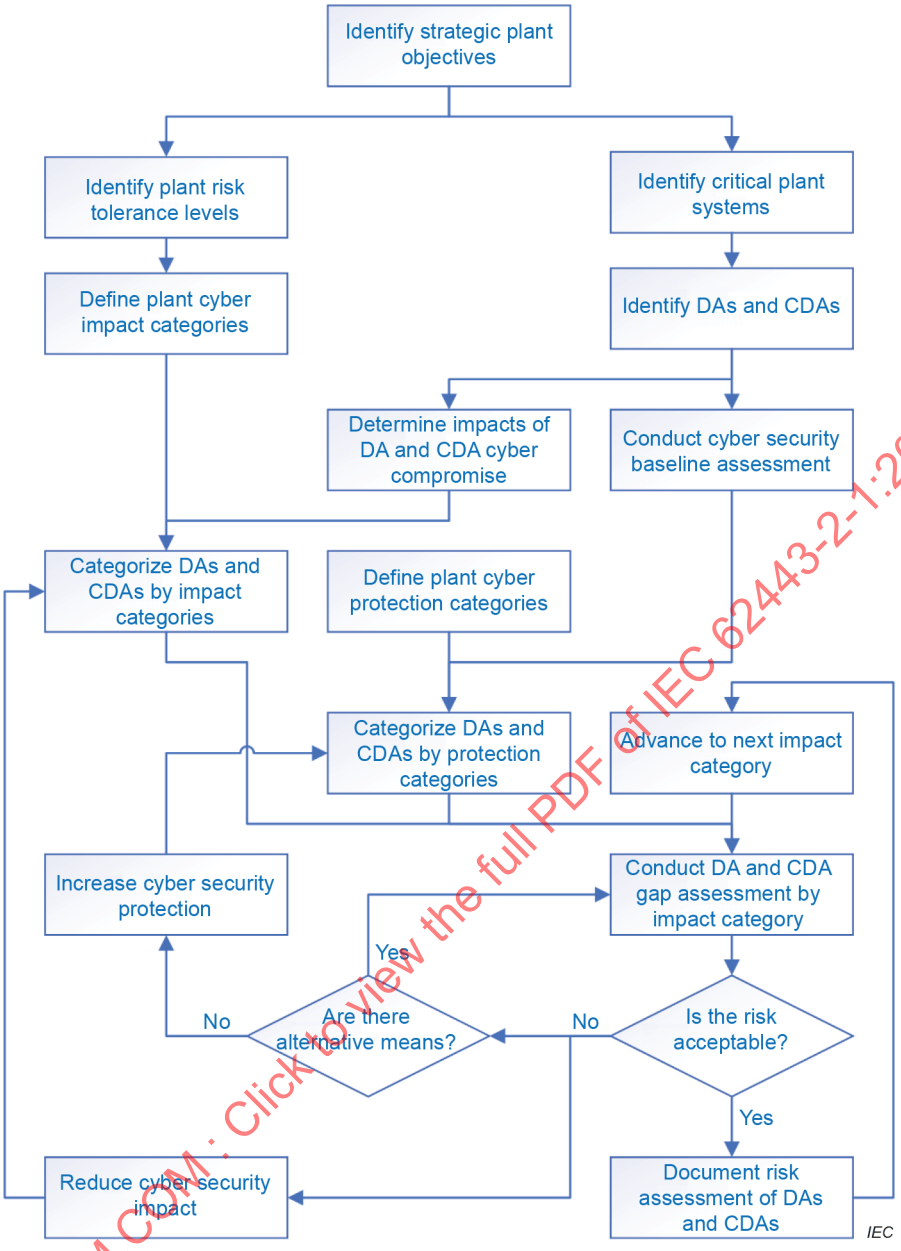

Figure B.1 – Example of process flow for cybersecurity risk management

B.4 Elements of a cybersecurity risk assessment/management process

This annex provides information for an asset owner to utilize their existing business risk processes to reduce/mitigate business risk from cyber events by the application of security measures. When selecting security measures to address identified security risk gaps, there is no "one size fits all" approach to closing the gap. Cybersecurity measures are the implementation/application of security measures that are formally documented as requirements in this document, IEC 62443-2-4, IEC 62443-3-3 and IEC 62443-4-2. Generally, there are two types of security elements:

a) process security measures that are implemented in policies, procedures, training and processes contained within facility-wide programs such as operations, maintenance and engineering, and

b) technical security measures that are targeted to specific assets, equipment or systems where the level of technical security measure comprehensiveness will vary by the risk significance of the asset.

In most cases, the optimal actions consist of a combination of process and technical security measures. In fact, one approach is to define a hierarchy of security measures to assure consistency and standardization in the organization's security measure approach. As conceptually illustrated in Figure B.2, the security measures regime is structured such that an asset's comprehensiveness of security measures is directly proportional to the level of protection an asset requires in order to achieve a tolerable cyber risk.

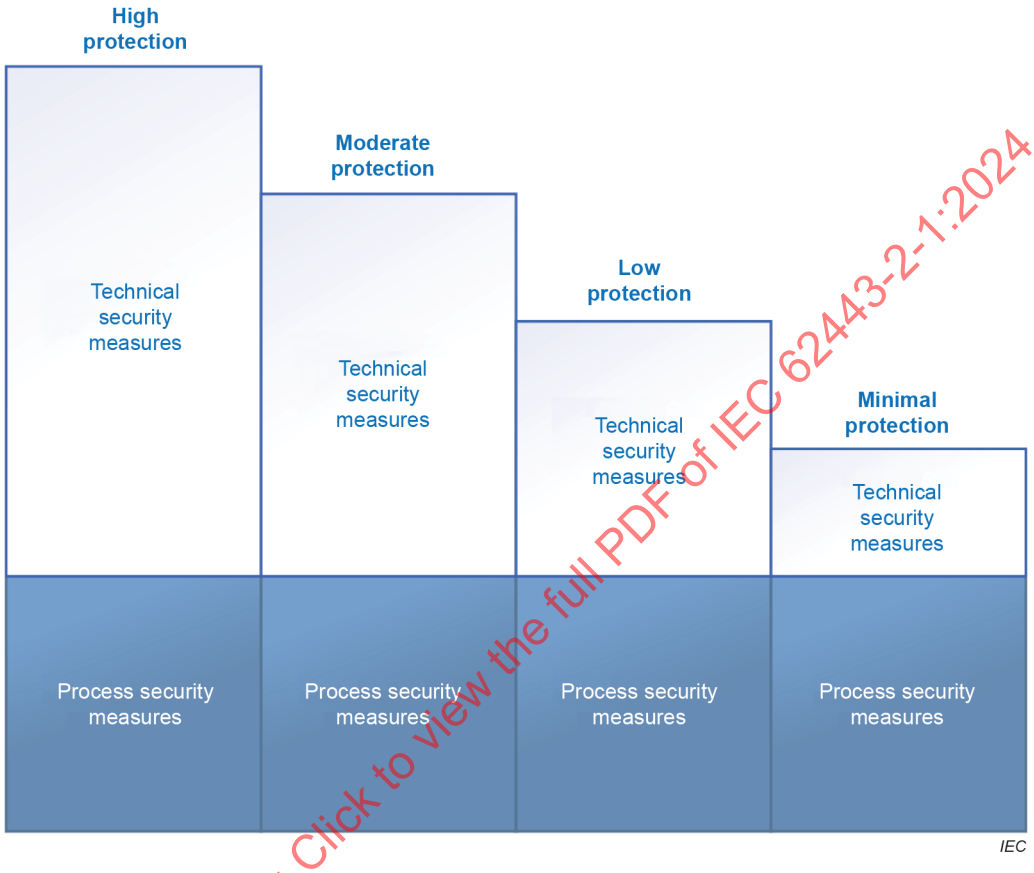

Figure B.2 – Levels of protection an asset requires

Annex C
(informative)

Evaluating MLs

C.1 Approach to evaluating MLs

How an asset owner approaches evaluating their maturity has two parts: scoping and methodology. When considering the scope of the ML assessment, it will be very dependent on the IACS SP and its application across the IACSs of the asset owner.

For asset owners who use the same IACS SP for all or most of its IACSs, the scope of the ML assessment can be that portion of organization that uses this IACS SP. This is because part of the evaluation method is determining how well the asset owner has applied each of their required SP processes across their entire organization. For some very large organizations, it is possible for them to evaluate different IACSs or business units independently if they act like or operate separately. For example, if a multi-national corporation owns multiple companies in different industries, each of the independent companies can conduct ML assessments separately. In cases such as this, though, the individual companies would want to treat their entire organization as within scope and not subdivide the assessment any further.

While Clause 5 discusses formal conformance and assessment processes for an asset owner organization, asset owners can periodically conduct maturity self-assessments or contract third parties to help them develop their road map for improving their security posture. When considering an assessment methodology, it is important for the asset owner to establish or adopt a process that is repeatable. Since these assessments should be conducted periodically, the methodology should provide some way to compare the different assessments and show the overall change in maturity.

It can be difficult to fully evaluate and compare an asset owner's maturity by aggregating the MLs of each of the evaluated SP processes into a single number, but trying to present the results of evaluating dozens of requirements separately can be too granular for key stakeholders within the organization. The asset owner will need to strike a balance between presenting the results of the ML assessment in enough granularity to be useful but not overwhelm decision makers with too much information. One possible method would be to present the ML results based on the score for each SP element (SPE). The asset owner would still evaluate each requirement separately, but those individual requirement evaluations could be aggregated together to form a score for each SPE.

The way to evaluate the individual requirements contained in this document will be dependent on the methodology developed or adopted by the asset owner. The organization might see value in expanding upon each of the requirements to create one or more written questions using their own vernacular to help communicate the proper industry or organizational jargon. When adding additional questions, the asset owner should consider the length of time necessary to conduct the assessment and whether they will require evidence during the self-assessment or third-party evaluation.

It is important to remember that any ML assessment is only a point-in-time evaluation. Asset owner organizations often have projects being conducted during the time of the assessment. The organization should evaluate its current as-is state. It can look at and acknowledge that there are activities currently being implemented; however, only the currently implemented process and technical security measures should be considered when evaluating the MLs during the assessment.

C.2 Examples of how to evaluate MLs

The criteria an evaluator uses when scoring MLs can seem very subjective. Subtle differences in interpretation of the language used to define the MLs can lead one evaluator to come up with different scores than another evaluator. The following are some examples of different cases where an evaluator could determine the differences between one level and another. These are not meant as modifications to the definitions for MLs, only as guidance to assist asset owners conducting self-assessments and third-party evaluators understand the differences between the MLs.

When conducting an assessment, an evaluator can come across some requirements where the organization has not met even the minimum level of maturity. For these requirements, the organization would have no policies or procedures documented and no personnel would be performing any actions, even in an ad hoc manner, related to the requirement. This would be different from a requirement where the organization has made a conscious, risk-based decision to not implement some technology. The complete lack of any documentation or performed processes, would result in the evaluator scoring the requirement as not conformant, which could be represented as a zero in a numeric scoring sheet.

For ML1, Initial, the organization has demonstrated that they are performing some actions related to this requirement. This often relies on personnel knowing what they are supposed to do, even though there are not always any policies or procedures. In these cases, if the organization needed to bring on new personnel, whether from outside the organization or from other business units, there might be a long timeframe before they could perform the tasks necessary due to the time it took to become proficient. They would not have any documentation or formal training to use to learn the tasks. They would have to rely on shadowing other personnel to learn. With respect to the implementation of technology, the organization could have technology deployed related to assist with that specific requirement; however, the implementation might not be consistently applied across the organization or well documented.

ML 2, Managed, mostly has to do with policies and procedures being documented. The organization could produce evidence if asked related to how they meet the specific requirement but cannot always provide proof that they are executing those policies and procedures yet. Personnel can know about the policies and procedures, and they can be performing some of the actions related to them, but the organization cannot show that they are performing them consistently yet. This can be the case when an organization has gone through the process to build policies and procedures but has not fully implemented them. ML 2 is a steppingstone to ML 3, where the organization is working towards a goal of fully implementing the security measures but has not completed that process yet. For ML 2, the policies and procedures have not been tested, so are not always tailored to the environment. There can be aspects to the policies and procedures that need to be changed or adapted to the organization's environment before they can achieve ML 3.

At ML 3, the organization has demonstrated that they have well-documented policies and procedures, as well as shown that their personnel are performing actions related to those policies and procedures. These policies and procedures will also be tailored to their environment, as the organization can demonstrate that they are meeting the requirements in operations. Since personnel can now demonstrate proficiency with the policies and procedures, they should be able to rely on the documented procedures during normal and adverse conditions, such as during an incident response situation.

For ML 4, the organization has demonstrated that they are not just performing actions, a process that implements a requirement, they have evidence that the process has been improved, or they have active processes in place to evaluate, update, and improve those policies and procedures to meet changing conditions. This might include continuous improvement cycles for the policies and procedures, or it could include technology re-evaluation cycles based on different conditions. Organizations that are evaluated as ML 4 for one or more security requirements are often being proactive in how they apply changes, often using feedback from personnel and technical solutions as a way to initiate review cycles.

Bibliography

NOTE This Bibliography includes references to sources used in the creation of this document as well as references to sources that can help the reader in developing a greater understanding of cybersecurity as a whole and developing a management system.

[1] IEC 62443-3-2:2020, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*

[2] IEC 62443-2-4:2023, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

[3] IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

[4] IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

[5] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[6] ISO 31000, *Risk management – Guidelines*

[7] NIST SP 800 39, *Managing Information Security Risk: Organization, Mission, and Information System View*

[8] ISO/IEC 27001:2013[7], *Information technology – Security techniques – Information security management systems – Requirements*

[9] NIST Cybersecurity Framework, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*

[10] IEC 62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Product security development lifecycle requirements*

[11] Software Engineering Institute (SEI), CMMI for Services, Version 1.3

[12] ISO/IEC 17000:2020, *Conformity assessment – Vocabulary and general principles*

[13] IEC TS 62443-1-5:2023, *Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 security profiles*

[14] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection – Information security controls*

[15] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

[16] NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*

[17] IEC TR 62443-2-3:2015, *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*

7 This document has been withdrawn. References to the ISO/IEC 27001:2022 will be considered in the next edition of IEC 62443-2-1.

[18] IEEE Std 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

[19] NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*

[20] IEEE 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity*

[21] IETF RFC 3748, *Extensible Authentication Protocol (EAP)*

[22] IETF RFC 7057, *Update to the Extensible Authentication Protocol (EAP), Applicability Statement for Application Bridging for Federated Access Beyond Web (ABFAB)*

[23] IEEE 802.1X-2020, *IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control*

[24] IEC 62591:2016, *Industrial networks – Wireless communication network and communication profiles – WirelessHART™*

[25] IEC 62734:2014, *Industrial networks – Wireless communication network and communication profiles – ISA 100.11a*
IEC 62734:2014/AMD1:2019

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments du présent document de l'IEC peuvent faire l'objet de droits de brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété. À la date de publication du présent document, l'IEC n'a reçu aucune déclaration relative à des droits de brevets, qui pourraient être exigés pour la mise en œuvre du présent document. Toutefois, il est rappelé aux responsables de cette mise en œuvre qu'il ne s'agit peut-être pas des informations les plus récentes, qui peuvent être obtenues dans la base de données disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62443-2-1 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels, en collaboration avec le comité de liaison ISA99: Comité ISA pour la sécurité des systèmes d'automatisation et de commande industrielles. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2010. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) la structure des exigences a été révisée en éléments SP (SPE – SP element);
b) les exigences ont été révisées pour éliminer la répétition d'un système de management de la sécurité de l'information (SMSI); et
c) un modèle de stabilisation a été défini pour l'évaluation des exigences.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
65/1044/FDIS	65/1053/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

Une liste de toutes les parties de la série IEC 62443, publiées sous le titre général *Sécurité des systèmes d'automatisation et de commande industrielles*, se trouve sur le site web de l'IEC.

Les futures normes de cette série porteront le nouveau titre général cité ci-dessus. Le titre des normes qui existent déjà dans cette série sera mis à jour lors de leur prochaine édition.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

INTRODUCTION

Le présent document est la partie de la série IEC 62443 qui contient les exigences de sécurité pour les propriétaires d'actif des systèmes d'automatisation et de commande industrielles (IACS – industrial automation and control system). Dans le contexte du présent document, le propriétaire d'actif inclut également l'opérateur de l'IACS. Ses exigences portent sur la cybersécurité et permettent aux capacités de sécurité qui les satisfont d'être fournies combinées à la fois avec des mesures de sécurité techniques, physiques, procédurales et compensatoires.

La cybersécurité est un sujet dont l'importance ne cesse de prendre de l'ampleur dans les organisations modernes. Le terme cybersécurité est généralement utilisé pour décrire l'ensemble des mesures de sécurité ou pratiques adoptées pour protéger un ordinateur ou un système informatique contre un accès non autorisé ou une attaque. Dans l'IACS, les problèmes principaux résident dans le fait qu'un accès indésirable ou des attaques peuvent empêcher la bonne exécution des fonctions l'IACS dans les délais exigés.

En général, lorsqu'un problème difficile se pose, l'approche technique consiste à subdiviser le problème en parties plus petites et à traiter méthodiquement chacune de ces parties. Cette approche est valable pour traiter les risques liés à la cybersécurité des IACS. Cependant, l'erreur fréquemment commise consiste à traiter le problème de cybersécurité d'un système à la fois. La cybersécurité est un défi beaucoup plus vaste pour lequel il convient de prendre en considération l'ensemble des composants IACS ainsi que les politiques, les procédures, les pratiques qui encadrent ces IACS et le personnel qui les utilise. La mise en œuvre d'un système de gestion d'une telle ampleur peut exiger une évolution culturelle de l'organisation.

Traiter le problème de cybersécurité au niveau d'une organisation complète peut sembler une tâche impossible. Il n'existe pas de livre de recettes simples pour la sécurité ni de "modèle à taille unique" pour les pratiques de sécurité. La sécurité absolue peut être atteinte, mais cela n'est pas souhaitable, car atteindre cet état de quasi-perfection se ferait au prix d'une certaine perte de fonctionnalité. La sécurité est un équilibre entre les risques et les coûts.

Aucune situation ne ressemble à une autre. Dans certaines situations, le risque peut être lié aux facteurs de santé, de sécurité et d'environnement (HSE – health, safety and environmental) plutôt qu'à un impact purement économique. Le risque peut être une conséquence irréversible plutôt qu'un contretemps financier temporaire. Par conséquent, un ensemble prédéfini de pratiques de sécurité obligatoires peut être soit trop restrictif et sans doute très coûteux à mettre en œuvre, soit insuffisant pour prendre en considération le risque.

Le présent document prend en charge le besoin de prise en considération de la cybersécurité d'un IACS opérationnel en spécifiant des exigences pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du programme de sécurité (SP – security program) d'un IACS (SP IACS). La mise en œuvre consciencieuse de ces exigences offre des capacités de sécurité destinées à ramener les risques de sécurité pour l'IACS à un niveau tolérable. Ces exigences sont définies de manière à être indépendantes d'une mise en œuvre, ce qui permet aux propriétaires d'actif de choisir les approches les mieux adaptées à leurs besoins. L'IEC 62443-3-2 [1] [1] décrit la méthodologie qui permet de traiter les risques de cybersécurité lors de la conception d'un IACS, d'identifier les risques et de choisir des exigences de sécurité et des capacités associées appropriées pour un SP IACS.

Ces technologies disponibles dans le commerce (COTS – commercial-off-the-shelf) ne sont généralement pas assez renforcées ou assez rigoureusement conçues pour les environnements IACS dans lesquels elles peuvent introduire des vulnérabilités et des menaces supplémentaires pour l'IACS.

---

1 Les chiffres entre crochets renvoient à la Bibliographie.

Lorsque les technologies COTS sont utilisées dans un IACS, elles sont souvent configurées de manière à satisfaire aux besoins fonctionnels et aux contraintes opérationnelles spécifiques de ce système. Par exemple, la gestion des événements de sécurité dans les produits COTS peut être configurée différemment pour les applications IACS et pour les applications de technologie de l'information (TI) classiques. Les équipements COTS types sont conçus pour des environnements dont l'objectif principal est la protection de l'information. Les objectifs principaux d'un IACS sont la préservation de la santé, de la sécurité et de l'environnement dans l'installation, ainsi que la réduction le plus possible de l'impact opérationnel et professionnel sur le fonctionnement de l'installation. Les technologies COTS peuvent être utilisées dans les applications IACS, mais il est nécessaire que le propriétaire d'actif comprenne les risques associés à leur utilisation.

Les organisations peuvent essayer d'utiliser les solutions existantes de cybersécurité TI et professionnelles pour résoudre la sécurité des IACS, sans comprendre les conséquences. Nombre de ces solutions peuvent être appliquées aux équipements IACS, mais il est important qu'elles le soient de façon correcte pour éviter toute conséquence désastreuse et indésirable. Par exemple, dans un IACS, la disponibilité peut avoir une priorité plus élevée que la confidentialité, contrairement aux applications TI classiques.

Les propriétaires d'actifs peuvent souhaiter appliquer leur SP IACS dans l'ensemble de l'organisation pour satisfaire aux besoins, aux objectifs, aux exigences de sécurité, aux processus d'activité et aux processus de travail de l'organisation, ainsi qu'à sa taille et à sa structure. Tous ces facteurs d'influence sont dynamiques et varient probablement avec le temps. L'adoption d'un SP IACS est donc une décision stratégique pour l'organisation.

L'efficacité d'un SP IACS est souvent améliorée par la coordination ou l'intégration avec les processus de l'organisation et avec l'ensemble du système de management de la sécurité de l'information (SMSI). Par exemple, la fonction de sécurité peut être ajoutée aux processus de la chaîne logistique de l'organisation afin d'exiger une telle fonction dans la conception des processus, des systèmes et des commandes. Il est également prévu que le SP IACS soit dimensionné par rapport aux besoins de l'IACS et de l'organisation.

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

1 Domaine d'application

La présente partie de l'IEC 62443 spécifie les exigences de politiques et de procédures du programme de sécurité (SP) du propriétaire d'actif pour un système d'automatisation et de commande industrielle (IACS) opérationnel. Le présent document utilise, au sens large, la définition et le domaine d'application de ce qui constitue un IACS décrit dans l'IEC TS 62443-1-1. Dans le contexte du présent document, le propriétaire d'actif inclut également l'opérateur de l'IACS.

Le présent document reconnaît que la durée de vie d'un IACS peut dépasser vingt ans et que de nombreux systèmes patrimoniaux contiennent du matériel et du logiciel qui ne sont plus pris en charge. Par conséquent, le SP de la plupart des systèmes patrimoniaux ne concerne qu'un sous-ensemble des exigences définies dans le présent document. Les exigences en matière de correctifs de sécurité, par exemple, ne peuvent pas être satisfaites si l'IACS ou le logiciel composant n'est plus pris en charge. De même, le logiciel de sauvegarde de la plupart des systèmes plus anciens n'est pas disponible pour tous les composants de l'IACS. Le présent document ne précise pas qu'un IACS doit satisfaire à ces exigences techniques. Il indique qu'il est nécessaire que le propriétaire d'actif dispose de politiques et de procédures relatives à ces types d'exigences. Dans le cas où le propriétaire d'actif possède des systèmes patrimoniaux qui ne comportent pas des capacités techniques natives, des mesures de sécurité compensatoires peuvent faire partie des politiques et procédures spécifiées dans le présent document.

Le présent document reconnaît également que toutes les exigences spécifiées dans le présent document ne s'appliquent pas à tous les IACS. Par exemple, les exigences associées à certaines technologies (telles la technologie sans-fil) ou fonctions (comme l'accès distant) ne s'appliquent pas aux IACS qui ne comportent pas ces technologies ou fonctions. De même, les exigences en matière de protection contre les programmes malveillants ne sont pas toutes applicables lorsqu'aucun appareil des systèmes n'est équipé de logiciels anti-programme malveillant. Par conséquent, le présent document indique qu'il est nécessaire que le propriétaire d'actif identifie les exigences de sécurité IACS applicables à ses IACS dans leurs environnements d'exploitation spécifiques.

Les éléments d'un SP IACS décrits dans le présent document définissent des exigences en matière de capacités de sécurité qui s'appliquent au fonctionnement sécurisé d'un IACS. Bien que le fonctionnement sécurisé d'un IACS relève en définitive de la responsabilité du propriétaire d'actif, la mise en œuvre des capacités de sécurité intègre souvent les contributions de ses fournisseurs de service et fournisseurs de produit. Pour cette raison, le présent document donne des recommandations aux propriétaires d'actif en spécifiant des exigences de sécurité pour leurs fournisseurs de service et fournisseurs de produit, et en faisant référence à d'autres parties de l'IEC 62443 (toutes les parties).

La Figure 1 représente les rôles et responsabilités de sécurité du propriétaire d'actif, du ou des fournisseurs de service et du ou des fournisseurs de produit d'un IACS, et les relations qu'ils entretiennent entre eux et avec la Solution d'Automatisation. La Solution d'Automatisation est une solution technique qui met en œuvre les fonctions de contrôle/sécurité et les fonctions complémentaires nécessaires à l'IACS. Elle est constituée de composants matériels et logiciels qui ont été installés et configurés pour fonctionner dans l'IACS. L'IACS est une combinaison de la Solution d'Automatisation et des mesures organisationnelles nécessaires à sa conception, son déploiement, son exploitation et à sa maintenance.

Certaines de ces capacités reposent sur l'application appropriée des capacités de maintenance et d'intégration définies dans l'IEC 62443-2-4 [2] et des capacités de sécurité techniques définies dans les normes IEC 62443-3-3 [3] et IEC 62443-4-2 [4].

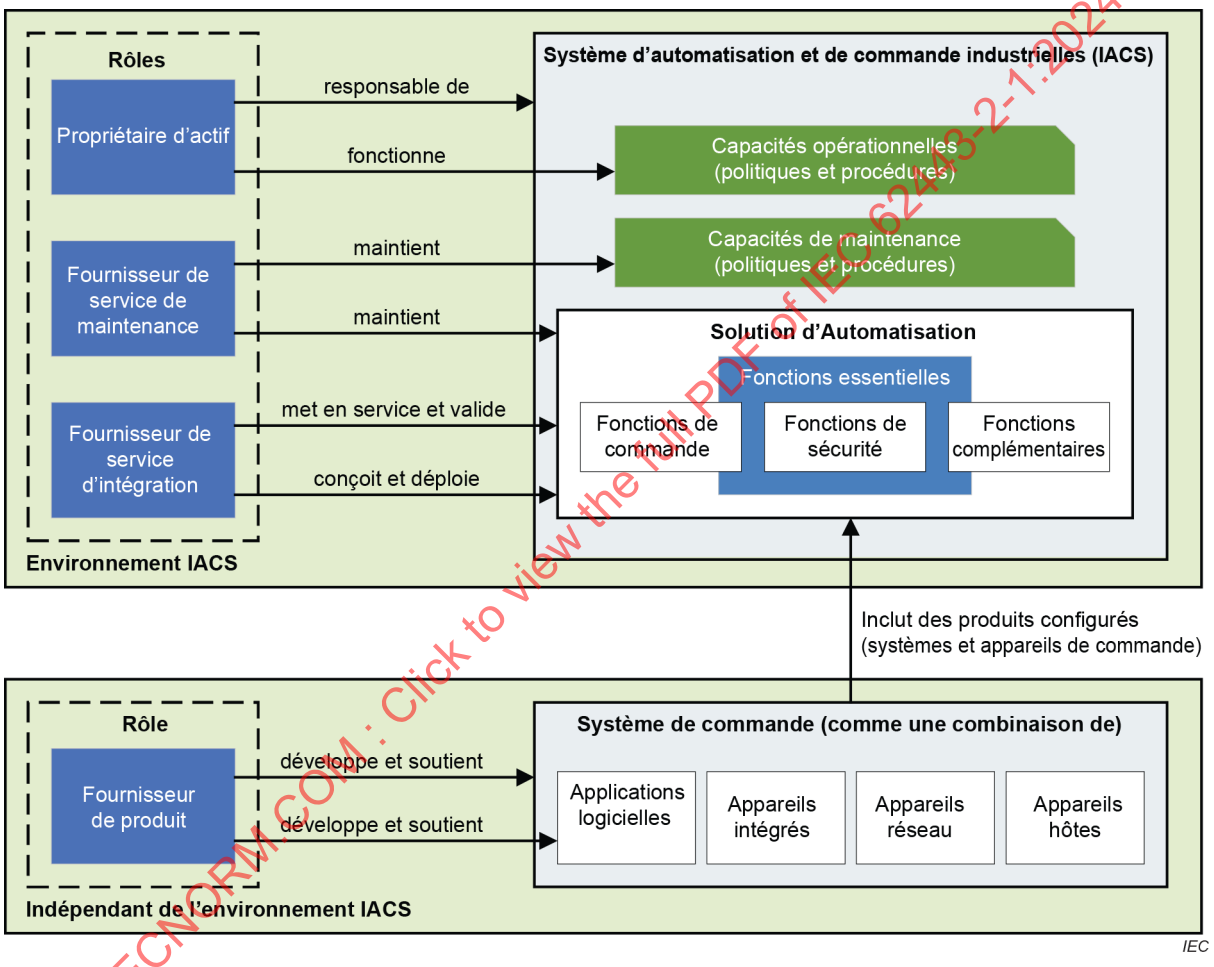

Figure 1 – Rôles et responsabilités dans la série IEC 62443

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

3 Termes, définitions, abréviations et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC TS 62443-1-1, ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

3.1.1
droit d'accès
permission d'accéder aux ressources d'un système ou privilège d'exécuter des fonctions système

Note 1 à l'article: Les permissions sont généralement des droits d'accéder à des ressources telles que les fichiers exécutables et les données, tandis que les privilèges sont généralement des droits d'exécuter des appels de fonctions fournis par le système d'exploitation (OS).

3.1.2
propriétaire d'actif
rôle organisationnel responsable en dernier ressort d'un ou de plusieurs IACS

Note 1 à l'article: Ce terme est utilisé à la place du terme générique "utilisateur final" pour marquer la distinction.

Note 2 à l'article: Dans le contexte du présent document, "propriétaire d'actif" inclut également l'opérateur de l'IACS.

[SOURCE: IEC 62443-3-3:2013, 3.1.2, modifié – "individu ou entreprise chargé(e)" a été remplacé par "rôle organisationnel responsable en dernier ressort" afin de mieux refléter le rôle. Dans la Note 1 à l'article, "Le terme 'propriétaire d'actif' est utilisé" a été remplacé par "Ce terme est utilisé". L'ancienne Note 2 à l'article a été supprimée. Dans la nouvelle Note 2 à l'article, "de la présente norme, le propriétaire d'actif" a été remplacé par "du présent document, 'propriétaire d'actif'".]

3.1.3
solution d'automatisation
système de commande et tous les composants matériels et logiciels complémentaires qui ont été installés et configurés pour fonctionner dans un IACS

Note 1 à l'article: Dans le présent document, la Solution d'Automatisation est utilisée comme un nom propre.

Note 2 à l'article: La différence entre le système de commande et la Solution d'Automatisation est que le système de commande est intégré dans la conception de la Solution d'Automatisation (un nombre spécifique de stations de travail, de contrôleurs et d'appareils dans une configuration spécifique, par exemple), qui est alors mise en œuvre. La configuration obtenue est appelée Solution d'Automatisation.

Note 3 à l'article: La Solution d'Automatisation peut être constituée de composants en provenance de plusieurs fournisseurs, y compris d'un fournisseur de produit de système de commande.

3.1.4
mesure de sécurité compensatoire
mesure de sécurité employée au lieu de ou en plus des capacités de sécurité inhérentes afin de satisfaire à une ou plusieurs exigences de sécurité

EXEMPLE 1 (Au niveau du composant) Une armoire verrouillée près d'un contrôleur ne comportant pas de mesures de sécurité de contrôle de cyberaccès suffisantes.

EXEMPLE 2 (Au niveau de la zone/du système de commande) Un contrôle d'accès physique (protections, grilles et armes) qui permet d'assurer la protection d'une pièce de commande et de restreindre l'accès à un groupe de personnel connu afin de compenser l'exigence technique du personnel identifié uniquement par l'IACS.

EXEMPLE 3 (Au niveau du composant) Un automate programmable (PLC, programmable logic controller) d'un fournisseur de produit ne satisfait pas aux capacités de contrôle d'accès d'un propriétaire d'actif, le fournisseur de produit installe donc un pare-feu devant le PLC et le vend en tant que système.

3.1.5
consultant
sous-traitant qui donne des conseils d'expertise ou des recommandations à leurs clients, tels que les fournisseurs de produit, fournisseurs de service d'intégration et de maintenance et propriétaires d'actif

3.1.6
appareil
actif qui incorpore un ou plusieurs processeurs ayant la capacité d'envoyer ou de recevoir des données/commandes de ou vers un autre actif

EXEMPLES Contrôleurs, interfaces homme-machine (IHM), automates programmables, terminaux à distance (RTU), émetteurs, actionneurs, valves, commutateurs réseau, etc.

3.1.7
niveau de maturité
méthode qualitative qui permet de caractériser la capacité d'une organisation à mettre en œuvre les exigences de sécurité conformément aux politiques et procédures documentées, ainsi que ses performances historiques en la matière

3.1.8
support portable
appareils portables qui contiennent des capacités de stockage des données, pouvant être utilisés pour copier physiquement des données à partir d'un élément de matériel et les transférer à un autre

Note 1 à l'article: Les types de supports portables incluent, entre autres: disque compact (CD)/ disque numérique polyvalent (DVD)/Blu-raymedia, périphériques de stockage à bus série universel (USB), téléphones intelligents, mémoire flash, disques statiques à semiconducteurs, disques durs, ordinateurs de poche et ordinateurs portables.

Note 2 à l'article: Le terme "support amovible" est un autre terme souvent utilisé pour "support portable".

3.1.9
fournisseur de produit
rôle organisationnel responsable de la fabrication et de la prise en charge des produits matériels et/ou logiciels de l'IACS

Note 1 à l'article: Ce terme est utilisé à la place du terme générique "fournisseur" pour marquer la distinction.

3.1.10
capacité de sécurité
mesure, fonctionnalité ou mécanisme technologique ou procédural qui peut être utilisé(e) pour assurer la protection contre les cyberattaques et les attaques contre la sécurité physique

Note 1 à l'article: Les capacités de sécurité sont généralement mises en œuvre par une combinaison de moyens technologiques et procéduraux. Le terme "contre-mesure" est souvent utilisé pour décrire la mise en œuvre de la "capacité de sécurité".

Note 2 à l'article: Le terme "commande" est également utilisé pour décrire ce concept dans certains contextes. Le terme "capacité de sécurité" a été choisi pour le présent document afin d'éviter toute confusion avec le terme "commande" dans le contexte d'une "commande de processus".

3.1.11
faille de sécurité
violation de la sécurité d'un système telle qu'une (1) divulgation ou modification non autorisée d'informations, (2) une action/exécution de fonctions ou (3) un refus de service (DoS) est susceptible de s'être produit(e)

Note 1 à l'article: Une faille de sécurité représente une violation de la sécurité d'un système ou une infraction à ses politiques de sécurité. Elle est indépendante de l'incidence ou de l'incidence potentielle du système.

[SOURCE: IEC 62443-2-4:2023, 3.1.20, modifié – Dans la définition, "(2) un refus de service est susceptible de s'être produit(e)" a été remplacé par "(2) une action/exécution de fonctions ou (3) un refus de service (DoS) est susceptible de s'être produit(e)"]

3.1.12
incident de sécurité
faille de sécurité qui revêt une certaine importance pour le propriétaire d'actif ou tentative infructueuse de compromettre le système dont le résultat est susceptible de revêtir une certaine importance pour le propriétaire d'actif

Note 1 à l'article: Le terme "une certaine importance" se rapporte à l'environnement dans lequel la faille de sécurité est détectée. Par exemple, la même faille peut être déclarée comme incident de sécurité dans un environnement et pas dans un autre. Les activités de tri sont souvent utilisées par les propriétaires d'actifs pour évaluer les failles de sécurité et identifier celles qui sont suffisamment importantes pour être considérées comme des incidents.

Note 2 à l'article: Dans certains environnements, les tentatives infructueuses de compromettre le système, telles que les tentatives de connexion infructueuses, sont considérées comme suffisamment importantes pour être classées comme des incidents de sécurité.

[SOURCE: IEC 62443-2-4:2023, 3.1.21]

3.1.13
système de management de la sécurité
SMS
ensemble d'éléments corrélés ou interactifs d'un organisme qui visent à établir des politiques et des objectifs de sécurité, ainsi qu'une série de processus systématiques permettant d'atteindre ces objectifs

Note 1 à l'article: Cette définition repose sur la définition et la description du terme "système de management" en 3.41 de l'ISO/IEC 27000:2018 [5].

3.1.14
correctif de sécurité
modification logicielle incrémentielle en vue de résoudre une vulnérabilité de sécurité, un bogue, un problème de fiabilité ou d'opérabilité (mise à jour), ou d'ajouter une nouvelle fonctionnalité (mise à niveau)

Note 1 à l'article: Pour les besoins de cette définition, un micrologiciel est considéré comme un logiciel.

Note 2 à l'article: Les correctifs logiciels peuvent résoudre les vulnérabilités connues ou potentielles, ou tout simplement améliorer la sécurité du composant logiciel, y compris la fiabilité de son fonctionnement.

3.1.15
programme de sécurité
SP
portefeuille des services de sécurité, y compris les services d'intégration et les services de maintenance, et leurs politiques, procédures et produits connexes qui sont applicables à l'IACS

Note 1 à l'article: Le SP pour les propriétaires d'actif IACS se rapporte aux politiques et procédures qu'ils ont définies pour résoudre les problèmes de cybersécurité de l'IACS. Il peut s'agir de mesures de sécurité techniques, procédurales, physiques et compensatoires utilisées pour réduire la surface d'attaque contre la cybersécurité.

Note 2 à l'article: L'abréviation "SP" est dérivée du terme anglais développé correspondant "security program".

[SOURCE: IEC 62443-2-4:2023, 3.1.23, modifié – Ajout de l'abréviation "SP". Dans la Note 1 à l'article, "programme de sécurité" a été remplacé par "SP", "fournisseurs de services" a été remplacé par "propriétaires d'actif", et "Il peut s'agir de mesures de sécurité techniques, procédurales, physiques et compensatoires utilisées pour réduire la surface d'attaque contre la cybersécurité." a été ajouté]

3.1.16
fournisseur de service
rôle organisationnel chargé de fournir des services et des prestations connexes pour l'IACS conformément à un accord conclu avec le propriétaire d'actif

Note 1 à l'article: Ce terme est utilisé à la place du terme générique "fournisseur" pour marquer la distinction.

3.1.17
service logiciel
programme logiciel installé et géré par un logiciel d'infrastructure plutôt que par ou pour le compte d'un utilisateur connecté, généralement sans interface utilisateur propre

Note 1 à l'article: Certains systèmes d'exploitation (OS – operating system) permettent aux utilisateurs connectés qui disposent de privilèges élevés de démarrer/arrêter des services logiciels.

3.1.18
risque tolérable
niveau de risque jugé acceptable pour une organisation

Note 1 à l'article: Il convient que les organisations tiennent compte des exigences légales lorsqu'elles établissent le risque tolérable. Des recommandations supplémentaires relatives à l'établissement des risques tolérables peuvent être consultées dans les normes ISO 31000 [6] et NIST SP 800-39 [7].

Note 2 à l'article: L'IEC 62443-3-2 fournit des recommandations en vue d'établir le risque tolérable.

[SOURCE: IEC 62443-3-2:2020, 3.1.22, modifié – La Note 2 à l'article a été ajoutée.]

3.2 Abréviations et acronymes

Ce paragraphe définit les abréviations et les acronymes utilisés dans le présent document.

ANIMA	(autonomic network integrated model and approach) modèle et approche intégrés de mise en réseau autonome[2]
ANSI	(american National Standards Institute) institut national américain de normalisation
API	(application programming interface) interface de programmation d'application
BCP	(business continuity plan) plan de continuité d'activité
BOOTP	(bootstrap protocol) protocole d'amorce/protocole BOOTP

[2] IETF (Internet Engineering Task Force)

BRSKI	(bootstrapping of a remote secure key infrastructure) amorçage d'une infrastructure de clé sécurisée distante[2]
C2M2	(cybersecurity capability maturity model) modèle de stabilisation des capacités de cybersécurité[3]
CD	(compact disc) disque compact
CDA	(critical digital asset) actif critique numérique
CSF	(cybersecurity Framework) cadre de cybersécurité[4]
CIS	(center for Internet Security) centre pour la sécurité Internet
CMMI	(capability maturity model integration) intégration du modèle de stabilisation des capacités
CMMI-SVC	(CMMI for services) CMMI pour les services
CONOPS	(concept of operations) concept d'opérations
COTS	(commercial-off-the-shelf) disponible dans le commerce
DA	(digital asset) actif numérique
DES	(data encryption standard) norme de chiffrement de données
DHCP	(dynamic host control protocol) protocole DHCP/Protocole de configuration dynamique des hôtes
DMZ	(demilitarized zone) zone démilitarisée
DOD	(Department of Defense) Département de la Défense[5]
DOE	(Department of Energy) Département de l'Énergie[5]
DoS	(denial of service) refus de service
DRP	(disaster recovery plan) plan de reprise après sinistre
DVD	(digital versatile disc) disque numérique polyvalent
EAP	(Extensible Authentication Protocol) protocole d'authentification extensible[2]
GPS	(global positioning system) système mondial de localisation
IHM	interface homme-machine
HSE	(health, safety and environment) santé, sécurité et environnement
IACS	(industrial automation and control system(s)) système(s) d'automatisation et de commande industrielle
IEC	(International Electrotechnical Commission) Commission Électrotechnique Internationale
IEEE	(Institute of Electrical and Electronics Engineers) Institut des ingénieurs électriciens et électroniciens
IETF	Internet Engineering Task Force (groupe de travail IETF)
IIS	(Internet Information Services) services de ressources Internet[6]
IP	(internet protocol) protocole Internet

---

3 Département de l'Énergie des États-Unis (US DOE – United States Department of Energy)

4 Institut national des normes et de la technologie (NIST – National Institue of Standards and Tehcnology) des États-Unis

5 États-Unis

6 Microsoft®. Cette appellation commerciale est donnée à des fins d'intérêt public ou de sécurité publique. Cette information est donnée à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve l'emploi ainsi désigné.

ISA	(International Society of Automation) Société internationale d'automatisation
SMSI	système de management de la sécurité de l'information
ISO	(International Organization for Standardization) Organisation internationale de normalisation
TI	technologie de l'information
MFA	(multifactor authentication) authentification à plusieurs facteurs
ML	(maturity level) niveau de maturité
NIST	(National Institute of Standards and Technology) Institut national des normes et de la technologie[5]
NTP	(network time protocol) protocole de temps réseau
OPC	(open platform communications) communications sur plateforme ouverte
OS	(operating system) système d'exploitation
PII	(personally identifiable information) informations personnellement identifiables
PIN	(personal identification number) numéro d'identification personnel
PLC	(programmable logic controller) automate programmable
RBAC	(role-based access control) contrôle d'accès basé sur le rôle
RF	radiofréquence
RFC	(request for comment) demande de commentaires[2]
RFQ	(request for quote) appel d'offres
RTU	(remote terminal unit) terminal à distance
SI	système international d'unités
SL	(security level) niveau de sécurité
SL-T	(target SL) SL cible
SP	(security program) programme de sécurité
SPE	(SP elements) éléments SP
SPR	(security program rating) indice de programme de sécurité
SPS	(security protection scheme) système de protection de la sécurité
SSID	(service set identifier) identificateur d'ensemble de service
TCP	(transmission control protocol) protocole de contrôle d'émission
UAC	(user account control) contrôle de compte de l'utilisateur[6]
UDP	(user datagram protocol) protocole UDP
USB	(universal serial bus) bus série universel
VPN	(virtual private network) réseau privé virtuel

3.3 Conventions

Une exigence sans qualificatif est identique à une exigence avec un qualificatif d'exigence fondamentale (BR – Basic Requirement). Par exemple, ORG 1.1 et ORG 1.1 BR constituent la même exigence.

Une exigence dont les champs numériques sont précédés d'un 0 est identique à une exigence dont les champs numériques ne sont pas précédés d'un 0. Par exemple, SR 2.03 et SR 2.3 constituent la même exigence.

Les conventions ci-dessus tiennent compte des différentes façons dont les exigences sont désignées dans les autres parties de la série IEC 62443.

Le terme "Solution d'Automatisation" est utilisé comme un nom propre (et donc avec des majuscules) dans le présent document afin d'éviter toute confusion avec d'autres utilisations de ce terme.

4 Concepts

4.1 Utilisation du présent document

4.1.1 Rôles applicables

Le présent document s'applique principalement au rôle de propriétaire d'actif et, dans une moindre mesure, aux rôles de fournisseur de service et de fournisseur de produit (voir la Figure 1). La série IEC 62443 considère comme des propriétaires d'actif les organisations responsables de l'IACS. Les organisations responsables de l'élaboration et de la prise en charge du matériel et des logiciels utilisés dans l'IACS remplissent le rôle de fournisseur de produit. Les organisations qui fournissent des services d'intégration pour l'IACS remplissent le rôle de fournisseur de service d'intégration, tandis que celles qui fournissent des services de maintenance remplissent le rôle de fournisseur de service de maintenance. Ces rôles et responsabilités sont représentés à la Figure 1.

Il n'est pas rare que l'organisation agissant en tant que propriétaire d'actif exécute non seulement tout ou partie des rôles de fournisseur de service d'intégration ou de maintenance, mais aussi tout ou partie du rôle de fournisseur de produit pour certains composants de l'IACS. Dans ces cas, les 4.1.2 et 4.1.3 s'appliquent à l'organisation propriétaire d'actif.

Dans d'autres cas, le propriétaire d'actif peut signer un contrat avec un ou plusieurs fournisseurs de produit et/ou de service pour le déploiement et la maintenance de l'IACS. Dans de pareils cas, ces organisations peuvent jouer un ou plusieurs rôles de fournisseur de service d'intégration, de fournisseur de service de maintenance ou de fournisseur de produit.

De même, une partie ou la totalité d'une installation peut être exploitée par une entité autre que le propriétaire d'actif. Dans tous les cas, les exigences spécifiées dans le présent document s'appliquent au propriétaire d'actif. Le propriétaire d'actif peut avoir un programme de chaîne logistique, pour les fournisseurs de produit et les fournisseurs de service, dont les exigences de sécurité sont dérivées du présent document.

4.1.2 Utilisation du présent document par les propriétaires d'actif

4.1.2.1 Atténuation des risques

Le présent document définit les exigences pour les propriétaires d'actif des SP IACS. En général, un SP consiste à définir, à mettre en œuvre et à maintenir des capacités procédurales, humaines et technologiques destinées à atténuer les risques de cybersécurité d'un IACS.

Le principal objectif de chacune des exigences du SP contenues dans le présent document est d'atténuer les risques. Cependant, l'atténuation des risques peut prendre différentes formes, telles que l'atténuation de la probabilité d'un incident, l'atténuation de l'impact d'un incident, l'atténuation du délai de récupération d'un incident, etc. Dans de nombreux cas, une exigence SP atténue le risque global de plusieurs façons.

Elles permettent également aux utilisateurs du présent document de choisir une combinaison d'approches architecturales (par exemple, l'utilisation de zones de sécurité), de politiques, de procédures et de technologies les plus appropriées pour leurs applications.

L'IEC 62443-3-2 [1] décrit une méthodologie qui permet de résoudre les risques de cybersécurité dans une conception de Solution d'Automatisation de l'IACS, y compris l'utilisation de niveaux de sécurité (SL) et de zones de sécurité.

Un SP IACS est généralement spécifique à un IACS individuel, dont l'installation peut en avoir plusieurs. Lorsqu'il y en a plus d'un, il est recommandé de définir un seul SP de haut niveau d'installation dont les exigences sont répercutées en cas de besoin vers les SP IACS individuels. Chaque SP IACS est spécifique à la disponibilité, à la confidentialité et à l'intégrité des ressources de production spécifiques de son IACS, y compris contrôleurs, appareils de terrain et autres appareils intégrés, ainsi qu'à la protection des secrets commerciaux et autres informations confidentielles de l'IACS.

Il convient qu'un SP IACS soit compatible avec les autres SP IACS installés dans l'installation, mais cela n'est pas toujours pratique ni réalisable, car la technologie et les risques associés à un IACS peuvent être très différents de ceux d'un autre IACS.

Il est attendu que les SP IACS complètent également le système de management de la sécurité de l'information (SMSI) d'une organisation propriétaire d'actif, afin d'assurer, de façon coordonnée, la sécurité opérationnelle et informationnelle du site. Les exigences du SMSI ne répondent généralement pas de manière spécifique à tous les besoins opérationnels et de sécurité d'un IACS. Le présent document, ainsi que les parties connexes de la série IEC 62443, définissent les exigences nécessaires pour assurer la sécurité opérationnelle et informationnelle d'un IACS tout au long de son cycle de vie.

Il convient que les SP IACS soient, dans la mesure du possible, compatibles avec le système SMSI de l'organisation. Toutefois, une cohérence totale avec ce système n'est généralement pas possible en raison d'objectifs contradictoires des systèmes de technologie de l'information (TI) et des IACS, et surtout de contraintes essentielles associées à la disponibilité et aux performances des installations de production. En outre, certaines exigences de sécurité informationnelle qui s'appliquent à la protection des aspects TI de l'IACS peuvent être mises en œuvre différemment pour le système TI et l'IACS.

NOTE Il est possible d'améliorer l'alignement des SMSI et des SP IACS en harmonisant les buts et objectifs de sécurité entre les deux systèmes et en documentant formellement leurs similitudes et leurs différences.

Par exemple, les politiques de correctif peuvent être différentes entre les SP IACS et les SMSI par suite des différences en matière d'exigences de disponibilité entre les stations de travail d'opérateur IACS et les stations de travail bureautiques SMSI. Les contraintes opérationnelles comme celle-ci se traduisent généralement par des ensembles différents de politiques et procédures pour les SP IACS et les SMSI.

Étant donné que les IACS combinent du personnel, du matériel, des logiciels et des processus, les SP des propriétaires d'actif conformes au présent document sont constitués de:

a) capacités organisationnelles qui:
   1) comprennent un SMSI définissant généralement les politiques et pratiques au niveau d'une organisation pour les systèmes TI; et
   2) assurent la coordination entre le SMSI et l'infrastructure TI dans son environnement;
b) capacités de sécurité techniques mises en œuvre dans les composants matériels et logiciels de la Solution d'Automatisation de l'IACS (voir la Figure 1); et
c) processus liés à la sécurité, utilisés pour déployer, configurer et exploiter de manière sécurisée l'IACS, ainsi que pour maintenir ses capacités de sécurité techniques.

4.1.2.2 Mise en œuvre du SP

Le présent document fournit aux propriétaires d'actif IACS un cadre pour développer et faire évoluer leurs SP. La mise en œuvre efficace d'un SP pour un IACS implique la définition et l'exécution des capacités globales qui:

a) traitent de tous les aspects de la gestion des risques de sécurité, depuis l'identification des objectifs programmatiques jusqu'au fonctionnement quotidien; et

b) incluent un audit continu pour la conformité et l'amélioration du programme.

Un engagement organisationnel de haut en bas est indispensable pour le succès du SP IACS. La sécurité d'un IACS est une responsabilité partagée par tous les membres de l'organisation et ses prestataires/consultants, et l'intégration de la sécurité dans les activités quotidiennes des membres permet à l'organisation de fonctionner plus efficacement et de protéger l'IACS. Les SP fondés sur le présent document varient en principe de manière significative selon l'organisation et du secteur d'activité du propriétaire d'actif. L'application du présent document à un SP du propriétaire d'actif commence par la détermination des exigences applicables parmi les exigences qui y sont définies. Les exigences sont souvent déterminées comme applicables selon l'architecture et les caractéristiques de l'IACS, de l'environnement dans lequel l'IACS fonctionne et des risques de sécurité qui lui sont associés (pour de plus amples informations sur la gestion des risques de sécurité de l'IACS, voir l'Annexe B et l'IEC 62443-3-2).

Il convient que les propriétaires d'actif mettent en œuvre, pour chaque exigence applicable, la combinaison appropriée de capacités techniques et de capacités orientées processus. Les capacités techniques sont des caractéristiques de l'IACS et de ses composants, et les capacités orientées processus sont des processus organisationnels utilisés pour intégrer/déployer l'IACS, le faire fonctionner et le maintenir.

Des références croisées à l'IEC 62443-3-3 et à l'IEC 62443-4-2 sont fournies pour les capacités techniques et à l'IEC 62443-2-4 pour les capacités d'intégration et de maintenance. Les propriétaires d'actif peuvent se fonder sur ces capacités sous références croisées pour déterminer les capacités techniques et orientées processus à mettre en œuvre et pour spécifier des exigences de sécurité à l'endroit de leurs fournisseurs de produit et de leurs fournisseurs de service.

Il peut s'avérer impossible ou peu pratique pour un propriétaire d'actif d'établir et de mettre en œuvre un SP qui satisfasse à la fois à toutes les exigences applicables. Par conséquent, les propriétaires d'actif peuvent, s'il y a lieu, adopter une approche par étapes pour mettre au point leur SP. Dans ce cas, il convient de mettre au départ l'accent sur la gestion efficace des risques les plus élevés.

Le présent document reconnaît également qu'il peut être utile pour les propriétaires d'actif de mettre en œuvre un SP qui satisfait aux exigences du présent document d'une manière compatible avec les autres spécifications de sécurité. Par conséquent, l'Annexe A fait état de références croisées entre chaque exigence du présent document et les exigences qui figurent dans des références externes connexes, tout particulièrement l'ISO/IEC 27001 [8] et le National Institute of Standards and Technology Cybersecurity Framework (NIST CSF, Cadre de cybersécurité du NIST) [9]. À l'aide de ces références croisées, le propriétaire d'actif peut s'aligner sur les exigences externes connexes à la mise en œuvre de chaque capacité de son SP.

NOTE Dans le contexte d'un IACS, toutes les références à "management de l'information" dans l'ISO/IEC 27001 renvoient à l'IACS.

Certains IACS patrimoniaux peuvent empêcher la mise en œuvre directe d'exigences spécifiques ou de sous-ensembles d'exigences applicables. Dans ce cas, il convient de mettre en œuvre des mesures de sécurité compensatoires dans la mesure du possible.

4.1.2.3 Interfaces organisationnelles

Bien que le propriétaire d'actif soit ultimement responsable du fonctionnement de l'IACS et des processus contrôlés par ce dernier, des responsabilités associées sont souvent assumées avec le soutien des fournisseurs de service et des fournisseurs de produit. Les rôles et responsabilités juridiques, opérationnels et techniques respectifs de ces entités sont généralement définis dans des contrats et des documents d'achat, tels que les appels d'offres (RFQ) et les commandes d'achat. Dans l'idéal, les exigences de sécurité sont incluses dans ces documents.

De tels contrats peuvent ne pas être nécessaires lorsque le fournisseur de service ou le fournisseur de produit fait partie de l'organisation du propriétaire d'actif, mais les exigences de sécurité relatives aux produits et aux processus d'intégration ou de maintenance sont toujours spécifiées pour l'IACS.

Le présent document fournit à l'Annexe A des références croisées à chaque exigence du présent document et aux exigences des fournisseurs de service et de produit spécifiées dans l'IEC 62443-2-4, l'IEC 62443-3-3 et l'IEC 62443-4-2. Les propriétaires d'actif peuvent utiliser ces références croisées pour faciliter l'élaboration d'exigences de sécurité pour les documents d'achat des fournisseurs de service et des fournisseurs de produit. Ces documents référencés et les références croisées aux exigences qui figurent à l'Annexe A du présent document peuvent aider les propriétaires d'actif, les fournisseurs de service et les fournisseurs de produit à s'accorder sur un ensemble cohérent d'exigences lors des achats.

4.1.3 Utilisation du présent document par les fournisseurs de service et les fournisseurs de produit

Comme cela est indiqué en 4.1.2.3, les normes IEC 62443-2-4, IEC 62443-3-3 et IEC 62443-4-2 définissent des exigences de sécurité pour les produits et services proposés par les propriétaires d'actif. Ces exigences étant liées par références croisées à celles du présent document à l'Annexe A, le présent document peut offrir un contexte utile aux fournisseurs de service et aux fournisseurs de produit.

4.2 Définitions des niveaux de maturité (ML)

Les exigences du SP définies dans le présent document à partir de 5.3 ont été spécifiées comme étant indépendantes de toute mise en œuvre. Cette approche donne une certaine latitude au propriétaire d'actif dans l'application du présent document tout en satisfaisant aux besoins de son organisation.

Le Tableau 1 définit une plage de niveaux de maturité (ML), allant des processus initiaux aux processus affinés et améliorés, pour prendre en charge l'indépendance de mise en œuvre des mesures de sécurité des processus qui satisfont à ces exigences. Les niveaux de maturité (ML) s'appliquent indépendamment pour les exigences de SP, et il convient que le propriétaire d'actif choisisse le ML le plus approprié pour une exigence en se fondant sur les objectifs de gestion des risques (voir l'IEC 62443-3-2). Bien que le propriétaire d'actif puisse avoir des politiques et des procédures qui satisfont à plusieurs exigences SP, il convient d'évaluer chaque exigence SP de manière indépendante. Voir l'Annexe C pour de plus amples informations sur l'évaluation des ML.

De plus, étant donné que certains propriétaires d'actif peuvent avoir besoin d'adopter une approche par étapes pour élaborer leurs SP, une plage des ML du programme peut s'avérer utile lors de la planification et de la programmation de ces étapes. À noter que d'autres parties de l'IEC 62443 définissant des exigences relatives aux mesures de sécurité des processus, telles que l'IEC 62443-2-4 et l'IEC 62443-4-1 [10], intègrent également le concept de ML.

La plage des ML du présent document est définie par un modèle composé de repères de maturité pour la mise en œuvre des mesures de sécurité des processus. Les repères pour chaque ML sont présentés dans le Tableau 1. Les ML reposent sur le modèle Intégration du modèle de stabilisation des capacités (CMMI) pour les services (CMMI-SVC) [11]. La colonne "Description/Comparaison avec CMMI-SVC" du Tableau 1 présente les relations avec CMMI-SVC.

Tableau 1 – Niveaux de maturité et descriptions

Niveau	CMMI-SVC	Le présent document	Description/Comparaison avec CMMI-SVC
1	Initial	Initial	À ce niveau, les modèles sont foncièrement identiques. Les processus sont exécutés de manière ponctuelle et souvent non documentée (ou pas totalement documentée). La cohérence dans le temps peut donc être difficile à démontrer. NOTE Dans ce contexte, le terme "documenté" fait référence à la procédure d'exécution de ce processus (les instructions détaillées adressées au personnel du fournisseur de service, par exemple) et non pas aux résultats de son exécution. Dans la plupart des IACS, toutes les modifications résultant de l'exécution des processus procéduraux sont souvent documentées.
2	Géré	Géré	À ce niveau, les modèles sont foncièrement identiques, sauf que le présent document reconnaît la possible existence d'un délai significatif entre la définition d'un processus et son exécution ou sa mise en pratique. Par conséquent, les aspects liés à l'exécution de CMMI-SVC Niveau 2 sont reportés au Niveau 3. À ce niveau, il existe une documentation décrivant comment gérer la fourniture et l'exécution de la capacité. Cette documentation peut être sous la forme de procédures écrites ou de programmes de formation rédigés pour l'exécution de la capacité. La discipline reflétée par le niveau ML 2 aide à faire en sorte que les pratiques soient répétables, même en période de stress. Lorsque ces pratiques sont en place, elles sont exécutées et gérées selon leurs plans documentés.
3	Défini	Défini / Mis en pratique	À ce niveau, les modèles sont foncièrement identiques, sauf que les aspects liés à l'exécution de CMMI-SVC Niveau 2 sont inclus ici. Par conséquent, un processus au Niveau 3 est un processus de Niveau 2 qui est mis en pratique dans l'IACS. Les performances d'une pratique de Niveau 3 peuvent être présentées comme étant répétables dans le temps dans l'IACS.
4	Quantitativement géré Optimisation	Amélioration	À ce niveau, les niveaux "Quantitativement géré" et "Optimisaton" de CMMI-SVC sont combinés. Les mesurages adaptés de processus permettent de démontrer l'efficacité et/ou les améliorations des performances du processus. Cela donne lieu à un SP qui améliore le processus par des modifications de technologie/procédure/gestion.

Les processus doivent être documentés à partir du ML 2. Cela inclut la documentation des politiques et procédures, ainsi que de la formation du personnel. En conséquence, les exigences du SP définies dans le présent document ne spécifient pas la nécessité de documentation, car les niveaux de maturité ML 2 et plus l'exigent déjà.

Dans ce modèle de stabilisation, chaque niveau est progressivement plus avancé que le niveau précédent, et s'applique indépendamment pour chaque exigence. Les ML font partie du processus d'évaluation de conformité, par conséquent les propriétaires d'actif doivent déterminer la satisfaction ou non à chaque exigence, et le cas échéant, le ML associé à la mise en œuvre de chaque exigence ou groupe d'exigences.

NOTE Il est prévu pour l'évolution d'un PS que, dans le temps et pour une exigence particulière, un processus évolue à des niveaux plus élevés au fur et à mesure que l'organisation gagne en compétence pour satisfaire aux exigences.

4.3 Niveaux de sécurité (SL)

Les niveaux de sécurité (SL) pour l'IACS représentent la force relative des capacités de sécurité définies pour la Solution d'Automatisation de l'IACS dans l'IEC 62443-3-3 et pour les composants intégrés dans l'IEC 62443-4-2.

Le présent document ne décrit pas les méthodes qui visent à définir des zones et des conduits ni à déterminer des SL pour les zones, les conduits et les composants. Ces méthodes sont définies dans l'IEC 62443-3-2 pour les zones et les conduits, et dans l'IEC 62443-4-2 pour les composants. Le présent document définit les exigences relatives à l'ensemble du SP au sein de l'organisation afin de gérer les risques de manière continue, par la mise en œuvre et le maintien de capacités fondées sur les processus, le personnel et la technologie.

Pour corréler les exigences SP du présent document avec les SL cibles (SL-T) pour les zones, les conduits et les composants, le propriétaire d'actif peut se servir des références croisées à l'IEC 62443-3-3 et à l'IEC 62443-4-2 qui sont fournies avec l'exigence SP afin de comprendre les exigences/améliorations d'exigences associées au SL-T à partir desdits documents.

Par exemple, le présent document peut indiquer qu'il convient qu'un SP contienne un processus qui permet d'assurer une authentification correcte dans l'ensemble de l'organisation. Cependant, pour assurer la confiance dans la mise en œuvre des capacités d'authentification d'utilisateur, il convient que le propriétaire d'actif demande à ses fournisseurs de produit de démontrer que le produit concerné a été conçu à l'aide de processus conformes à l'IEC 62443-4-1, et que les capacités du produit sont conformes aux exigences applicables de l'IEC 62443-4-2. De la même manière, pour assurer la confiance dans l'installation, la configuration et la maintenance des capacités d'authentification d'utilisateur, le propriétaire d'actif peut demander à ses fournisseurs de service de recourir, pour ces capacités, aux processus conformes à l'exigence SP.03.07 RE(1) à partir de la référence croisée à l'IEC 62443-2-4.

4.4 Définition des exigences

4.4.1 Organisation des exigences

Le paragraphe 5.3 et les Articles 6 à 13 définissent la méthode de sélection et les exigences individuelles pour les SP des propriétaires d'actif. Ces exigences ont été spécifiées de manière à être indépendantes d'une mise en œuvre, ce qui permet au propriétaire d'actif de choisir la mise en œuvre la mieux adaptée à son IACS.

Les exigences sont organisées en SPE qui représentent les activités de haut niveau du SP, telles que les mesures de sécurité organisationnelles, la gestion de la configuration, la sécurité du réseau et des communications et la sécurité des composants. Les SPE sont composés d'exigences pour une combinaison des contrôles de sécurité organisationnels et techniques qui peuvent servir à mettre en œuvre une stratégie de défense en profondeur pour l'IACS.

4.4.2 Références croisées des exigences

Pour faciliter l'utilisation du présent document par le propriétaire d'actif, les exigences ont fait l'objet de références croisées avec d'autres parties de la série IEC 62443 et d'autres spécifications de sécurité qui contiennent des exigences relatives aux systèmes et aux composants. Ces références croisées visent à assister l'éventail des activités afférentes aux documents de la série, comme l'intégration du SP du propriétaire d'actif avec son SMSI et les processus de sa chaîne logistique en ce qui concerne la sécurité.

Ces références croisées soutiennent les efforts du propriétaire d'actif à mettre en œuvre les exigences du présent document de manière cohérente avec les autres parties de la série IEC 62443 et avec les autres spécifications citées en référence. Les entrées en blanc dans ces références croisées signifient qu'il n'existe pas d'exigence correspondante dans le document cité en référence croisée. Ces références croisées sont consignées à l'Annexe A.

4.4.3 Conventions relatives aux exigences

Certaines définitions des exigences contiennent l'expression: "communément admis(e)". Cette expression est utilisée lorsque la mise en œuvre de la capacité exigée dépend de l'état actuel de la technique et de l'état de la technique au moment auquel l'évaluation de conformité est utilisée pour déterminer si l'exigence a été satisfaite ou non. Par exemple, la norme de chiffrement de données (DES) ne comportait aucune vulnérabilité connue au moment auquel elle a été élaborée. Depuis lors, des vulnérabilités ont été découvertes et l'usage de cette norme dans les IACS n'est plus approprié. Le paragraphe "Justification et recommandations supplémentaires" de chaque exigence donne des explications supplémentaires sur l'utilisation de cette expression.

5 Conformité et évaluation

5.1 Vue d'ensemble

Les définitions formelles des termes tels que "conformité" et "évaluation" proviennent d'autres sources, telles que l'ISO/IEC 17000 [12]. La série IEC 62443 fournit des recommandations en matière de conformité et d'évaluation pour différents rôles (voir le 4.1.1). Ces recommandations ont pour but d'aider les différents rôles à comprendre le processus de conformité et d'évaluation et ne visent pas à remplacer les définitions fournies dans l'ISO/IEC 17000.

La conformité à la série IEC 62443 signifie que le rôle concerné a évalué et, le cas échéant, a appliqué et documenté toutes les méthodes identifiées dans chaque exigence de la partie applicable de la série, ce qui permet d'atténuer les risques de sécurité et d'identifier la conformité de tous les processus identifiés en apportant les preuves nécessaires.

L'évaluation signifie que le rôle concerné a effectué un mesurage spécifique de la conformité aux exigences par le biais d'un type donné de processus de vérification ou d'un processus de validation spécifique. Ces processus validés peuvent être appliqués par le biais d'un processus d'organisation interne ou par l'utilisation d'un processus identifié par une tierce partie conforme à la série IEC 62443, et sont également vérifiés en apportant les preuves nécessaires.

Les évaluations de conformité peuvent être des auto-évaluations, effectuées par le propriétaire d'actif, le fournisseur de service ou le fournisseur de produit à l'aide de processus internes. Elles peuvent également être effectuées par une tierce partie indépendante qualifiée. Lorsque des évaluations effectuées par une tierce partie indépendante sont utilisées, il est important de noter que les processus d'accréditation de la tierce partie sont très variés et ne relèvent pas du domaine d'application du présent document.

Les processus d'évaluation proprement dits ne relèvent pas non plus du domaine d'application du présent document.

Les propriétaires d'actif peuvent faire évaluer la conformité de leurs systèmes de commande "tels qu'ils sont déployés", c'est-à-dire leur IACS ou leurs Solutions d'Automatisation, à l'IEC 62443-3-3, et leurs services d'intégration et de maintenance "tels que fournis" à l'IEC 62443-2-4. Ces évaluations vérifient la conformité au moment du déploiement du système de commande ou de la fourniture des services. Ces évaluations sont complétées par des évaluations qui combinent les niveaux de sécurité (SL) et les niveaux de maturité (ML) pour établir la protection SP composite fournie à l'IACS.

Les propriétaires d'actif peuvent évaluer la conformité de leurs IACS et de leurs Solutions d'Automatisation au présent document, afin de vérifier qu'ils ont mis en place un SP pour maintenir un niveau de sécurité pour les IACS qui comprend tous les composants techniques et les processus organisationnels. Il est également souhaitable que l'IACS ou la Solution d'Automatisation utilise dans sa conception des produits certifiés en matière de sécurité qui sont correctement déployés et entretenus par des fournisseurs de service certifiés.

Les fournisseurs de produit fournissant des produits à un propriétaire d'actif peuvent faire évaluer la conformité de leurs produits et de leurs processus d'élaboration à l'IEC 624433-3, l'IEC 62443-4-1 et l'IEC 62443-4-2.

Les fournisseurs de service fournissant des services à un propriétaire d'actif peuvent faire évaluer la conformité de leurs services d'intégration et de maintenance à l'IEC 62443-2-4.

5.2 Preuve de conformité

La preuve et les méthodes de conformité peuvent être fournies sous de nombreuses formes, comme le présente le Tableau 2. La plupart des exigences identifient les preuves en précisant les méthodes spécifiques qui comprennent, entre autres:

- la vérification de l'utilisation;
- la capacité et la configuration de la technologie;
- leurs processus de prise en charge; et
- la validation par essai des capacités.

Tableau 2 – Types classiques de preuves de conformité

Type de preuve	Description
Enregistrements de configuration	Enregistrements indiquant les paramètres de configuration, les inventaires de composants, les enregistrements de correctifs, etc.
Documents juridiques	Contrats et documents connexes, y compris les accords de sous-traitance, les états signés des employés, les vérifications d'antécédents, les autorisations du propriétaire d'actif, etc.
Organigrammes, descriptions de poste et registres du personnel	Documentation liée au poste décrivant les rôles du client, y compris les besoins en personnel (par exemple, expertise/expérience), les responsabilités inhérentes au poste et les relations organisationnelles. En outre, les enregistrements indiquant celui qui a été affecté à /déchargé de ces postes (par exemple, pour les activités de la Solution d'Automatisation).
Documentation produit	Documents internes et externes décrivant le produit, tels que documents de conception, fiches techniques, articles fondés sur le savoir et outils d'analyse du réseau.
Captures d'écran	Captures d'écran d'interfaces utilisateur
Évaluations de sécurité	Rapports qui documentent les problèmes liés à la sécurité, tels que des risques, des incidents de sécurité et des vulnérabilités.
Documentation des essais de sécurité	Documents internes et externes décrivant les essais/résultats d'essais de sécurité utilisés pour vérifier les aspects de sécurité du produit ou de son installation.

Type de preuve	Description
Politiques et procédures de service	Documentation interne du client décrivant les politiques et procédures utilisées par le personnel du client pour installer, configurer, renforcer et maintenir la Solution d'Automatisation.
Documentation/listes de contrôle des activités liées à la sécurité	Documentation (listes de contrôle, par exemple) qui enregistre les résultats des activités liées à la sécurité, tels que les appréciations du risque, les modèles de menace, les revues, les dessins d'architecture, les résultats d'essai, les feuilles de calcul, etc.
Rapports automatiques	Rapports générés par l'IACS.
Matériels de formation / descriptions de cours	Documents décrivant la manière dont la formation est conduite et documents présentant le contenu du cours, tels qu'un syllabus ou un aperçu de cours.
Dossiers de formation	Documents indiquant la réalisation terminée d'une formation. Ces documents indiquent généralement les personnes formées, la période de formation et le nom des cours. Ils peuvent prendre la forme de listes de cours, de diplômes/certificats à l'issue des cours, de registres de ressources humaines, etc.
Documentation utilisateur	Manuels d'utilisation, modes d'emploi, etc., décrivant à l'utilisateur comment configurer, utiliser, maintenir ou autrement interagir avec l'IACS, ses produits et ses services.
Résultats des essais	Tous les essais, effectués par une personne qualifiée qui a reçu la formation appropriée, sur une configuration documentée de composants, d'IACS et de Solution d'Automatisation, qui vérifient la conformité à des exigences spécifiquement identifiées.

5.3 Évaluation des exigences et profils

5.3.1 Vue d'ensemble

Pour préparer une évaluation de conformité, il est nécessaire que les propriétaires d'actif évaluent chaque exigence d'une partie applicable de la série selon les recommandations qu'elle fournit pour atténuer le risque visé par l'exigence.

Dans le cas où un rôle détermine, par le biais d'une évaluation, qu'une exigence peut ne pas s'appliquer, il incombe au propriétaire d'actif de justifier la raison pour laquelle ladite exigence n'est pas applicable et d'apporter les preuves qui étayent la raison, y compris la façon dont le risque de sécurité a été atténué par le biais d'autres mesures de sécurité.

5.3.2 Évaluation du risque par rapport aux exigences

La détermination des risques de cybersécurité à atténuer (voir les 4.1.2.1 et 6.3.1, ORG 2.1: Atténuation des risques de sécurité) est généralement réalisée dans le cadre du processus de gestion des risques du propriétaire d'actif, conformément à l'IEC 62443-3-2. Il convient que ce processus intègre les activités de "réponse aux risques" décrites dans l'IEC TS 62443-1-1 et dans l'IEC 62443-3-2, qui sont chargées de l'identification et de l'élimination des risques. Terminer le processus de gestion des risques de l'IEC 62443-3-2 est déterminant pour la sécurité de l'IACS, même en l'absence d'une évaluation de conformité.

Des exigences sont alors appliquées à partir de l'atténuation des risques et s'appliquent à toutes les situations pour lesquelles il est nécessaire d'atténuer les risques identifiés à un niveau tolérable. À l'inverse, des exigences peuvent ne pas s'appliquer lorsqu'il est démontrable que les risques peuvent avoir un niveau tolérable.

Chaque exigence est choisie selon l'atténuation des risques et est interprétée dans le cadre d'un risque tolérable. En d'autres termes, la satisfaction à cette exigence par le propriétaire d'actif implique qu'il a atténué ou accepté les risques associés à l'exigence à l'aide de preuves.

Lorsque le propriétaire d'actif n'est pas prêt à accepter ces risques, l'exigence n'est pas satisfaite.

5.3.3 Profils

Il peut être nécessaire pour certaines industries et certains marchés verticaux d'aligner les exigences du présent document et d'autres documents de l'IEC 62443 sur des concepts et une terminologie spécifiques à l'industrie ou au marché vertical. Afin d'assouplir davantage l'application de la série de normes, l'IEC TS 62443-1-5[13] décrit une méthode qui permet à une ou plusieurs organisations de créer un profil commun à l'IEC 62443 (toutes les parties). Un profil permet à une partie intéressée (organisation, groupe, secteur, organisme d'évaluation de conformité, etc.) de choisir un sous-ensemble d'exigences à partir d'une ou plusieurs normes de la série IEC 62443, de fournir un mapping contextuel pour ces exigences (par exemple, avec une industrie/un marché vertical) et de spécifier un niveau minimal de sécurité ou de maturité pour les exigences choisies.

Les profils publiés peuvent être utilisés comme base commune d'évaluation par rapport à un sous-ensemble ou à un mapping spécifique à l'industrie ou au marché vertical des exigences de la série IEC 62443. Ils assistent les parties intéressées lors des activités d'évaluation de conformité, afin d'assurer la comparabilité des exigences évaluées de l'IEC 62443.

5.3.4 Évaluation de conformité pour le rôle de propriétaire d'actif

Au cours de la préparation d'une évaluation de conformité, les propriétaires d'actif peuvent choisir les exigences qui doivent être évaluées, en fonction des éléments suivants:

a) un profil de sécurité pour lequel le propriétaire d'actif revendique la conformité; ou

b) le résultat d'une appréciation du risque de cybersécurité propre à l'IACS et la détermination des exigences applicables nécessaires pour atténuer les risques à un niveau tolérable.

Une exigence peut ne pas être applicable parce que, par exemple, l'IACS ne contient pas de composants/technologies tels que les systèmes sans fil et de sécurité visés par l'exigence.

La gestion des risques est déterminante pour la sécurité de l'IACS, même en l'absence d'une évaluation de conformité.

6 SPE 1 – Mesures de sécurité organisationnelles

6.1 Objectif

Les exigences de ce SPE sont définies pour garantir que l'organisation est prête à s'occuper de manière adéquate de la sécurité de l'IACS. Ce SPE met l'accent sur les politiques et procédures organisationnelles qui permettent d'appliquer les pratiques de sécurité et d'assurer que le personnel est sensibilisé aux questions de sécurité et est formé pour assumer ses responsabilités de sécurité.

6.2 ORG 1 – Organisation et politiques relatives à la sécurité

6.2.1 ORG 1.1: Système de management de la sécurité de l'information (SMSI)

6.2.1.1 Exigence

Lorsque le propriétaire d'actif dispose d'un SMSI, il doit coordonner le SP IACS avec le SMSI. Lorsque le propriétaire d'actif ne dispose pas de SMSI, il doit intégrer les processus de management appropriés dans le SP IACS.

6.2.1.2 Justification et recommandations supplémentaires

L'organisation propriétaire d'actif utilise souvent un SMSI formel pour protéger son système TI. Il convient de coordonner le SMSI et le SP IACS, lorsqu'ils sont utilisés, en vue d'offrir une stratégie intégrée de défense en profondeur pour l'IACS, évitant ainsi la répétition des efforts et fournissant une interface de sécurité efficace entre les technologies de l'information et l'IACS.

Les exigences et recommandations relatives à un SMSI formel sont disponibles dans les documents ISO/IEC 27001 [8], ISO/IEC 27002 [14], NIST CSF [9], NIST SP 800-53 [15], NIST SP 800-82 [16] ainsi que dans d'autres. Il convient de choisir les exigences et recommandations du SMSI, applicables à un IACS, en fonction de l'atténuation des risques (voir 4.1.2.1), ainsi que de synchroniser, dans toute la mesure du possible, leur mise en œuvre avec le SMSI afin de réduire le plus possible les différences et discordances entre les deux systèmes.

La coordination entre le SP IACS et le SMSI implique une coopération entre les administrateurs de la sécurité, la conception et la gestion d'interfaces réseau IACS partagées (par exemple, pare-feu, zones démilitarisées (DMZ) et accès distant) et la gestion de l'accès utilisateur par ces interfaces. Le système SMSI formel peut être mis en œuvre pour les systèmes TI de l'organisation ou pour l'IACS lui-même.

Il convient d'identifier, d'examiner et de traiter les domaines de conflits potentiels, tels que les politiques et pratiques de gestion des correctifs (voir également l'IEC TR 62443-2-3 [17]) et les mises à jour des logiciels anti-programmes malveillants, afin d'éviter qu'ils s'interfèrent ou qu'ils déclenchent des vulnérabilités entre l'IACS et les systèmes de l'installation.

6.2.2 ORG 1.2: Vérification des antécédents

6.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures liées à la vérification des antécédents de l'ensemble du personnel qui exige d'accès à l'IACS (y compris les employés, les prestataires, les sous-traitants, les consultants, les fournisseurs de produit et les fournisseurs de service) avant de leur en accorder l'accès. Dès lors que le droit applicable le permet et l'autorise, la vérification des antécédents doit comprendre la vérification de l'identité et du casier judiciaire.

6.2.2.2 Justification et recommandations supplémentaires

La vérification des antécédents est utilisée afin d'éviter qu'un personnel dont l'intégrité et la fiabilité peuvent être contestables n'ait accès à l'IACS. Cela concerne, entre autres, les employés, les prestataires, les sous-traitants, les consultants, les fournisseurs de produit et les fournisseurs de service.

Bien que la vérification des antécédents ne puisse pas garantir ces qualités morales, elle peut toutefois identifier le personnel qui a eu des problèmes avec elles. Les vérifications des antécédents incluent, par exemple, la vérification de l'identité et la vérification du casier judiciaire.

Cette exigence reconnaît que la réalisation des vérifications d'antécédents n'est pas toujours possible en raison des lois en vigueur ou du manque de soutien des autorités locales et/ou des organismes de services. Certains pays interdisent les vérifications d'antécédents, pendant que d'autres les permettent. Certains pays parmi ceux qui les permettent ne fournissent aucun soutien pour leur réalisation, ce qui rend impossible ou peu réalisable la vérification des antécédents.

Il convient que le propriétaire d'actif ait une politique indiquant la méthode et la fréquence de réalisation des vérifications d'antécédents lorsque celles-ci sont possibles.

6.2.3 ORG 1.3: Rôles et responsabilités de sécurité

6.2.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la définition et à l'attribution des rôles et des responsabilités en matière de sécurité au personnel qualifié, y compris les employés, les prestataires, les sous-traitants et les consultants.

6.2.3.2 Justification et recommandations supplémentaires

Les rôles de sécurité, tels que les administrateurs de la sécurité, les responsables de la sécurité et les points de contact de sécurité, sont nécessaires pour établir / maintenir la sécurité de l'IACS. De plus, il est nécessaire que le personnel jouant ces rôles soit qualifié pour ses tâches liées à la sécurité afin de garantir qu'elles sont effectuées correctement. Il est nécessaire que le propriétaire d'actif définisse les exigences de qualification, qui consistent généralement en différents niveaux d'éducation, d'expérience et de formation. Certaines formations, telles qu'une formation technique spécifique à l'installation, sont souvent dispensées par le propriétaire d'actif et sont généralement exclues des exigences d'expérience préalable.

Il convient que l'organisation détermine les processus organisationnels nécessaires pour établir/maintenir la sécurité de l'IACS, et identifie le personnel qui sera responsable de leur gestion et de leur mise en œuvre. Il convient également qu'elle détermine le niveau de base d'expertise nécessaire pour effectuer ces tâches et vérifie que le personnel identifié possède cette expertise. L'expertise peut être démontrée par l'expérience et/ou la formation.

6.2.4 ORG 1.4: Formation à des fins de sensibilisation à la sécurité

6.2.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures exigeant que l'ensemble du personnel (y compris les employés, les prestataires, les sous-traitants, les consultants, les fournisseurs de produit et les fournisseurs de service) qui interagit avec l'IACS, reçoive une formation officielle à des fins de sensibilisation à la cybersécurité qui est régulièrement actualisée.

6.2.4.2 Justification et recommandations supplémentaires

Une formation à des fins de sensibilisation à la sécurité est nécessaire pour que le personnel ayant un contact physique avec l'IACS ou ayant accès à ce système comprenne que son comportement peut avoir un impact sur la sécurité de l'IACS. Le maintien de la sensibilisation à la sécurité est essentiel pour établir une culture organisationnelle qui reconnaît que le personnel joue un rôle important dans la sécurité de l'IACS.

Le contact physique avec l'IACS inclut le contact avec des appareils IACS (écrans d'affichage et appareils intégrés, par exemple), des supports de communication, des supports portables, des armoires et tout autre équipement dont la compromission peut avoir un impact sur l'IACS. L'accès au IACS comprend les interfaces utilisateur, les interfaces de communication et les interfaces d'appareils locaux qui permettent d'accéder à l'IACS.

La formation à des fins de sensibilisation à la sécurité permet d'informer le personnel des principes de sécurité de base qu'il doit appliquer dans son comportement au quotidien. Il convient que cette formation soit personnalisée ou liée aux politiques et aux exigences de sécurité spécifiques de l'ACS. Ces politiques et exigences proviennent du présent document et d'autres parties de la série IEC 62443 qui sont applicables à l'IACS. Il convient que le propriétaire d'actif dispose également d'une politique précisant la fréquence à laquelle son programme de formation à des fins de sensibilisation à la sécurité doit être revu afin de le maintenir à jour et pertinent.

Un examen et une mise à jour réguliers du contenu et des plans de formation sont nécessaires pour faire face aux changements intervenant dans le paysage des menaces, le paysage des vulnérabilités et dans la technologie associée à l'IACS.

6.2.5 ORG 1.5: Formation aux responsabilités de sécurité

6.2.5.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures exigeant que l'ensemble du personnel (y compris les employés, les prestataires, les sous-traitants, les consultants, les fournisseurs de produit et les fournisseurs de service) qui interagit avec l'IACS, reçoive une formation officielle en cybersécurité pertinente pour leurs responsabilités en matière de cybersécurité. Cette formation doit être acceptée ou dispensée par le propriétaire d'actif.

6.2.5.2 Justification et recommandations supplémentaires

La formation aux responsabilités de sécurité poursuit deux objectifs:

a) assurer que les membres du personnel responsables de certains aspects de la cybersécurité de l'IACS comprennent quelles sont leurs responsabilités et comment leur performance est mesurée; et

b) assurer qu'ils comprennent les processus et procédures nécessaires pour s'acquitter de ces responsabilités.

NOTE Le personnel ciblé par la formation en sécurité comprend, entre autres, les employés, les prestataires, les sous-traitants, les consultants, les fournisseurs de produit et les fournisseurs de service.

La formation aux responsabilités de sécurité est généralement administrée au personnel sur une base récurrente. Elle comprend les objectifs de sécurité à atteindre ainsi que les critères de rendement au travail associés. Il est important que chaque personne comprenne ce qu'il est attendu d'elle dans l'acquittement de ses responsabilités de sécurité.

Il convient que la formation aux responsabilités de sécurité également décrive comment s'acquitter des responsabilités en matière de sécurité. Ces descriptions peuvent inclure des enseignements en classe/en ligne, des références à des manuels ou à des politiques et procédures écrites. Il convient qu'à l'issue de la formation, tout participant comprenne clairement ses objectifs et comment son rendement sera évalué en fonction de ses responsabilités de sécurité.

6.2.6 ORG 1.6: Sécurité de la chaîne logistique

6.2.6.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui précisent les exigences applicables aux fournisseurs de produit et de service en ce qui concerne les risques de cybersécurité de l'IACS. Les politiques et procédures du propriétaire d'actif doivent prendre en considération les exigences récurrentes imposées aux fournisseurs, lorsque cela est possible.

6.2.6.2 Justification et recommandations supplémentaires

Les IACS sont généralement composés de produits et services intégrés de manière à fonctionner ensemble, et soumis aux essais pour vérifier un tel fonctionnement. Chacun de ces produits et services est fourni au propriétaire d'actif par une organisation (qui peut inclure le propriétaire d'actif), généralement appelée fournisseur. Chaque fournisseur a souvent ses propres fournisseurs et chacun de ces fournisseurs de second niveau peut avoir ses propres fournisseurs. Cette cascade de fournisseurs est appelée la chaîne logistique.

Il convient pour la mise en place d'un processus efficace de la chaîne logistique que le propriétaire d'actif identifie chaque mesure de sécurité technique et procédurale intégrée à l'IACS, puis définisse les exigences de sécurité appropriées pour celles qui sont fournies directement ou indirectement par les fournisseurs de produit ou les fournisseurs de service. L'objectif est que des mesures de sécurité appropriées soient intégrées dans les produits et que les services incluent des processus de sécurité appropriés.

Pour qu'un produit ou service satisfasse aux exigences de sécurité de l'IACS, il incombe au fournisseur de veiller à ce que les composants et les services du produit ou du service soient eux-mêmes soumis à une appréciation du risque dans le contexte de leur utilisation, et il convient que des exigences de sécurité leur soient spécifiées. Il convient que ce processus de détermination du risque et de définition des exigences de sécurité s'effectue de manière récursive tout au long de la chaîne logistique, créant ainsi un processus formel pour traiter le problème de sécurité dans la chaîne logistique.

6.3 ORG 2 – Évaluations et revues de sécurité

6.3.1 ORG 2.1: Atténuation des risques de sécurité

6.3.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'identification, la documentation et l'atténuation ou la gestion des risques de cybersécurité liés à l'IACS, y compris la détermination d'un niveau de risque tolérable et la réponse aux risques dépassant ce niveau de risque tolérable.

6.3.1.2 Justification et recommandations supplémentaires

Les risques de sécurité représentent le potentiel de perte découlant d'une faille de sécurité. Le potentiel de perte s'accroît à mesure que le risque augmente. La gestion des risques implique de comprendre l'environnement opérationnel de l'IACS, d'identifier, d'apprécier et de quantifier les risques dans cet environnement, de déterminer ceux qui ne peuvent pas être tolérés par l'organisation et de les atténuer à un niveau de risque tolérable. Les risques qui ont été atténués à un niveau tolérable indiquent que l'organisation est disposée à "vivre avec" ou est prête à gérer le risque atténué. Voir l'IEC 62443-3-2 pour de plus amples informations sur l'appréciation du risque et la tolérance au risque. Voir l'IEC 62443-3-3 pour de plus amples informations sur l'application de mesures de sécurité techniques qui permettent d'atténuer les risques en dehors du niveau de risque tolérable.

L'atténuation des risques implique l'élaboration de scénarios d'attaque, l'évaluation et la hiérarchisation des conséquences potentielles associées, ainsi que la mise en œuvre de mesures de sécurité en réponse à des risques jugés intolérables. Les mesures de sécurité comprennent généralement une combinaison de mécanismes architecturaux et techniques, de moyens de résolution des vulnérabilités et de mesures de sécurité procédurales. L'atténuation des risques inclut également des activités qui visent à garantir le maintien des risques à un niveau tolérable, telles que des réévaluations périodiques ou induites par des événements (modifications du paysage des menaces et découvertes de nouvelles vulnérabilités, par exemple), des audits internes ou externes vérifiant l'existence et la mise en œuvre appropriée de mesures de sécurité techniques et procédurales, ainsi que des certifications de conformité aux normes de cybersécurité applicables.

Les exigences du présent document décrivent des capacités qui, lorsqu'elles sont correctement mises en œuvre, constituent des mesures de sécurité pour l'IACS. Il convient que le propriétaire d'actif sélectionne dans le présent document les exigences applicables à l'IACS pour les mettre en œuvre en conséquence. Il convient que le propriétaire d'actif indique pour les exigences non sélectionnées, pourquoi elles ne sont pas applicables ou n'ont pas été sélectionnées. Par exemple, elles ne traitent pas un risque de sécurité ou le risque qu'elles traitent est tolérable sans atténuation. Lors de la documentation des risques, des capacités souhaitées, des exigences (toutes deux choisies ou non) et des mesures de sécurité, il est préférable de les renseigner dans un document parfois appelé "système de protection de la sécurité" (SPS) ou "concept d'opérations" (CONOPS). Il convient que le SPS comprenne des mesures de sécurité techniques et procédurales et qu'il indique l'intervention de chaque rôle principal dans l'IACS.

Le développement de scénarios d'attaque implique généralement l'identification de menaces et de vulnérabilités connues qui sont applicables au système. Les vulnérabilités connues sont celles qui ont été découvertes et, dans de nombreux cas, communiquées dans le secteur. Les vulnérabilités connues sont souvent liées au système d'exploitation (OS), aux logiciels libres et aux logiciels des systèmes de commande; cependant, elles peuvent être associées à un quelconque élément de l'IACS. Pour de plus amples informations sur la résolution des vulnérabilités nouvellement découvertes, voir le 12.2.9, EVENT 1.9: Gestion des vulnérabilités.

6.3.2 ORG 2.2: Processus de découverte des anomalies de sécurité

6.3.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la détection et au traitement périodiques, par le biais de processus manuels ou automatisés:

a) des composants/logiciels non documentés et non autorisés qui sont connectés à l'IACS ou qui communiquent dans ce système;

b) du trafic réseau non documenté et/ou non autorisé;

c) des vulnérabilités nouvelles et/ou connues mais non documentées dans l'IACS; et

d) d'autres anomalies de sécurité ainsi que d'autres non-conformités.

6.3.2.2 Justification et recommandations supplémentaires

Les anomalies de sécurité, les non-conformités et les composants, logiciels et trafic réseau non documentés/non autorisés représentent des menaces potentielles pour l'IACS pendant que les vulnérabilités nouvelles et/ou connues mais non documentées constituent des points d'entrée potentiels pour les attaquants.

L'identification et l'évaluation de leur impact potentiel sur l'IACS constituent un élément essentiel de la gestion des risques. L'utilisation régulière de processus manuels ou d'outils automatisés limite l'exposition à ces menaces et l'exploitation des vulnérabilités, ce qui permet de les détecter puis de les traiter.

Il convient, par exemple, d'explorer ou d'examiner régulièrement le réseau pour détecter les composants non autorisés et les services accessibles par le réseau. Il convient d'utiliser ensuite d'autres processus/outils pour identifier les logiciels associés à ces ports du protocole de contrôle d'émission (TCP)/de protocole Internet (IP).

Il convient de veiller à ce que les outils automatisés utilisés n'entravent ni ne compromettent le fonctionnement, les performances et la disponibilité de l'IACS.

6.3.3 ORG 2.3: Développement et prise en charge sécurisés

6.3.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation d'un processus de cycle de vie de développement sécurisé pour le développement et la prise en charge des systèmes et des composants utilisés dans l'IACS.

6.3.3.2 Justification et recommandations supplémentaires

Le développement sécurisé et les essais des systèmes et des composants avant leur intégration dans l'IACS assurent qu'ils protègent l'intégrité et la disponibilité de l'IACS, ainsi que la confidentialité de ses données. Les processus de prise charge sécurisés garantissent le maintien de la sécurité des systèmes et des composants tout au long de leur cycle de vie. Voir l'IEC 62443-4-1 pour les exigences de développement et de prise en charge sécurisés des produits.

Exiger l'utilisation de processus de développement et de prise en charge sécurisés pour les systèmes et les composants d'un IACS garantit la mise en œuvre et l'essai de la sécurité des systèmes et des composants avant leur intégration dans l'IACS ainsi que sa prise en charge lorsque l'IACS est opérationnel et sa gestion pendant toutes les phases du cycle de vie, y compris la mise hors service en fin de vie et/ou de l'utilisation opérationnelle.

6.3.4 ORG 2.4: Revues du SP

6.3.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'examen périodique du SP pour:

a) vérifier la bonne application;

b) valider la satisfaction des mesures de sécurité techniques et procédurales aux exigences de sécurité du système;

c) tenir compte des changements intervenus dans l'organisation et ses processus, des changements techniques apportés à la Solution d'Automatisation et de l'évolution de l'environnement des menaces; et

d) apporter des améliorations, le cas échéant.

6.3.4.2 Justification et recommandations supplémentaires

Les évaluations régulières permettent de vérifier la conformité au SP, de valider la satisfaction du SP aux exigences de sécurité souhaitées et d'assurer que le SP couvre non seulement les modifications apportées à l'organisation, à ses politiques, à la Solution d'Automatisation, mais aussi les menaces qui pèsent sur l'IACS. Ces évaluations servent généralement à mettre au point le SP en fonction des exigences qu'il satisfait et du niveau de maturité (ML) auquel elles sont satisfaites.

Il n'est pas rare qu'un propriétaire d'actif élabore un plan à long terme, appelé feuille de route, pour la mise en œuvre des exigences sur une période donnée. Des évaluations régulières peuvent ensuite être utilisées pour assurer le suivi de:

- de la feuille de route et l'ajuster au besoin; et
- ses progrès.

6.4 ORG 3 – Sécurité de l'accès physique

6.4.1 ORG 3.1: Contrôle d'accès physique

6.4.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'accès physique à l'IACS, y compris l'accès aux installations, aux équipements et au câblage, de façon que l'accès physique soit contrôlé pour satisfaire aux objectifs en matière de risque.

6.4.1.2 Justification et recommandations supplémentaires

Les contrôles d'accès physique protègent l'IACS de la proximité physique indésirable du personnel et des équipements. La proximité physique peut occasionner la connexion d'un équipement filaire ou sans fil à l'IACS et l'utilisation de ressources IACS telles que les stations de travail ou les dispositifs de surveillance (les caméras, par exemple). En règle générale, les organisations restreignent l'accès physique aux systèmes, structures et composants associés à l'IACS, et permettent l'accès uniquement au personnel autorisé, y compris les employés, les prestataires, les consultants, les fournisseurs de produit et les fournisseurs de service.

Différents mécanismes (clôtures, protections, badges, portes verrouillées, caméras et conduits de câblage, par exemple) peuvent être utilisés pour assurer les contrôles d'accès physiques.

7 SPE 2 – Gestion de la configuration

7.1 Objectif

Les exigences de ce SPE sont définies pour garantir que le propriétaire d'actif documente l'architecture de l'IACS, tient un inventaire de ses composants matériels et logiciels et contrôle leurs modifications.

7.2 CM 1 – Gestion d'inventaire des composants matériels/logiciels de l'IACS et des communications réseau

7.2.1 CM 1.1: Base de référence de l'inventaire des actifs

7.2.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures pour documenter, vérifier et tenir à jour, tout au long du cycle de vie de l'IACS, la base de référence d'inventaire de tous les appareils, composants matériels, composants logiciels, protocoles de communication et ports de communication ouverts utilisés dans l'IACS, y compris, entre autres, les éléments suivants:

a) les responsabilités organisationnelles;

b) le fabricant;

c) le modèle;

d) les numéros de version;

e) les numéros de série;

f) les interfaces de réseau;

g) les adresses de communication;

h) les niveaux de révision/correctif; et

i) l'historique.

7.2.1.2 Justification et recommandations supplémentaires

La possession et la tenue à jour d'une base de référence d'inventaire vérifiée sont nécessaires pour valider que tous les appareils, composants matériels, composants logiciels et protocoles/ports/points d'extrémité de communication sont connus du propriétaire d'actif, et par conséquent autorisés et configurés pour satisfaire aux exigences de sécurité. Alimenter la base de référence d'inventaire de l'IACS confirme que la mise en œuvre réelle du système correspond à la conception approuvée. Il convient que la base de référence d'inventaire reflète le système mis en œuvre pendant toutes les phases du cycle de vie de l'IACS, y compris la conception, la spécification, la mise en œuvre, la vérification et la validation, l'exploitation, la maintenance et la mise hors service.

Afin d'identifier et de gérer les risques liés à la cybersécurité de la chaîne d'approvisionnement, il convient que la base de référence d'inventaire tienne compte des actifs tiers qui font partie de l'IACS.

Détenir et alimenter une base de référence d'inventaire permet également au propriétaire d'actif d'examiner les propriétés des composants et des voies de communication. Cela permet de gérer les modifications apportées aux composants et aux voies de communication, y compris les ajouts, les suppressions et les mises à jour.

Les bases de référence de la configuration sont en principe tenues dans une base de données qui contient les propriétés des composants et des protocoles. Il convient que ces propriétés incluent des informations qui identifient et décrivent le composant ou le protocole, ainsi que son utilisation, son état actuel et son historique.

7.2.2 CM 1.2: Schémas/documents d'infrastructure

7.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de vérifier et d'actualiser les schémas/documents de la base de référence présentant la connectivité physique et logique de tous les appareils et composants logiciels IACS.

7.2.2.2 Justification et recommandations supplémentaires

La possession et la tenue à jour des dessins et des descriptions d'architecture vérifiés permettent de réaliser des évaluations de sécurité, y compris l'identification des limites de confiance. Il est nécessaire de vérifier que les dessins correspondent à la mise en œuvre afin de vérifier que des appareils non autorisés ne sont pas connectés au système.

Bases de référence de la configuration décrites en 7.2.1, CM 1.1: Il convient de compléter la base de référence de l'inventaire des actifs par des dessins et des descriptions d'architecture. Il convient que les relations architecturales incluent la connectivité réseau, les protocoles/ports de communication et les flux de données/commande entre les composants.

Il convient de classer et de protéger les schémas et la documentation de l'infrastructure conformément à 10.2.1, DATA 1.1: Classification des données et 10.2.2, DATA 1.2: Confidentialité des données.

Les documents souvent utilisés comprennent, par exemple, les dessins au trait, les dessins fonctionnels, les élévations et aménagements de bâtis, les aménagements de salles, les dessins de périmètre de sécurité (électroniques et physiques) et les informations relatives aux protocoles et points d'extrémité de voie de communication.

7.2.3 CM 1.3: Paramètres de configuration

7.2.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de documenter les paramètres de configuration de tous les appareils et applications logicielles de l'IACS et de vérifier leur conformité opérationnelle à la configuration documentée.

7.2.3.2 Justification et recommandations supplémentaires

La configuration des éléments de l'IACS change souvent au cours du cycle de vie du système afin de satisfaire aux objectifs de fonctionnement à différents stades, notamment à l'installation, au déploiement, à la maintenance, à la réparation et lors des mises à niveau. Il est essentiel pour la sécurité et le fonctionnement du système de documenter les paramètres de configuration approuvés et de pouvoir vérifier qu'ils ont été appliqués ou écrits correctement en fonction des composants.

Il est important de posséder les registres exacts des configurations de l'IACS pour veiller à ce qu'un système fonctionne comme prévu et qu'il soit identifié et documenté de manière suffisamment détaillée pour assurer son cycle de vie prévu.

7.2.4 CM 1.4: Contrôle des modifications

7.2.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent d'autoriser, de valider et d'approuver les modifications apportées à la base de référence de la configuration actuelle et aux schémas/documentation de l'infrastructure, y compris les niveaux de révision et de correctifs.

7.2.4.2 Justification et recommandations supplémentaires

La validation du système mis en œuvre par rapport à la base de référence de la configuration et le contrôle des modifications sont les principaux mécanismes de protection contre l'ajout ou la suppression non autorisé(e) de matériels, de logiciels, et de communications vers l'IACS, mais aussi contre les substitutions, les mises à jour de logiciels et l'ajout de voies de communication.

La combinaison de ces mécanismes avec les 7.2.1 CM 1.1: Base de référence de l'inventaire des actifs, 7.2.2 CM 1.2: Schémas/documents d'infrastructure et 7.2.3 CM 1.3: Paramètres de configuration, permet aux propriétaires d'actifs de soutenir les analyses judiciaires en examinant les composants/communications pour déterminer le moment de leur ajout au système, le moment de leur mise à jour, la personne qui a autorisé la mise à jour et celle qui l'a effectuée.

Il est nécessaire de mettre en place un processus formel de documentation, de soumission et d'approbation des demandes de modification. Il convient que ce processus identifie les rôles et le personnel de l'organisation qui sont responsables de ces activités.

En outre, une bonne pratique à appliquer est la "séparation des tâches", dans laquelle les personnes qui mettent en œuvre la modification, valident la modification et approuvent la modification sont toutes différentes.

8 SPE 3 – Sécurité du réseau et des communications

8.1 Objectif

Les exigences de ce SPE sont définies pour garantir la protection de l'IACS contre les attaques menées à travers le réseau et sur les capacités de communication. Ces attaques peuvent provenir de l'extérieur de l'IACS, des zones non sécurisées au sein de l'IACS et des systèmes ou des appareils non autorisés ou compromis connectés à des réseaux IACS. Voir l'IEC 62443-3-2 pour des recommandations relatives à l'appréciation du risque et au partitionnement des systèmes en zones de sécurité.

8.2 NET 1 – Segmentation du système

8.2.1 NET 1.1: Segmentation du système des zones non-IACS

8.2.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui segmentent les IACS des zones non-IACS et limitent toute interconnexion au niveau minimal nécessaire pour les opérations IACS et dans la limite du risque tolérable.

8.2.1.2 Justification et recommandations supplémentaires

Les réseaux distants/externes fournissent un accès à l'IACS à partir de sources potentiellement inconnues, et constituent donc une menace pour l'IACS. La segmentation de réseau permet de limiter le trafic (flux de données et de contrôle) et la visibilité entre l'IACS et les systèmes externes.

Il convient d'identifier, de gérer, d'autoriser et de documenter le trafic entre l'IACS et les systèmes externes. L'autorisation et la gestion font généralement partie des politiques qui définissent les aspects techniques et procéduraux de l'accès distant sécurisé. De plus, il convient que ce trafic soit caractérisé par ses points d'extrémité (un appareil et une application logicielle, par exemple) et par son protocole de communication.

Les appareils de sécurité du réseau situés aux frontières des segments IACS et non-IACS sont utilisés pour appliquer, autoriser et contrôler les flux de données. Il convient que leur configuration soit appropriée, documentée et à jour. Il convient de les configurer de manière à limiter l'accès aux seuls chemins d'accès nécessaires et pour lesquels le niveau de confiance associé à leur point d'extrémité externe et le risque associé sont tolérables.

Il convient que le propriétaire d'actif détermine les SL-T de l'IACS à partir des risques tolérables. L'IEC 62443-3-2 décrit les étapes du processus de partitionnement de la Solution d'Automatisation en zones et en conduits. Elle décrit également la méthode d'identification du SL-T pour chaque zone et chaque conduit.

Pour de plus amples informations sur la surveillance, voir le 12.2.1, EVENT 1.1: Détection des événements. Pour de plus amples informations sur la segmentation zone à zone dans l'environnement de l'IACS, voir 8.2.6, NET 1.6: Contrôle d'accès au réseau interne.

8.2.2 NET 1.2: Documentation des zones et de l'interconnexion des zones du réseau

8.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de documenter et d'alimenter une base de référence de toutes les zones de l'IACS et des interconnexions et/ou conduits des zones de réseau, des risques de sécurité associés à chacun et leur désignation comme étant fiables ou non fiables.

8.2.2.2 Justification et recommandations supplémentaires

Il convient d'évaluer, dans le cadre du processus de segmentation de réseau ou après la segmentation du réseau, les interconnexions entre les zones et/ou conduits pour déterminer les menaces et les risques associés. Les interconnexions sont généralement mises en œuvre par des appareils de réseau (les routeurs, les pare-feu et les diodes réseau, par exemple) qui permettent au trafic réseau de circuler entre les segments.

L'identification des interconnexions comme étant fiables ou non fiables constitue une tâche essentielle dans la détermination des endroits pour lesquels des contrôles d'accès au réseau sont exigés (voir le 8.2.3, NET 1.3: Segmentation des réseaux des systèmes de sécurité, et le 8.2.4, NET 1.4: Autonomie du réseau). Il convient que les interconnexions non fiables fassent l'objet d'un degré de protection plus élevé.

NOTE Les zones et les conduits (voir l'IEC TS 62443-1-1 et l'IEC 62443-3-2) sont utilisés pour représenter des partitions logiques du système et des canaux de communication entre eux, dont la mise en œuvre peut être prise en charge par la segmentation de réseau et les appareils de réseau.

8.2.3 NET 1.3: Segmentation des réseaux des systèmes de sécurité

8.2.3.1 Exigence

Si l'IACS contient un réseau de système de sécurité, le propriétaire d'actif doit disposer de politiques et de procédures relatives à la protection du système de sécurité contre les perturbations des réseaux autres que ceux du système de sécurité et de leurs appareils.

8.2.3.2 Justification et recommandations supplémentaires

Il convient que les systèmes de sécurité soient, sur le plan opérationnel, indépendants des systèmes commande et des autres réseaux, y compris les réseaux câblés et sans fil. S'il est souvent nécessaire que le système de sécurité soit connecté à l'IACS pour un accès opérateur, ingénieur et administrateur, il convient de ne pas le connecter aux réseaux du système de commande de sorte que le système de commande puisse perturber ou compromettre autrement les fonctions et les communications du système de sécurité. Il convient alors de protéger le système de sécurité des perturbations en provenance d'applications qui lui sont extérieures.

NOTE L'IEC 62443-3-2 recommande de porter une attention particulière aux systèmes de sécurité lors de la création des zones et des conduits.

Des pare-feu, des passerelles et d'autres méthodes de gestion de l'accès au système de sécurité peuvent permettre de réaliser un degré de séparation adéquat entre le système de commande et le système de sécurité. D'autres mécanismes ou stratégies de conception protégeant le système de sécurité des perturbations peuvent également être utilisés.

8.2.4 NET 1.4: Autonomie du réseau

8.2.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la capacité de faire fonctionner l'IACS comme prévu (par exemple, fonctionnement à sécurité intégrée, arrêt sécurisé, fonctionnement en mode limité, fonctionnement normal) lorsqu'il est déconnecté des réseaux externes.

8.2.4.2 Justification et recommandations supplémentaires

Il convient que l'IACS soit en mesure de fonctionner comme prévu en cas de perte de communication avec les systèmes non-IACS. En d'autres termes, il convient qu'une défaillance des communications réseau avec des systèmes externes ne provoque pas la défaillance de l'IACS. L'IACS peut fonctionner en mode dégradé ou de manière moins optimisée, mais il convient qu'il puisse continuer à assumer au moins les fonctions essentielles.

Dans certains cas, tels que l'Internet industriel des objets et/ou l'Industrie 4.0, il existe des connexions externes à l'IACS. Dans de tels cas, il convient de concevoir l'IACS de manière que les fonctions essentielles continuent à fonctionner lorsque les connexions externes sont déconnectées.

8.2.5 NET 1.5: Déconnexion du système des réseaux externes

8.2.5.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la capacité de déconnecter l'IACS des réseaux externes afin de se protéger ou de protéger les réseaux externes des menaces réelles ou suspectées.

8.2.5.2 Justification et recommandations supplémentaires

Il convient que l'IACS puisse être déconnecté, de manière logique ou physique, des réseaux externes en réponse à des conditions de sécurité défavorables (voir le 8.2.4, NET 1.4: Autonomie du réseau) en provenance soit de l'IACS, soit des réseaux externes. Cependant, il convient que le propriétaire d'actif détermine quand une telle déconnexion est conseillée pour assurer que la déconnexion ne crée pas un risque plus élevé que les menaces réelles ou suspectées.

Les techniques de déconnexion peuvent inclure la déconnexion manuelle ou automatique. Les appareils de réseau qui permettent de désactiver ou de bloquer le trafic vers/depuis des réseaux externes peuvent être utilisés à cette fin.

8.2.6 NET 1.6: Contrôle d'accès au réseau interne

8.2.6.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'identification, à la documentation et à l'atténuation ou à la gestion des risques de sécurité associés aux communications entre les segments du réseau interne de l'IACS. Cela peut comprendre la détermination d'un niveau de risque tolérable et la réponse aux risques qui dépassent ce niveau tolérance.

8.2.6.2 Justification et recommandations supplémentaires

Lors de l'analyse des risques entre les zones internes du réseau de l'IACS en 8.2.2, NET 1.2: Documentation des zones et de l'interconnexion des zones du réseau, il est important de prendre en considération le risque de perturbation des fonctions essentielles en déconnectant ou en limitant les communications du réseau entre ces zones. Les communications entre les zones du réseau IACS interne peuvent aussi présenter des risques, tels que ceux associés à des interfaces non fiables qu'il est nécessaire d'atténuer. Lorsqu'elles présentent effectivement ces risques, ils peuvent être atténués en limitant le trafic entre les segments et en n'autorisant que les flux de données et de contrôle qui sont nécessaires et qui ont été autorisés.

Il convient que les communications entre les segments du réseau IACS interne (voir le 8.2.2, NET 1.2: Documentation des zones et de l'interconnexion des zones du réseau) identifiées comme présentant des risques tolérables soient admises et autorisées si elles sont indispensables. Il convient de bloquer et de signaler tout trafic présentant des risques intolérables. Cette tâche peut être accomplie en utilisant des appareils de segmentation de réseau qui inspectent l'ensemble du trafic et bloquent tout trafic non autorisé, également appelé refus par défaut.

8.2.7 NET 1.7: Services accessibles par réseau

8.2.7.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui visent à protéger les services accessibles par le réseau contre les accès non autorisés.

8.2.7.2 Justification et recommandations supplémentaires

Les services d'application accessibles par le réseau fournissent généralement un accès aux ressources IACS. Il convient qu'ils ne soient accessibles uniquement par des appareils, applications et utilisateurs et par des segments de réseau autorisés. Cette recommandation protège l'IACS contre les accès non autorisés et contre les sondes qui tentent de détecter et d'exploiter les vulnérabilités des services d'application, réduisant ainsi la surface d'attaque de l'IACS.

Il convient de configurer les mécanismes de contrôle d'accès au réseau, y compris entre autres les commutateurs, les routeurs avec des listes de contrôle d'accès et les pare-feu, pour permettre l'accès aux services d'application uniquement à partir d'adresses, de ports et de protocoles réseau client autorisés. Il convient également de configurer les services d'application pour permettre uniquement aux utilisateurs autorisés d'établir des sessions avec eux, ce qui offre une couche de protection supplémentaire.

8.2.8 NET 1.8: Messagerie utilisateur

8.2.8.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui visent à limiter la capacité des messages d'utilisateur à utilisateur transmis sur des réseaux IACS à contenir des charges utiles, telles que des pièces jointes, des liens de réseau ou des scripts, pouvant favoriser des attaques contre l'IACS.

8.2.8.2 Justification et recommandations supplémentaires

Les pièces jointes, les liens de réseau vers des applications distantes et les scripts peuvent introduire des programmes malveillants dans l'IACS.

Il convient de ne pas utiliser dans l'IACS, la messagerie électronique, la messagerie instantanée et d'autres mécanismes qui peuvent permettre de transférer des fichiers ou établir des liens vers des destinations inconnues.

8.2.9 NET 1.9: Distribution du temps réseau

8.2.9.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la distribution et à la synchronisation sécurisées du temps dans l'IACS.

8.2.9.2 Justification et recommandations supplémentaires

L'heure système exacte est utilisée pour horodater les événements lorsqu'ils se produisent. Par conséquent, il est nécessaire de répartir l'heure dans l'ensemble de l'IACS à l'aide d'un protocole assurant la synchronisation entre les appareils et qui, de préférence, offre un certain niveau de protection contre les altérations.

Il est important de vérifier que le protocole de distribution du temps utilisé est communément admis pour les utilisations industrielles et qu'il possède la granularité nécessaire pour l'IACS. Au moment de la publication du présent document, la norme IEEE 1588 [18] offre une granularité plus fine que le protocole NTP (protocole de temps réseau) et est plus rentable que les technologies du système GPS (système mondial de localisation). Des versions sécurisées de certains protocoles de synchronisation temporelle courants peuvent être utilisées pour fournir une authentification et une validation supplémentaires afin d'aider à la protection contre les risques d'altération.

8.3 NET 2 – Accès sans fil sécurisé

8.3.1 NET 2.1: Protocoles sans fil

8.3.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures liées à l'utilisation des communications sans fil dans l'IACS et les protocoles reconnus par l'industrie dont l'utilisation est autorisée, le cas échéant. Tout protocole sans fil doit être documenté et la documentation doit être alimentée pour inclure:

a) une configuration de base courante de chaque protocole;

b) les échanges de données avec d'autres segments de réseau; et

c) les capacités et fonctionnalités de sécurité utilisées par chaque réseau sans fil.

8.3.1.2 Justification et recommandations supplémentaires

Les réseaux sans fil ne sont pas limités par des frontières physiques, ce qui permet aux appareils situés hors du périmètre physique de l'IACS d'y accéder. Il est donc important que le propriétaire d'actif utilise des protocoles sans fil éprouvés. Il est également important que le propriétaire d'actif sache comment ils sont utilisés, les données qui y sont transférées et leurs capacités de sécurité, y compris leurs points forts et leurs limites. Les enquêtes sur les réseaux sans fil et en radiofréquences (RF) et les évaluations de sécurité peuvent permettre de mieux connaître leurs capacités. Le propriétaire d'actif dépourvu de ces connaissances peut ne pas être en mesure de prendre, par rapport à leur utilisation, des décisions ayant trait à la sécurité.

Le propriétaire d'actif doit assurer qu'il a identifié et documenté, dans le cadre de la tenue de la base de référence de l'IACS, tous les réseaux sans fil utilisés par l'IACS et leurs flux de données. Il convient que le propriétaire d'actif connaisse les fonctions de sécurité que ces protocoles assurent et qu'il rende toutes ces informations disponibles pour les évaluations de sécurité sur l'IACS. Dans le cadre d'une étude sur les réseaux sans fil et les radiofréquences, il convient que les propriétaires d'actif envisagent également de rechercher d'éventuels réseaux sans fil inconnus et/ou non autorisés dans leur environnement, car ceux-ci peuvent représenter un vecteur d'attaque potentiel pour leur IACS.

8.3.2 NET 2.2: Segmentation des réseaux sans fil

8.3.2.1 Exigence

Lorsque l'utilisation des communications sans fil est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures qui permettent la segmentation des réseaux sans fil des autres segments du réseau IACS.

8.3.2.2 Justification et recommandations supplémentaires

Les réseaux sans fil ne sont pas limités par des frontières physiques, ce qui permet aux appareils situés hors du périmètre physique de l'IACS d'accéder aux données et de les transférer vers/depuis ces réseaux. Il est donc important que le propriétaire d'actif contrôle/gère tous les accès, y compris les flux de données, à l'intérieur et à partir des réseaux sans fil. Le paragraphe 8.3.1, NET 2.1: Protocoles sans fil, spécifie l'exigence de décrire les caractéristiques de sécurité qui permettent d'accéder à l'IACS depuis les réseaux sans fil.

Il convient de configurer les contrôles d'accès, tels que ceux fournis par les appareils de segmentation de réseau et les passerelles sans fil, de manière à permettre uniquement les communications nécessaires vers/depuis les réseaux sans fil. Il convient d'utiliser ces appareils aux interfaces entre l'IACS et le réseau sans fil.

8.3.3 NET 2.3: Propriétés et adresses de réseau sans fil

8.3.3.1 Exigence

Lorsque l'utilisation des communications sans fil est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à la configuration des réseaux sans fil avec des propriétés et des adresses réseau qui réduisent le plus possible les informations utiles aux attaquants.

8.3.3.2 Justification et recommandations supplémentaires

Les propriétés visibles du réseau (par exemple, les noms réseau et les identificateurs d'ensemble de service (SSID)) peuvent donner aux attaquants des informations qui leur permettent d'affiner leur attaque, lorsque ces propriétés sont trop descriptives. Les adresses réseau peuvent être configurées de manière statique ou peuvent être attribuées automatiquement à l'aide du protocole DHCP (protocole de configuration dynamique des hôtes) ou du protocole BOOTP (protocole d'amorce). Malheureusement, les protocoles DHCP et BOOTP présentent des vulnérabilités connues pouvant être exploitées par des attaquants. Il convient donc que les approches d'attribution d'identificateurs SSID et d'adresses réseau suivent les pratiques de sécurité communément admises dans le secteur.

Les pratiques communément admises pour les noms réseau au moment de la publication du présent document consistent à utiliser des noms descriptifs qui créent moins de confusion chez les administrateurs, mais ne fournissent pas d'indications d'emplacement, de propriété, de fonction ou d'autres informations pouvant être utiles aux attaquants.

8.4 NET 3 – Accès distant sécurisé

8.4.1 NET 3.1: Applications d'accès distant

8.4.1.1 Exigence

Lorsque l'utilisation de l'accès distant est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation des applications d'accès distant communément admises dans l'IACS.

8.4.1.2 Justification et recommandations supplémentaires

Les applications d'accès distant, telles que les applications de bureau à distance, permettent la connexion à distance aux stations de travail et aux appareils. D'autres applications d'accès distant, comme les communications sur plateforme ouverte (OPC) permettent des connexions à distance à l'IACS. De nombreuses applications d'accès distant étaient auparavant développées sans une sécurité adéquate et avaient donc subi des intrusions. Il convient donc de vérifier correctement les applications d'accès distant avant leur utilisation dans l'IACS.

Il convient que les connexions d'accès distant soient examinées afin de veiller à ce que la version et les paramètres de configuration de la ou des applications utilisées ne présentent aucune vulnérabilité connue. Il convient de ne pas utiliser les nouveaux produits d'accès distant jusqu'à ce que des tiers de confiance et de renom aient soigneusement évalué et vérifié par essai leurs faiblesses en matière de sécurité.

8.4.2 NET 3.2: Connexions d'accès distant

8.4.2.1 Exigence

Lorsque l'utilisation de l'accès distant est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'autorisation, l'authentification, le chiffrement, la documentation, la journalisation et la surveillance de toutes les connexions d'accès distant interactives. La documentation pour chaque connexion doit inclure, entre autres:

a) son objectif;

b) l'application d'accès distant à utiliser;

c) les technologies de chiffrement et d'authentification utilisées;

d) la méthode d'établissement de la connexion (par exemple, par Internet, à travers un réseau privé virtuel (VPN), à travers une DMZ) avec les instructions nécessaires;

e) les circonstances qui rendent la connexion nécessaire;

f) la durée à laquelle il est nécessaire de garder la connexion ouverte, y compris les périodes d'inactivité prévues;

g) l'emplacement et l'identité de l'appareil client, de l'application et de l'utilisateur distants; et

h) toute exigence de conformité qu'il est nécessaire de satisfaire avant d'établir la connexion.

8.4.2.2 Justification et recommandations supplémentaires

Les applications d'accès distant interactives, telles que les applications de bureau à distance, permettent la connexion à distance aux stations de travail et aux appareils. D'autres applications d'accès distant (OPC, par exemple) permettent des connexions à distance à l'IACS. Dans les deux cas, les applications d'accès distant offrent la possibilité à un ordinateur distant (une station de travail ou un ordinateur portable, par exemple) potentiellement infecté par un programme malveillant d'infecter ou d'attaquer l'IACS. Par exemple, un ordinateur portable avec des privilèges d'accès distant peut être amené hors site, connecté à Internet, puis infecté. L'utilisateur peut ensuite créer, à partir du même ordinateur portable, une connexion VPN et établir une connexion de bureau à distance à l'IACS, à travers un VPN d'entreprise. S'il est écrit avec suffisamment d'intelligence, le programme malveillant a alors un accès direct à l'IACS.

Il convient que le propriétaire d'actif dispose d'un processus qui permet de documenter et d'autoriser toutes les connexions d'accès distant avant leur utilisation. Cela inclut généralement un processus de demande d'une connexion d'accès distant entre un client et un serveur, un processus de validation et d'approbation de la connexion en fonction de son utilisation prévue, et un processus de préparation de l'utilisation de la connexion comprenant l'élaboration des règles de pare-feu, la configuration des VPN et de la DMZ et l'octroi au client d'un accès utilisateur à l'application serveur.

Il convient de documenter ces processus avec toutes les instructions nécessaires à la préparation et à l'utilisation de la ou des connexion(s) d'accès distant. Il convient que la documentation indique en quoi la connexion est nécessaire, la durée à laquelle il est nécessaire de la garder ouverte, les périodes d'inactivité éventuelles prévues et la condition/circonstance qui rend la connexion nécessaire. Il convient que cette documentation soit adéquate pour évaluer et approuver la demande et, si elle est approuvée, pour authentifier l'appareil client et l'utilisateur.

8.4.3 NET 3.3: Fin de l'accès distant

8.4.3.1 Exigence

Lorsque l'utilisation de l'accès distant est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à la fin de toutes les connexions d'accès distant interactives après une période d'inactivité configurée.

8.4.3.2 Justification et recommandations supplémentaires

Laisser les connexions d'accès distant ouvertes, lorsqu'elles ne sont pas utilisées, crée un risque inutile d'utilisation inappropriée de ces connexions ou un risque inutile de contrôle de celles-ci par les attaquants, augmentant ainsi la surface d'attaque.

Il convient d'approuver les connexions d'accès distant pour utilisation pendant une période spécifique ou pendant leur utilisation active, et de les configurer pour une fin automatique après une période d'inactivité donnée.

9 SPE 4 – Sécurité des composants

9.1 Objectif

Les exigences de ce SPE sont définies pour garantir que l'IACS et ses composants (par exemple, les appareils et les logiciels) sont correctement protégés contre les attaques. Ces attaques peuvent provenir d'interfaces de composant externes et internes. Les interfaces externes comprennent, par exemple, les interfaces réseau, les interfaces USB et les ports de configuration. Les interfaces internes comprennent, par exemple, les interfaces de communication interprocessus et les interfaces de programmation d'application (API).

Le paragraphe 9.4 COMP 3 – Gestion des correctifs, traite de l'application des correctifs de sécurité pour supprimer des composants IACS les vulnérabilités de sécurité connues. Pour plus de précisions sur la gestion des correctifs, voir l'IEC TR 62443-2-3.

9.2 COMP 1 – Appareils et supports

9.2.1 COMP 1.1: Renforcement des composants

9.2.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de renforcer les composants avant leur utilisation dans l'IACS afin de protéger leurs caractéristiques logicielles et matérielles, de maintenir l'état renforcé pendant la durée de vie des composants et de conserver la documentation relative aux éléments, moyens et procédures de renforcement des composants.

9.2.1.2 Justification et recommandations supplémentaires

Le renforcement vise à réduire la surface d'attaque de l'appareil. Le renforcement d'un appareil implique la suppression ou la désactivation de fonctionnalités non nécessaires au fonctionnement dans l'IACS, la protection de ses interfaces contre les accès physiques et logiques non autorisés et la garantie que les processus de maintenance ne compromettent ni ne dégradent l'état renforcé de l'appareil.

Le renforcement est souvent effectué avant ou pendant l'installation d'un appareil dans l'IACS. Les modèles de sécurité, tels que ceux spécifiés par le Centre pour la sécurité Internet (CIS), définissent les paramètres de sécurité pouvant être appliqués pour restreindre l'utilisation de l'appareil et le protéger contre les attaques. En outre, il convient de supprimer ou de désactiver les applications inutiles (les jeux, les protocoles et les certificats numériques, par exemple) livrées avec les systèmes d'exploitation disponibles dans le commerce (COTS) et autres logiciels d'infrastructure, ainsi que les ports de communication inutiles et services d'accès aux communications associés, pour empêcher qu'ils ne soient utilisés intentionnellement ou non pour interférer dans les opérations de l'appareil ou pour infecter l'appareil avec des programmes malveillants.

Les mesures de renforcement sont spécifiques à chaque composant. Les exemples de mesures de renforcement comprennent, entre autres:

- suppression/désactivation des applications et des services logiciels inutiles (par exemple, courrier électronique, applications bureautiques et jeux) et de leurs points d'accès de communication associés (par exemple, ports TCP/protocole UDP);
- habilitation des interfaces pour les supports portables lorsque leur utilisation est autorisée et désactivation des interfaces sans autorisation d'utilisation;
- suppression/désactivation des communications sans fil qui ne sont pas exigées par l'IACS;
- suppression/désactivation des adresses réseau dont l'utilisation n'est pas autorisée;
- protection de l'accès physique et logique aux ports de diagnostic et de configuration contre les accès et utilisations non autorisés;
- configuration des ports inutilisés sur les appareils réseau (par exemple, les commutateurs et les routeurs) afin d'éviter tout accès non autorisé à l'infrastructure de réseau IACS; et
- garantie du maintien de l'état renforcé de l'IACS, par les processus de maintenance, pendant toute sa durée de vie.

Au cours du fonctionnement, il est souvent nécessaire de modifier la configuration des composants en raison des conditions opérationnelles. Par exemple, une organisation tierce peut exiger au propriétaire d'actif d'ouvrir des ports afin d'exécuter des activités de maintenance sur les actifs dans l'IACS. Il est nécessaire de définir des procédures pour garantir que l'état renforcé de l'IACS et de ses composants soit rétabli après les modifications de configuration.

9.2.2 COMP 1.2: Supports portables spécifiques

9.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation ou aux fonctions approuvées ou non des supports portables dans l'IACS.

9.2.2.2 Justification et recommandations supplémentaires

Un support portable est un support amovible qui peut être amené hors site vers d'autres emplacements auxquels il peut être infecté. Utiliser des supports portables (tels des périphériques de stockage USB, par exemple) propres à l'IACS et à une utilisation spécifique dans l'IACS peut réduire le plus possible le risque d'infection par des programmes malveillants.

Il convient de mettre en place des politiques et procédures qui

- Définissent les supports portables qui peuvent être utilisés et les fonctions au sein de l'IACS pour lesquelles ils peuvent être utilisés, et.
- Limitent son utilisation aux fonctions approuvées au sein de l'IACS et uniquement par des appareils approuvés.

En outre, des mesures techniques peuvent être prises pour authentifier les supports portables afin de garantir que leur utilisation a été autorisée dans l'IACS. Par exemple, si l'utilisation d'un support portable est autorisée pour exécuter une fonction essentielle, telle qu'une fonction de sécurité, il est nécessaire que le propriétaire d'actif veille à ce que le support portable utilisé soit uniquement conçu à cette fin et à l'emplacement prévu.

9.3 COMP 2 –Protection contre les programmes malveillants

9.3.1 COMP 2.1: Absence de programme malveillant

9.3.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent que tous les composants et supports portables (si l'utilisation d'un support portable est autorisée dans l'IACS) soient exempts de programmes malveillants connus avant d'être utilisés dans l'IACS.

9.3.1.2 Justification et recommandations supplémentaires

Les appareils et les supports portables peuvent être infectés avant ou pendant leur expédition. Cette possibilité offre une méthode d'attaque ne nécessitant pas une connectivité réseau ni une présence physique de l'attaquant. Veiller à l'absence de programmes malveillants dans les appareils et les supports portables installés dans l'IACS réduit le plus possible ce type d'attaque. Il convient que le propriétaire d'actif obtienne, pour les supports chiffrés, l'assurance du fournisseur que des procédures sont en place pour vérifier que les données contenues sur le support chiffrés sont exemptes de programmes malveillants.

Les mécanismes utilisés pour assurer que les programmes malveillants ne sont pas présents dans les appareils et les supports portables incluent l'analyse et les contrôles d'authenticité, tels que les signatures numériques. Les contrôles d'authenticité peuvent déterminer si les images de logiciels dans l'appareil n'ont pas été modifiées. L'analyse est utilisée pour détecter les programmes malveillants connus et est utile, en particulier lorsque les contrôles d'authenticité ne sont pas pris en charge. En outre, des protections de chemin de distribution, telles que les dispositifs inviolables, peuvent également être utilisées pour satisfaire à cette exigence.

9.3.2 COMP 2.2: Protection contre les programmes malveillants

9.3.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'installation, au fonctionnement et à la maintenance des mécanismes de protection contre les programmes malveillants, lorsque cela est possible.

9.3.2.2 Justification et recommandations supplémentaires

Les mécanismes de protection contre les programmes malveillants connus permettent de détecter ces programmes et d'empêcher leur exécution. Il est nécessaire de les vérifier afin d'éviter l'infection du système par des programmes malveillants. Il est également nécessaire de vérifier par essai la compatibilité de ces mécanismes au composant, ce qui signifie qu'ils ont été soumis à l'essai pour assurer qu'ils n'interfèrent pas avec les fonctions et le fonctionnement du composant.

Les logiciels de protection contre les programmes malveillants ne sont souvent pas disponibles pour tous les composants de l'IACS. Il convient de documenter les composants pour lesquels il n'existe pas de logiciel de protection contre les programmes malveillants et de les protéger à l'aide de mesures de sécurité compensatoires adaptées au niveau de risque déterminé dans l'IACS.

L'antivirus, la liste d'autorisation et la vérification de signature numérique constituent trois méthodes principales de protection d'un composant contre les programmes malveillants. Un antivirus est utilisé pour examiner les fichiers et les données entrant dans l'appareil et les comparer à des configurations binaires connues, appelées signatures de programmes malveillants, mais souvent appelées listes noires. Il est nécessaire de mettre à jour les signatures de programmes malveillants pour couvrir tous les programmes malveillants connus. Tout programme malveillant détecté par un antivirus est normalement mis en quarantaine et l'utilisateur est invité à prendre les mesures appropriées. La liste d'autorisation, en revanche, est configurée pour permettre uniquement l'exécution de logiciels autorisés. Ainsi, l'établissement de listes d'autorisation n'exige pas de mises à jour des signatures de programmes malveillants et offre également une protection contre les programmes malveillants inconnus jusqu'à présent. La vérification de signature numérique peut être considérée comme une forme de liste d'autorisation, car elle authentifie un logiciel en fonction de sa signature numérique (généralement une forme de hachage sécurisé) avant de permettre son exécution.

9.3.3 COMP 2.3: Validation et installation du logiciel de protection contre les programmes malveillants

9.3.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives aux essais de compatibilité, à l'approbation et à l'installation des logiciels de protection contre les programmes malveillants et de tous les fichiers de signatures de programmes malveillants connexes, en temps utile après leur publication.

9.3.3.2 Justification et recommandations supplémentaires

Les mécanismes anti-programmes malveillants sont souvent intégrés aux routines du système d'exploitation (OS) et peuvent donc affecter le fonctionnement du système. De plus, puisque le logiciel de protection contre les programmes malveillants examine les fichiers et les données par rapport à des configurations binaires prédéfinies, il est possible que des logiciels ou des données légitimes de l'appareil possèdent les mêmes configurations binaires. Une telle situation est peu probable, mais elle s'est déjà produite. Il convient donc de vérifier la compatibilité de tous les logiciels antiprogrammes malveillants avec le logiciel de l'appareil afin d'assurer qu'ils n'interfèrent pas avec les fonctions et le fonctionnement de l'appareil.

Il convient de soumettre à l'essai le logiciel antiprogrammes malveillants avant de l'utiliser sur un appareil. Cet essai est généralement effectué par le fournisseur de service ou le fournisseur de produit.

Il est important de procéder à une installation à temps, l'IACS étant vulnérable aux programmes malveillants connus jusqu'à l'installation du logiciel de protection contre les programmes malveillants et de ses fichiers de signature de programmes malveillants. La rapidité de réaction est donc un facteur de réduction des risques à un niveau tolérable.

9.4 COMP 3 – Gestion des correctifs

9.4.1 COMP 3.1: Authenticité/intégrité des correctifs de sécurité

9.4.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la vérification de l'authenticité et de l'intégrité de tous les correctifs avant leur installation.

9.4.1.2 Justification et recommandations supplémentaires

Les correctifs sont généralement distribués par le fournisseur de produit à l'aide de différents mécanismes de distribution, notamment des transferts par réseau, des CD/DVD et des périphériques de stockage USB. Les correctifs sont susceptibles d'être interceptés et infectés par un programme malveillant pendant le transfert. Il est donc nécessaire de vérifier leur intégrité et leur authenticité.

Il convient que les propriétaires d'actifs vérifient que tous les correctifs sont reçus directement du développeur de correctifs, que le chemin de distribution est protégé et que du soutien (par exemple, les signatures numériques) est apporté à la vérification de l'authenticité et de l'intégrité ou que des mesures de sécurité compensatoires sont appliquées lorsqu'il n'est pas possible de procéder à la vérification de l'authenticité et de l'intégrité numérique. En outre, il convient que les propriétaires d'actifs vérifient que les correctifs n'ont pas été infectés sur le site du fournisseur de produit. Il convient également d'utiliser des dispositifs inviolables pour les supports de distribution tels que les CD/DVD/USB. Pour des recommandations supplémentaires, voir l'IEC TR 62443-2-3.

9.4.2 COMP 3.2: Validation et installation des correctifs de sécurité

9.4.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives aux essais de compatibilité, à l'approbation et à l'installation des correctifs de sécurité applicables aux composants en temps utile après leur publication.

9.4.2.2 Justification et recommandations supplémentaires

Des correctifs de sécurité sont souvent fournis pour les OS et les logiciels d'infrastructure développés indépendamment des logiciels IACS. En conséquence, le logiciel IACS peut être affecté par ces correctifs. Il est donc nécessaire de soumettre à l'essai les correctifs de sécurité avec l'IACS avant de les utiliser.

Il convient de soumettre à l'essai les correctifs de sécurité avant de les utiliser sur un appareil. Cet essai est généralement effectué par le fournisseur de service ou le fournisseur de produit.

L'IACS reste vulnérable aux attaques associées jusqu'à l'installation des correctifs, ceux-ci étant destinés à éliminer les vulnérabilités. Une installation opportune est donc importante et constitue un facteur de réduction des risques à un niveau tolérable.

9.4.3 COMP 3.3: État des correctifs de sécurité

9.4.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la documentation et à la maintenance de l'état des correctifs de sécurité de tous les composants.

9.4.3.2 Justification et recommandations supplémentaires

Lors du dépannage ou lors de la réalisation de diagnostics ou d'investigations, il est nécessaire de connaître la configuration du logiciel, y compris l'état des correctifs, d'un appareil. De plus, lors de l'évaluation des vulnérabilités d'un appareil, il est essentiel de connaître les correctifs de sécurité qui ont été appliqués.

Il convient d'alimenter l'état du correctif de sécurité pour indiquer au moins:

- l'identificateur du correctif;
- le logiciel applicable qui fait l'objet du correctif;
- la date de publication du correctif; et
- la date (prévue ou réelle) d'installation du correctif.

Pour des recommandations supplémentaires, voir l'IEC TR 62443-2-3.

9.4.4 COMP 3.4: Maintien de la sécurité par les correctifs de sécurité

9.4.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de vérifier que l'installation du correctif de sécurité n'abaisse pas la sécurité du composant.

9.4.4.2 Justification et recommandations supplémentaires

Dans certains cas, l'installation de correctifs peut introduire des vulnérabilités connues, entraîner la suppression des paramètres de configuration, modifier la manière dont le logiciel traite ces paramètres ou modifier la fonction du logiciel. Lorsque l'installation n'est pas correctement gérée, elle peut également entraîner une perte d'intégrité du contenu de l'appareil, certains éléments de l'appareil ayant été supprimés dans le cadre du processus d'installation. En outre, des correctifs non authentifiés dans le cadre du processus d'installation peuvent être installés, ce qui éventuellement entraîne l'installation de correctifs qui ont fait l'objet d'altération.

Il convient que les procédures de maintenance incluent une vérification indiquant que l'état du contenu et la configuration d'un appareil n'ont pas été dégradés par l'installation des correctifs. Pour des recommandations supplémentaires, voir l'IEC TR 62443-2-3.

9.4.5 COMP 3.5: Atténuation du risque associé aux correctifs de sécurité

9.4.5.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'appréciation du risque encouru lorsque les correctifs applicables de sécurité ne sont pas installés. Si le risque n'est pas tolérable, elles doivent être relatives au traitement du risque et à la documentation de la résolution.

9.4.5.2 Justification et recommandations supplémentaires

Lorsque des correctifs de sécurité ne sont pas installés, du fait par exemple de leur échec aux essais, de la non-approbation de leur installation ou lorsqu'ils n'ont pas été mis à disposition à temps, les vulnérabilités associées demeurent. Il convient d'utiliser, par conséquent, des solutions de rechange ou d'autres mesures de sécurité compensatoires.

Il convient que le propriétaire d'actif assure que tous les correctifs de sécurité applicables à l'appareil, mais non installés, font l'objet d'une appréciation du ou des risques, et que les risques associés sont résolus, s'ils sont inacceptables, par le biais de solutions de rechange ou de mesures de sécurité compensatoires. Il convient de documenter les risques et les résolutions. Pour des recommandations supplémentaires, voir l'IEC TR 62443-2-3.

10 SPE 5 – Protection des données

10.1 Objectif

Les exigences de ce SPE sont définies pour garantir que les données sont protégées contre la divulgation (confidentialité) et l'altération (intégrité).

10.2 DATA 1 – Protection des données

10.2.1 DATA 1.1: Classification des données

10.2.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent d'identifier et de classer toutes les données de l'IACS devant être sauvegardées en fonction de leurs exigences en matière de protection.

10.2.1.2 Justification et recommandations supplémentaires

Pour protéger les données de la divulgation et de l'altération, il est nécessaire de connaître les données qui ont besoin d'être protégées et si elles ont besoin d'être protégées de la divulgation, de l'altération, de la perte, de la perte d'utilisation ou de toute autre compromission. Le niveau de risque de la compromission est également nécessaire pour l'organisation, car il sert à déterminer le degré de protection dont elle a besoin.

Une appréciation du risque sert généralement à identifier les données et le risque/impact associé à leur compromission pour l'organisation, y compris la divulgation, l'altération, la perte ou la perte d'utilisation.

Il convient d'identifier et de classer les exemples de types de données IACS suivants:

a) les informations d'authentification et d'autorisation de l'utilisateur;
b) les informations du journal d'audit et de sécurité, y compris l'historique d'audit;
c) les données d'essai;
d) les données de configuration;
e) les clés cryptographiques;
f) les données de sauvegarde;
g) les transferts d'action de commande, y compris la direction du transfert;
h) les données exclusives et de secrets commerciaux; et
i) toute information personnellement identifiable (IPI) collectée ou traitée dans l'IACS.

10.2.2 DATA 1.2: Confidentialité des données

10.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la confidentialité des données de l'IACS en tenant compte des risques de compromission des données selon leur classification.

10.2.2.2 Justification et recommandations supplémentaires

Il est nécessaire de protéger la confidentialité des données, qu'elles soient inactives ou mobiles. L'absence de protection de la confidentialité des données peut occasionner une compromission de ces données. Les données inactives sont généralement considérées comme des données conservées dans une mémoire volatile (par exemple, une mémoire d'ordinateur) ou dans une mémoire non volatile (par exemple, un disque, un CD/DVD/USB ou une mémoire flash). Les données en transit sont généralement considérées comme des données déplacées entre deux ou plusieurs emplacements, soit électroniquement par un lien de communication, soit physiquement.

Les données peuvent être protégées d'un accès non autorisé au moyen d'un certain nombre de mécanismes. Le mécanisme utilisé, y compris la combinaison appliquée, dépend de la classification des données et de leur valeur pour l'organisation. En règle générale, les contrôles d'accès des utilisateurs constituent le premier niveau de défense pour les données inactives, permettant uniquement aux utilisateurs autorisés à accéder aux données et aux logiciels utilisant les données d'y accéder.

Les approbations relatives au transfert de données peuvent être utilisées pour limiter les données transférées.

Le chiffrement peut permettre de protéger les données de la divulgation. Il peut être utilisé pour les données inactives lorsque les intrus ont d'une façon ou d'une autre défait les contrôles d'accès. Il est souvent utilisé pour les données en transit afin d'empêcher toute personne capable d'intercepter ou de surveiller les transmissions de données de pouvoir récupérer les informations d'origine.

Lorsque ces capacités ne sont pas réalisables ou lorsqu'une protection supplémentaire est souhaitée, des contrôles d'accès limitant l'accès physique et l'accès au réseau pour les ordinateurs et les liaisons de communication permettent d'isoler les données des attaquants.

10.2.3 DATA 1.3: Mode de configuration du système de sécurité

10.2.3.1 Exigence

Lorsque l'utilisation de systèmes de sécurité est autorisée dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à:

a) la mise à jour de la configuration du système de sécurité uniquement lorsque le mode de configuration est activé; et

b) l'activation du mode de configuration uniquement lorsque des modifications de configuration sont nécessaires.

10.2.3.2 Justification et recommandations supplémentaires

À l'instar d'un système de commande, le système de sécurité fonctionne selon les paramètres de configuration qui y sont écrits ou téléchargés. En règle générale, la configuration est statique et ne change que lorsque cela est nécessaire. Pour assurer la protection contre les changements non autorisés de la configuration du système de sécurité, il convient de mettre à jour cette configuration uniquement aux heures approuvées, et de ne permettre les changements de configuration que pour une durée finie. Une telle approche est souvent appelée mode de configuration du système de sécurité. Le mode de configuration peut être activé à l'aide d'actions explicites de l'administrateur du système de sécurité et désactivé pour un fonctionnement normal du système de sécurité à la fin de la mise à jour de la configuration.

Il convient qu'un mode de configuration du système de sécurité soit pris en charge par un logiciel, un matériel ou une interface mécanique disponible uniquement pour les administrateurs du système de sécurité autorisés. Il convient que la valeur par défaut soit toujours "désactivée".

10.2.4 DATA 1.4: Politique de rétention des données

10.2.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la rétention des données tout au long du cycle de vie de l'IACS, y compris l'élimination.

10.2.4.2 Justification et recommandations supplémentaires

La rétention des données consiste à conserver les valeurs de donnée et les événements, tels que les journaux, les historiques et les sauvegardes, pendant une période spécifiée. Cela comprend également l'élimination des données nécessitant une sauvegarde lorsque l'appareil est mis hors service ou retiré autrement de l'IACS. Il convient de mettre en place les politiques de rétention de données (par exemple, la durée de conservation des valeurs) et les capacités associées pour prendre en charge les opérations de sécurité (la reprise et l'analyse judiciaire, par exemple) et les opérations de contrôle telles que l'analyse des tendances. Il convient de spécifier et de documenter ces politiques et capacités en vue de réduire le plus possible les risques pour l'organisation.

Les politiques de rétention des données incluent généralement la durée de conservation des valeurs de donnée et des événements pour les copies d'exécution, les copies accessibles localement (par exemple, les journaux et les historiques) et les copies archivées. Les capacités incluent les capacités de prise en charge des politiques et la rapidité avec laquelle il est possible de récupérer les copies souhaitées.

Il convient d'éliminer de la mémoire des appareils les données confidentielles lorsque l'appareil est mis hors service ou autrement retiré de service. Cette recommandation empêche la divulgation de ces données à ceux qui peuvent ultérieurement avoir accès à l'appareil. Il convient d'éliminer la mémoire d'un appareil avant renvoi d'une carte ou d'un appareil défectueux au fournisseur pour réparation en vertu d'un contrat de service d'assistance. Voir le 10.2.2, DATA 1.2: Confidentialité des données, pour de plus amples informations sur la protection de la confidentialité des données de l'IACS.

Dans certaines situations, il convient de conserver la mémoire en lecture seule pour permettre au fournisseur de produit de résoudre le problème. Pour tenir compte de ces cas, il convient d'inclure la protection des données des propriétaires d'actif dans les accords conclus avec le fournisseur.

Il convient que les appareils utilisés dans l'IACS soient équipés de mécanismes ou de procédures documentées qui permettent d'éliminer de ces appareils les données confidentielles non volatiles. Le support de données non volatile comprend les disques et la mémoire flash.

10.2.5 DATA 1.5: Mécanismes cryptographiques

10.2.5.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation de mécanismes cryptographiques communément acceptés dans l'IACS.

10.2.5.2 Justification et recommandations supplémentaires

Il convient que l'IACS emploie des mécanismes cryptographiques qui sont couramment utilisés par les applications TI et les applications industrielles, et qui sont considérés comme étant exempts de vulnérabilités et de faiblesses connues du public.

10.2.6 DATA 1.6: Gestion des clés

10.2.6.1 Exigence

Lorsqu'il est autorisé de faire usage de mécanismes cryptographiques utilisant des clés dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation, la protection et l'exécution de la durée de vie des clés cryptographiques, suivant les pratiques et recommandations communément admises par les communautés de la sécurité et l'automatisation industrielle.

10.2.6.2 Justification et recommandations supplémentaires

La gestion des clés est un composant important qui permet l'utilisation de mécanismes cryptographiques tels que le chiffrement des données, les signatures numériques et l'authentification. Une mauvaise gestion des clés peut compromettre la sécurité des clés, ce qui peut entraîner une défaillance de la cryptographie.

Il est nécessaire de tenir compte de la gestion de l'expiration des certificats afin d'éviter les risques opérationnels pour l'IACS en cas d'expiration du certificat.

10.2.7 DATA 1.7: Intégrité des données

10.2.7.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la protection de l'intégrité des données contre toute compromission, qu'elles soient inactives ou mobiles (électroniquement ou physiquement), qui tiennent compte des risques applicables.

10.2.7.2 Justification et recommandations supplémentaires

Il est nécessaire de protéger l'intégrité des données qui en ont besoin, qu'elles soient inactives ou mobiles. Lorsque l'intégrité des données n'est pas protégée, une compromission susceptible d'entraver le processus industriel peut survenir.

Les approbations relatives au transfert de données peuvent être utilisées pour limiter les données transférées et la validation de données/paramètres peut servir à déterminer si les données ont été modifiées pendant le transit ou si des valeurs non valides sont transmises.

Les signatures numériques peuvent être utilisées pour protéger les données inactives ou mobiles des altérations. Elles fournissent une somme de contrôle sécurisée qui permet l'authentification et la détection des changements.

Lorsque ces capacités ne sont pas réalisables ou lorsqu'une protection supplémentaire est souhaitée, des contrôles d'accès limitant l'accès physique et l'accès au réseau pour les ordinateurs et les liaisons de communication permettent d'isoler les données des attaquants.

11 SPE 6 – Contrôle d'accès des utilisateurs

11.1 Objectif

Les exigences de ce SPE sont définies pour garantir que les utilisateurs (utilisateurs humains, processus logiciels et appareils) se voient attribuer des comptes qui permettent de contrôler l'accès à l'IACS, à ses ressources et à ses commandes. Le contrôle d'accès implique l'identification, l'authentification et l'autorisation afin d'attribuer et d'appliquer des droits d'accès ainsi que le contrôle des sessions d'utilisateurs. Les utilisateurs humains de l'IACS incluent, entre autres, les ingénieurs, les opérateurs, les administrateurs et le personnel de support.

Les droits d'accès à l'OS et au système de commande accordent aux utilisateurs la permission d'utiliser des ressources IACS et d'émettre des commandes. Les droits typiques incluent, entre autres, la lecture, l'écriture et l'exécution. Les sessions sont des connexions de l'utilisateur au système qui sont établies par suite d'une identification et d'une authentification réussies.

En règle générale, il convient de définir des politiques de gestion des comptes d'utilisateurs pour assurer la cohérence de ceux qui satisfont aux exigences de l'Article 11. Ces politiques sont généralement documentées de manière officielle et fournissent un cadre de création et de maintenance des comptes d'utilisateurs.

11.2 USER 1 – Identification et authentification

11.2.1 USER 1.1: Attribution d'identité utilisateur

11.2.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures pour attribuer aux utilisateurs (utilisateurs humains, processus logiciels et appareils) des identificateurs, des authentifiants et des rôles spécifiques à l'IACS.

11.2.1.2 Justification et recommandations supplémentaires

Les comptes d'utilisateurs sont des représentations numériques des utilisateurs. Les identificateurs relient les utilisateurs aux comptes et aux authentifiants (les mots de passe, par exemple), accordent aux utilisateurs humains, aux processus logiciels et aux appareils la permission d'utiliser leur compte associé. Les utilisateurs humains sont authentifiés lors de la connexion et bénéficient du droit d'exécuter des programmes sous le compte utilisé pour la connexion. Les processus logiciels sont authentifiés lorsqu'ils sont démarrés automatiquement par l'OS et exécutés sous le compte utilisé pour les démarrer.

Quant aux appareils, le système de gestion des comptes est configuré avec un compte utilisé pour vérifier l'identité de l'appareil lors de la connexion de l'appareil au système. Cette capacité vérifie que les appareils sont autorisés à participer aux opérations du système et complète l'authentification des appareils de réseau (voir le 11.2.19, USER 1.19: Authentification des composants), qui est utilisée pour empêcher les appareils non authentifiés d'émettre ou de recevoir sur le réseau.

Les utilisateurs humains et les processus logiciels peuvent également être authentifiés lorsqu'ils établissent une connexion de communication avec un autre processus logiciel, généralement appelé serveur. Dans ce cas, le processus serveur détermine s'il utilise le compte sous lequel il s'exécute ou le compte de l'utilisateur ou du processus logiciel authentifié.

Les rôles, tels qu'opérateur, ingénieur de processus, ingénieur de maintenance et administrateur, représentent des groupes / ensembles de droits d'accès pouvant être attribués à des utilisateurs humains. L'utilisation d'identificateurs, d'authentifiants et de rôles simplifie la gestion des contrôles d'accès des utilisateurs et réduit le risque d'erreur et d'omission dans les processus associés. Voir le 11.2.4, USER 1.4: Attribution de droits d'accès, pour l'attribution des droits d'accès aux comptes d'utilisateurs et aux rôles.

Il convient de définir les rôles pour l'IACS en fonction de la manière dont les utilisateurs utilisent le système. Lorsqu'un compte d'utilisateur est ajouté au système, il convient d'attribuer à ce compte un identificateur, un authentifiant (par exemple, un mot de passe ou une carte à puce) et un ou plusieurs rôles. Les comptes peuvent être créés pour des utilisateurs individuels (utilisateurs humains, processus logiciels et appareils) ou pour un utilisateur logique, généralement pour un logiciel (l'exécutable du logiciel est l'utilisateur logique, tandis que le processus instancié est l'utilisateur individuel). Toutefois, des utilisateurs logiques peuvent également être créés pour des utilisateurs humains (par exemple, un "opérateur de quart de nuit") à condition que le compte soit utilisé par une personne identifiée de manière unique. Les comptes individuels pour les utilisateurs humains sont préférables.

11.2.2 USER 1.2: Suppression de l'identité utilisateur

11.2.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures pour supprimer/désactiver les identificateurs, les authentifiants, les rôles et les droits d'accès spécifiques à l'IACS pour les utilisateurs humains, les processus logiciels et les appareils qui n'ont pas ou plus besoin d'accès.

11.2.2.2 Justification et recommandations supplémentaires

Il convient que l'accès d'un utilisateur à tous les comptes qui lui sont attribués soit supprimé ou désactivé lorsqu'il n'a plus besoin d'accéder à l'IACS, même pour une période temporaire. La conservation dans ce cas de l'accès aux comptes associés à l'utilisateur fournit un chemin d'accès inutile au système.

Il convient de mettre en place un processus pour signaler le moment auquel un utilisateur n'a plus besoin d'accéder au système et pour supprimer / désactiver son accès. Il convient que ce processus soit coordonné avec le service des ressources humaines pour garantir que toute opération concernant un employé (par exemple, mutations, démissions ou licenciements) qui nécessite des actions sur l'identité utilisateur soit immédiatement traitée.

La suppression/désactivation d'accès peut impliquer la suppression/désactivation des comptes attribués à l'utilisateur, la modification des mots de passe des comptes partagés protégés par mot de passe, la récupération des cartes à puce de l'utilisateur humain et leur désactivation, ou des actions similaires pour d'autres types d'authentifiants.

11.2.3 USER 1.3: Persistance de l'identité utilisateur

11.2.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent que les identificateurs, les authentifiants et les rôles d'utilisateur spécifiques à l'IACS, ainsi que les droits d'accès associés, utilisés pour assurer les opérations essentielles de l'IACS, y compris les comptes d'opérateur, soient configurés de manière à ne pas être désactivés automatiquement.

11.2.3.2 Justification et recommandations supplémentaires

L'expiration automatique et d'autres types de désactivations automatiques des comptes, groupes et authentifiants risquent d'entraîner un refus de service pour les opérations essentielles dont le logiciel est exécuté sous ces identités. Les opérations essentielles sont celles qui doivent maintenir la santé, la sécurité, l'environnement et la disponibilité de l'équipement sous contrôle.

Il convient qu'une appréciation des menaces ou du risque identifie les opérations essentielles et les dépendances de leur logiciel, ainsi que les comptes d'utilisateurs sous lesquels ce logiciel est exécuté. Il convient d'établir et d'appliquer des politiques (par le biais d'une vérification, par exemple) pour ces comptes, groupes et authentifiants afin de garantir qu'ils ne sont pas configurés pour une expiration ou une fin automatique.

11.2.4 USER 1.4: Attribution de droits d'accès

11.2.4.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures pour attribuer, réviser et supprimer des droits d'accès pour les rôles spécifiques à l'IACS et pour les utilisateurs.

11.2.4.2 Justification et recommandations supplémentaires

L'identification et l'authentification de l'utilisateur autorisent l'utilisateur à accéder au système et les droits d'accès lui donnent la permission d'utiliser les ressources et les commandes de l'OS et de l'IACS au sein du système. Les droits typiques incluent la lecture, l'écriture et l'exécution. Les droits d'accès sont généralement attribués à des rôles, dont les utilisateurs héritent ensuite des rôles qui leur ont été attribués.

Les droits d'accès appliqués par l'OS et les droits d'accès appliqués par le logiciel du système de commande sont généralement administrés séparément. Les ressources/commandes de l'OS comprennent généralement des fichiers, des données de configuration OS et des données et fonctions d'administrateur OS. Les ressources/commandes du système de commande incluent généralement des paramètres (par exemple, points de consigne et limites d'alarme) et des fonctions d'étalonnage et de maintenance.

11.2.5 USER 1.5: Droit d'accès minimal

11.2.5.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent de vérifier que les utilisateurs IACS se voient uniquement octroyer les droits d'accès minimaux nécessaires à l'exécution des tâches qui leur sont assignées.

11.2.5.2 Justification et recommandations supplémentaires

L'attribution aux utilisateurs IACS de plus de droits d'accès qu'il n'en faut signifie qu'ils ont reçu des capacités (qu'il convient qu'ils n'en disposent pas) de consulter des données, d'apporter des modifications au système, ou les deux. Cela signifie aussi que lorsque les logiciels exécutés sous leur compte sont infectés par des programmes malveillants, ceux-ci disposent également de ces droits supplémentaires. Les utilisateurs IACS incluent tous les utilisateurs qui détiennent des comptes IACS, y compris les opérateurs, les ingénieurs, les administrateurs, le personnel de maintenance et le personnel du fournisseur de produit/fournisseur de service.

Le contrôle d'accès basé sur le rôle (RBAC) est généralement utilisé pour attribuer aux rôles uniquement les droits dont ils ont besoin, puis pour assigner ces rôles uniquement aux utilisateurs qui en ont besoin. Les droits attribués aux comptes de logiciel constituent une préoccupation particulière. Ces comptes reçoivent souvent des privilèges élevés dont ils n'ont pas besoin. Il convient donc de mettre à la disposition des développeurs et des comptes de logiciel les exigences en matière de droit d'accès minimal.

11.2.6 USER 1.6: Authentification des services logiciels

11.2.6.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'identification et à l'authentification des services logiciels avant leur exécution.

11.2.6.2 Justification et recommandations supplémentaires

Deux techniques d'identification et d'authentification logicielles couramment utilisées sont décrites ci-dessous, bien que d'autres puissent satisfaire à cette exigence.

Les services logiciels sont généralement exécutés sous un compte qui leur est attribué. Deux ou plusieurs services logiciels peuvent partager un même compte ou un compte peut être spécifiquement créé pour un seul service logiciel. Il convient donc de ne pas autoriser le démarrage de ces services sans qu'ils aient été préalablement identifiés et authentifiés pour ce compte par l'infrastructure (par exemple, une application de gestion de contrôle de service).

Les signatures numériques et les listes d'autorisation constituent un moyen supplémentaire ou alternatif qui permet de vérifier l'identité et l'authenticité d'un logiciel et d'autoriser son exécution. Elles considèrent que les logiciels d'infrastructure participent également à la vérification de l'identité et à l'autorisation de l'exécution avant le démarrage du service.

11.2.7 USER 1.7: Droits de connexion interactive aux services logiciels

11.2.7.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives au refus de capacités de connexion interactive aux services logiciels.

11.2.7.2 Justification et recommandations supplémentaires

Les services logiciels qui s'exécutent sous un compte qui comporte des privilèges de connexion interactive donnent l'occasion aux attaquants d'utiliser ce compte pour se connecter au système, ce qui élargit la surface d'attaque.

Généralement, les comptes ont des propriétés qui contrôlent leur utilisation. En règle générale, une propriété définit qui autorise/interdit l'utilisation du compte pour les connexions interactives. Il convient de définir la propriété sur "interdire" pour les comptes servant à démarrer les programmes de contrôle de service lorsque cela est pris en charge par le service logiciel.

11.2.8 USER 1.8: Authentification de l'utilisateur humain

11.2.8.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'identification et à l'authentification de tous les utilisateurs humains sur toutes les interfaces IACS utilisables par des utilisateurs humains pour accéder à l'IACS. Ces interfaces comprennent, entre autres:

a) les interfaces de connexion interactive de l'utilisateur humain de l'appareil;

b) les interfaces d'application telles que les services web, les transferts de fichiers et les serveurs OPC; et

c) les interfaces de bureau à distance fournissant aux utilisateurs humains un accès en connexion à des appareils IACS à travers le réseau.

NOTE Certains systèmes d'exploitation assurent, de façon transparente, le transfert de l'identité utilisateur authentifiée vers l'application et mettent l'identité utilisateur à la disposition de l'application.

11.2.8.2 Justification et recommandations supplémentaires

Les utilisateurs humains qui accèdent à l'IACS sans être identifiés et authentifiés posent un risque pour l'IACS. Ces utilisateurs se voient souvent accorder l'accès au moyen des comptes d'"invités" pour l'accès au bureau et des comptes "anonymes" pour l'accès au serveur web. Ces deux types de comptes ont des privilèges restreints, mais ils permettent néanmoins à l'utilisateur de lancer des attaques qui cherchent à découvrir ou à exploiter des vulnérabilités internes du système. Il convient de ne pas utiliser des comptes d'invités et des comptes anonymes dans l'IACS. Il convient d'identifier et d'authentifier correctement tous les utilisateurs avant de leur accorder l'accès.

En outre, les applications client (les tunneliers, par exemple) qui ne transmettent pas de manière sécurisée au serveur l'identité de l'utilisateur humain IACS authentifié, peuvent poser un problème plus important en se connectant au serveur avec un compte qui comporte des privilèges plus élevés que ceux de l'utilisateur humain. Les utilisateurs humains fonctionnent alors avec des privilèges élevés auxquels il convient qu'ils n'aient pas droit.

11.2.9 USER 1.9: Authentification à plusieurs facteurs (MFA)

11.2.9.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation de la MFA par les appareils qui permettent une connexion interactive de l'utilisateur humain pour l'accès distant ou lorsqu'ils sont situés dans des zones d'accès public.

11.2.9.2 Justification et recommandations supplémentaires

La MFA constitue une méthode d'identification et d'authentification plus sécurisée. Elle est généralement composée d'une combinaison de choses connues de l'utilisateur (mot de passe ou numéro d'identification personnel (PIN), par exemple), d'une chose qu'il possède (par exemple, une carte à puce ou un jeton de sécurité) et d'une caractéristique personnelle (par exemple, empreintes digitales ou empreintes rétiniennes). L'utilisation de la MFA pour les stations de travail accessibles aux utilisateurs non-IACS rend plus difficile pour ces utilisateurs de contourner un mécanisme d'authentification à facteur unique, tel qu'un schéma à mot de passe uniquement.

Il convient d'évaluer tous les appareils qui prennent en charge la connexion interactive de l'utilisateur (les stations de travail, par exemple) et qui bénéficient d'un accès à l'IACS pour déterminer s'ils risquent d'être consultés par du personnel non autorisé. Il convient de protéger ceux qui font face à ce risque par un schéma MFA. Lorsque l'utilisation de la MFA n'est pas possible et lorsque le risque d'accès par du personnel non autorisé doit être réduit, des mesures de sécurité compensatoires (l'accès physique, par exemple) associées à l'authentification à facteur unique peuvent être utilisées. Outre ces informations, il convient que les politiques et procédures du propriétaire d'actif spécifient si l'utilisation de la MFA dans l'IACS est approuvée ou non et, le cas échéant, l'emplacement approuvé d'utilisation.

11.2.10 USER 1.10: Authentification mutuelle

11.2.10.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'utilisation de l'authentification mutuelle pour l'accès à toutes les applications serveur hébergées sur des appareils IACS, y compris les serveurs qui utilisent la technologie web.

11.2.10.2 Justification et recommandations supplémentaires

L'authentification mutuelle permet de vérifier dans le processus de connexion que l'utilisateur est connu et autorisé. Elle est également utilisée pour vérifier auprès de l'utilisateur que le processus de connexion est connu et autorisé et qu'il n'usurpe pas (ne prétend pas être) un processus de connexion légitime. Les processus de connexion qui usurpent des processus de connexion légitimes demandent généralement aux utilisateurs de fournir leurs identifiants pour les voler. La même technique d'usurpation peut être utilisée par des attaquants pour amener un opérateur à configurer le mauvais appareil, ce qui constitue un risque pour la disponibilité et l'intégrité de l'IACS.

Il convient d'installer des applications serveur pour utiliser l'authentification mutuelle. Les gestionnaires de serveur web, tels qu'Apache et Microsoft Internet Information Services (IIS), ont généralement la possibilité d'utiliser l'authentification mutuelle. Certains protocoles, comme mTLS, établissent un processus de chiffrement des connexions dans lequel les deux parties, le client et le serveur, utilisent des certificats numériques pour s'authentifier mutuellement à l'aide de services tiers fiables.

11.2.11 USER 1.11: Protection par mot de passe

11.2.11.1 Exigence

Lorsque des mots de passe sont utilisés dans l'IACS, le propriétaire d'actif doit disposer de politiques et de procédures qui visent à accroître le degré de difficulté de compromission des mots de passe, notamment en matière de complexité, de durée de vie et de réutilisation.

11.2.11.2 Justification et recommandations supplémentaires

Les politiques de mot de passe sont utilisées pour rendre plus difficiles la compromission et l'utilisation de mots de passe compromis.

Les politiques de longueur et de complexité de mot de passe peuvent permettre de rendre les compromissions plus difficiles. La durée de vie des mots de passe (délais d'expiration) et les propriétés de réutilisation limitent la période pendant laquelle un mot de passe compromis peut être utilisé pour accéder au système. NIST SP80063B [19] fournit des recommandations relatives à la complexité, à la durée de vie et à la réutilisation des mots de passe.

11.2.12 USER 1.12: Mots de passe partagés et divulgués/compromis

11.2.12.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures de gestion des mots de passe partagés et divulgués/compromis.

11.2.12.2 Justification et recommandations supplémentaires

Les mots de passe des comptes de maintenance et d'autres comptes, tels que les comptes d'opérateurs, sont souvent partagés pour simplifier la gestion des comptes et des mots de passe afin de répondre aux exigences de fonctionnement. Cependant, en l'absence de contrôles appropriés, il peut être difficile de connaître celui qui a accès au système. Dans ces cas, le personnel qui n'a plus besoin d'accès peut toujours être en mesure d'utiliser les mots de passe partagés.

Il convient de définir et d'appliquer les politiques et procédures d'utilisation de mots de passe partagés, y compris les approbations et les enregistrements. Il convient que ces politiques et procédures identifient les comptes sur lesquels des mots de passe peuvent être partagés, la personne qui peut utiliser un mot de passe partagé, la durée de validité d'un mot de passe partagé et les règles de révocation des mots de passe partagés. D'autres politiques et procédures peuvent être définies au besoin, généralement par suite de l'appréciation des risques associés à leur utilisation. Il convient de documenter les exceptions à ces règles.

À noter que des modèles de mot de passe sont parfois utilisés pour simplifier le partage des mots de passe. Toutefois, il est souvent préférable de disposer d'un système de gestion du partage de mot de passe écrit et sécurisé que d'utiliser des modèles de mot de passe pouvant être connus des personnes qui ne sont plus affectées à un espace de travail donné.

11.2.13 USER 1.13: Informations d'affichage de la connexion de l'utilisateur

11.2.13.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui permettent d'afficher les informations de connexion à l'utilisateur afin de faciliter la détection des connexions frauduleuses.

11.2.13.2 Justification et recommandations supplémentaires

Il convient que les utilisateurs participent à la sécurité du système en étant capables d'examiner l'historique des informations de connexion sur leur compte. Les utilisateurs peuvent utiliser, par exemple, ces informations pour déterminer si une autre personne utilisait ou utilise leur compte pour accéder au système.

Il convient de configurer les écrans de connexion de manière à fournir aux utilisateurs des informations adaptées au niveau de risque. Des informations sont normalement fournies sur les historiques de connexion des utilisateurs, tels que la date, l'heure et la station de travail de leur dernière connexion et déconnexion, ainsi que la date, l'heure et la station de travail des sessions de connexion encore ouvertes. D'autres informations peuvent être utiles, telles que celles sur les dernières tentatives de connexion infructueuses.

11.2.14 USER 1.14: Affichage des échecs de connexion de l'utilisateur

11.2.14.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'affichage d'informations après un échec de connexion afin de limiter les informations utiles aux attaquants.

11.2.14.2 Justification et recommandations supplémentaires

Les informations d'échec de connexion, telles que "nom d'utilisateur non valide" ou "mot de passe doit être composé de..." peuvent être utilisées par les attaquants pour affiner leurs tentatives d'intrusion dans le système. Toute information communiquée à des entités non authentifiées peut être utilisée pour des attaques par canal latéral. Il convient donc que les informations d'échec soient réduites le plus possible, en indiquant uniquement à l'utilisateur que la connexion a échoué.

11.2.15 USER 1.15: Échecs de connexion consécutifs

11.2.15.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives au refus de l'accès à la connexion pour les comptes d'utilisateurs pour une durée spécifiée ou jusqu'à ce qu'ils soient déverrouillés, après le nombre configuré de tentatives de connexion infructueuses consécutives, par un administrateur autorisé.

11.2.15.2 Justification et recommandations supplémentaires

L'application d'un nombre maximal d'échecs de connexion consécutifs empêche les attaquants d'essayer en permanence de se connecter, protégeant ainsi contre les tentatives d'épuisement des mots de passe. Cependant, le verrouillage d'un compte après plusieurs échecs de connexion consécutifs rend le compte vulnérable à une attaque par refus de service. Il est alors nécessaire de procéder à une appréciation du risque afin d'identifier les comptes ou les appareils qui doivent être exemptés de la politique de verrouillage, car l'impossibilité de se connecter représente alors un risque plus important pour l'IACS.

Il convient de définir des politiques de compte afin de gérer le verrouillage et le déverrouillage d'un utilisateur après un nombre défini d'échecs de connexion consécutifs.

11.2.16 USER 1.16: Intégrité des sessions

11.2.16.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la protection des sessions contre les accès et les modifications non autorisés.

11.2.16.2 Justification et recommandations supplémentaires

Les sessions sont des connexions d'utilisateur au système établies par le processus de connexion. Elles constituent des ressources système; il convient de les protéger contre les utilisations abusives et les piratages afin d'empêcher que des attaquants n'interfèrent dans les activités de l'utilisateur, ainsi que de les protéger contre les attaquants qui accèdent au système à travers elles.

Les sessions étant des ressources système fondamentales, il convient de les protéger par une authentification, un chiffrement et des listes de contrôle d'accès qui exigent des privilèges administratifs pour permettre l'accès aux sessions.

11.2.17 USER 1.17: Sessions concomitantes

11.2.17.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui visent à limiter le nombre de sessions concomitantes pour tout utilisateur humain, processus logiciel ou appareil.

11.2.17.2 Justification et recommandations supplémentaires

Les utilisateurs ont souvent besoin d'ouvrir plusieurs sessions au même moment pour le fonctionnement de l'IACS. Toutefois, le fait de permettre au système d'accepter un nombre illimité de sessions concomitantes expose l'IACS à un niveau de risque plus élevé lié au détournement de session et aux attaques par refus de service.

Il convient d'évaluer les activités des utilisateurs. Si un utilisateur a besoin de se connecter plusieurs fois simultanément, il convient de déterminer une limite supérieure pratique et de configurer le système en conséquence.

11.2.18 USER 1.18: Verrouillage d'écran

11.2.18.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives au verrouillage des écrans d'utilisateurs à la demande de ces derniers ou automatiquement après une période d'inactivité configurée, à moins que l'impossibilité d'accéder à l'écran n'entraîne un risque plus important pour l'IACS. Une nouvelle authentification doit être exigée d'un utilisateur autorisé avant qu'il ne déverrouille l'écran.

11.2.18.2 Justification et recommandations supplémentaires

Les écrans d'utilisateur inactifs pendant un certain temps sont souvent laissés sans surveillance par l'utilisateur. Il convient dans ces cas de verrouiller l'écran pour empêcher toute utilisation non autorisée de la session. Les écrans d'opérateur sont des écrans utilisés pour contrôler les opérations du processus physique, telles que la visualisation et la réponse aux alarmes, les faces de visualisation et la modification des points de consigne. Il est nécessaire que ces écrans soient disponibles pour contrôler le processus. Par conséquent, ils restent normalement déverrouillés. Il convient que le propriétaire d'actif prenne en considération les risques associés à l'utilisation ou non de verrous d'écran sur les écrans des opérateurs.

Les systèmes d'exploitation ont généralement une fonction de verrouillage d'écran qui peut être configurée pour verrouiller l'écran après une période d'inactivité. La durée d'utilisation dépend d'un certain nombre de facteurs liés à l'environnement physique dans lequel se trouve la station de travail et aux pratiques de travail de l'utilisateur. Il convient de sélectionner une valeur appropriée qui permet à l'utilisateur d'être productif, sans rendre l'écran vulnérable ou l'exposer.

11.2.19 USER 1.19: Authentification des composants

11.2.19.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'identification et à l'authentification de tous les composants connectés à l'IACS.

11.2.19.2 Justification et recommandations supplémentaires

Cette exigence traite de l'aptitude du composant à être authentifié à l'aide des identificateurs associés au 11.2.1, USER 1.1: Attribution d'identité utilisateur. Cependant, certains appareils (les appareils patrimoniaux et les appareils de terrain, par exemple) ne prennent pas toujours en charge des protocoles d'identification et d'authentification, ce qui nécessite l'application de mesures de sécurité compensatoires (des contrôles d'accès physique stricts, par exemple) à ces appareils pour satisfaire à cette exigence.

Au moment de la publication du présent document, des exemples de mécanismes d'authentification différents comprennent, entre autres, l'IEEE (Institut des ingénieurs électriciens et électroniciens) 802.1AR [20], l'EAP (Protocole d'authentification extensible) du Groupe de travail IETF (demande de commentaire RFC 3748 [21], RFC 7057 [22]) et l'ANIMA/BRSKI (Modèle et approche intégrés de mise en réseau autonome du Groupe de travail IETF /amorçage d'une infrastructure de clé sécurisée distante), ainsi que l'IEEE 802.1X [23] définissent des protocoles qui prennent en charge l'identification et l'authentification des appareils. Pour les réseaux d'instrumentation et de commande sans fil, voir l'IEC 62591 Wireless HART™ [24] et l'IEC 62734 ISA-100.11a [25] qui prévoient une connexion sécurisée des appareils aux réseaux sans fil.

11.3 USER 2 – Autorisation et contrôle d'accès

11.3.1 USER 2.1: Autorisation

11.3.1.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à l'application des droits d'accès attribués à tous les utilisateurs.

11.3.1.2 Justification et recommandations supplémentaires

Il convient que des droits d'accès qui permettent d'exécuter des commandes et d'accéder à des ressources (des fichiers, par exemple) soient attribués aux utilisateurs en fonction de leur description de poste. Les droits d'accès servent à protéger les commandes IACS de toute exécution non autorisée et les données IACS de toute divulgation et modification non autorisées.

Il est nécessaire d'appliquer ces droits d'accès pour empêcher les utilisateurs de les contourner au moyen, par exemple, de portes dérobées et de connexions directes aux appareils. Un tel contournement peut fournir un accès aux utilisateurs qui ne disposent pas de droits d'accès appropriés, occasionnant ainsi un accès non contrôlé aux commandes et données IACS et aux ressources physiques qu'elles représentent. Les applications client qui se connectent aux serveurs IACS à l'aide de comptes qui possèdent des privilèges de lecture et d'écriture sur les paramètres protégés (par exemple, points de consigne et limites d'alarme) peuvent également être utilisées pour contourner les contrôles d'accès. Cela peut se produire lorsque l'application client ne vérifie pas les privilèges utilisateur et que les utilisateurs ne disposant pas de privilèges d'accès aux paramètres protégés sont autorisés à exécuter l'application client.

Il convient d'effectuer des évaluations de sécurité pour identifier tous les chemins d'accès à l'IACS et pour vérifier que tous sont soumis à des contrôles d'accès. Se reporter à l'IEC 62443-3-2 pour plus de précisions sur l'utilisation des évaluations de sécurité dans un IACS.

11.3.2 USER 2.2: Séparation des tâches

11.3.2.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures relatives à la séparation des tâches, qui réduisent les privilèges accordés aux utilisateurs de l'IACS à un niveau minimal nécessaire.

11.3.2.2 Justification et recommandations supplémentaires

Il convient que les politiques et les procédures de séparation des tâches appliquent le principe du droit d'accès minimal. Selon ce droit, il convient qu'aucun utilisateur se voit octroyer des privilèges lui permettant de faire mauvais usage du système. Ce principe protège l'IACS du sabotage, de la fraude ou des erreurs accidentelles susceptibles d'endommager le système.

Il convient de ne pas autoriser les utilisateurs IACS connectés à l'OS avec des comptes d'administrateur à accéder aux ordres et ressources de commande IACS. Lorsqu'un tel utilisateur a effectivement accès à l'IACS et qu'un programme malveillant infecte son appareil, le programme malveillant prend entièrement contrôle de l'appareil (par exemple, les stations de travail des ingénieurs ou les stations d'opérateurs) et a ainsi accès à toutes les fonctions du système de commande accessibles par cet appareil. Il convient donc que les utilisateurs IACS qui doivent accéder à l'IACS soient connectés à l'OS avec des privilèges non administratifs.

11.3.3 USER 2.3: Approbations multiples

11.3.3.1 Exigence

Le propriétaire d'actif doit disposer de politiques et de procédures qui vérifient que les actions susceptibles de nuire au processus industriel exigent l'approbation de deux utilisateurs au moins, à moins que le défaut d'exécution de cette action puisse avoir une incidence plus importante sur le processus industriel.

11.3.3.2 Justification et recommandations supplémentaires

Certaines commandes ou modifications de données dans l'IACS peuvent avoir des implications importantes, notamment en matière de HSE. Dans ces cas, il est nécessaire qu'une appréciation du risque soit effectuée pour déterminer si les conséquences des modifications sont suffisamment graves pour exiger l'autorisation de deux utilisateurs au moins et pour déterminer si l'application d'approbations multiples peut introduire un risque plus important en augmentant les probabilités d'échec dans l'exécution de l'opération dans les délais impartis. Se reporter à l'IEC 62443-3-2 pour plus de précisions sur l'utilisation des évaluations de sécurité dans un IACS.

De nombreux composants de l'IACS n'ont pas toujours la possibilité d'appliquer des approbations multiples pour effectuer une action. Dans ce cas, la satisfaction à cette exigence doit être régie par une politique ou appliquée au moyen d'un système de gestion du réseau capable d'exiger des approbations multiples utilisant différents comptes de système pour effectuer une action. Cela assure la vérification par une seconde partie (ou plusieurs parties) avant l'exécution de ces commandes ou de ces modifications de données.

Il convient d'effectuer des évaluations de sécurité et de HSE pour identifier toutes les commandes et toutes les modifications de données qui ont des conséquences graves sur l'IACS. Pour celles qui l'ont, veiller à ce que l'approbation de deux utilisateurs au moins soit exigée et que cette capacité soit prise en charge par l'IACS.