# IEC 62443-2-1

Edition 1.0 2010-11

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

## Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

## About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

## About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

**Useful links:**

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

---

## A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

## A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

**Liens utiles:**

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

# IEC 62443-2-1

Edition 1.0 2010-11

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

colour inside

## Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

## Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XH

ICS 25.040.40; 33.040

ISBN 978-2-88912-037-6

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

# INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

## Part 2-1: Establishing an industrial automation and control system security program

## 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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This bilingual version (2012-04) corresponds to the monolingual English version, published in 2010-11.

The text of this standard is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 65/457/FDIS | 65/461/RVD |

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

The French version of this standard has not been voted upon.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all existing parts of IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website. The full list of existing and intended parts can also be found in the Bibliography of this standard.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

NOTE The revision of this international standard will be initiated shortly after this standard is published. The next revision will be aligned more closely with ISO/IEC 27001, which addresses many of the same issues but without consideration of the specialized requirements for continuous operation and safety that are common in the industrial automation and control systems environment.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.**

# 0 INTRODUCTION

## 0.1 Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established cyber security management systems (CSMS) in place as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (see ISO/IEC 17799 [23][1] and ISO/IEC 27001 [24]). These management systems provide an organization with a well-established method for protecting its assets from cyber attacks.

Industrial automation and control system (IACS) organizations have begun using commercial off the shelf (COTS) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the IACS equipment. These systems are not usually as robust, in the IACS environment, as are systems designed specifically as IACS at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the pre-existing IT and business cyber security solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent consequences.

## 0.2 A cyber security management system for IACS

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. This standard addresses the aspects of the elements included in a CSMS for IACS and also provides guidance on how to go about developing the CSMS for IACS.

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 cyber security risks with IACS. However, a frequent mistake made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that needs to address the entire set of IACS as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system may require a cultural change within the organization.

Addressing cyber security on an organization-wide basis can seem like a daunting task. Unfortunately there is no simple cookbook for security. There is good reason for this. There is not a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is really a balance of risk versus cost. All situations will be different. In some situations the risk may be related to HSE factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore a cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

## 0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799 [23] and ISO/IEC 27001 [24] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to IACS as well. This standard emphasizes the need

1 Numbers in square brackets refer to the Bibliography.

for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this standard are encouraged to read ISO/IEC 17799 and ISO/IEC 27001 for additional supporting information. This standard builds on the guidance in these ISO/IEC standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS may have HSE implications and should be integrated with other existing risk management practices addressing these risks.

# INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

# Part 2-1: Establishing an industrial automation and control system security program

## 1 Scope

This part of IEC 62443 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1.

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

NOTE 1 Other documents in the IEC 62443 series and in the Bibliography discuss specific technologies and/or solutions for cyber security in more detail.

The guidance provided on how to develop a CSMS is an example. It represents the author's opinion on how an organization could go about developing the elements and may not work in all situations. The users of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning CSMS for an organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE 2 There may be cases where a pre-existing CSMS is in place and the IACS portion is being added or there may be some organizations that have never formally created a CSMS at all. The authors of this standard cannot anticipate all cases where an organization will be establishing a CSMS for the IACS environment, so this standard does not attempt to create a solution for all cases.

## 2 Normative references

The following referenced documents are indispensable for the application 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[2] – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

## 3 Terms, definitions, abbreviated terms, acronyms, 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.

---

2 This standard is derived from ANSI/ISA 99.02.01:2009 and wholly replaces it for international use. It is intended that the second edition of IEC/TS 62443-1-1 be an International Standard, not a TS, after inclusion of some normative requirements to which conformance is possible.

**3.1.1**
**access account**
access control function that allows the user access to a particular set of data or functions for certain equipment

NOTE Many times accounts are linked to user identifications (IDs) and passwords. These user IDs and passwords may be linked to an individual or group of individuals such as a control room work team performing the same set of operating tasks.

**3.1.2**
**administrative practices**
defined and documented practices/procedures that individuals are personally accountable to follow at all times

NOTE These are usually in the conditions of employment for the organization. In the IACS environment, these often have HSE implications.

**3.1.3**
**asset**
physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

[IEC/TS 62443-1-1, 3.2.6]

NOTE In this specific case, an asset is any item that should be protected as part of the CSMS.

**3.1.4**
**authentication**
security measure designed to establish the validity of a transmission, message or originator or a means of verifying an individual's authorization to receive specific categories of information

[IEC/TS 62443-1-1, 3.2.13]

**3.1.5**
**burner management system**
system for the safe start-up, monitoring and shutdown of burner systems associated with boilers, flares, incinerators, gas turbines, thermal oxidizers, and other fired equipment

**3.1.6**
**business continuity plan**
document with identified procedures for recovering from a significant disruption and restoring business operations

NOTE 1 This umbrella term also refers to other aspects of disaster recovery, such as emergency management, human resources and media or press relations.

NOTE 2 A business continuity plan also identifies procedures for sustaining essential business operations while recovering from a significant disruption.

**3.1.7**
**business continuity planning**
process to develop a business continuity plan

**3.1.8**
**change management**
process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control

**3.1.9**
**compliance**
adherence to the requirements in one standard by another

Adapted from [ISO/IEC 10746-2, 15.1]

NOTE This is a relationship between two specifications, A and B, which holds when specification A makes requirements which are all fulfilled by specification B (when B complies with A)

**3.1.10**
**conformance**
relationship between an implementation and a standard where any proposition that is true in the standard must be true in its implementation

Adapted from [ISO/IEC 10746-2, 15.1]

NOTE The conformance relationship holds when specific requirements in the specification (the conformance requirements) are met by the implementation. Conformance assessment is the process through which this relation is determined.

**3.1.11**
**consequence**
result that occurs from a particular incident

**3.1.12**
**critical**
very important device, computer system, process, and the like that, if compromised by an incident, could have high financial, health, safety or environmental (HSE) impact to an organization

**3.1.13**
**cyber security management system**
program designed by an organization to maintain the cyber security of the entire organization's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the IACS side of the organization

**3.1.14**
**device requirements**
countermeasure characteristics necessary for the devices within a zone to achieve the desired target security level

**3.1.15**
**gatekeeper**
trusted individual that senior managers consult to prioritize issues they need to address over the remaining issues that others are more suited to address

**3.1.16**
**health, safety and environment**
responsibility for protecting the health and safety of workers and the surrounding community and maintaining high environmental stewardship

**3.1.17**
**human-machine interface**
aggregate of means by which people (the users) interact with a particular machine, device, computer program or other complex tool (the system)

NOTE In many cases, these involve video screens or computer terminals, push buttons, auditory feedback, flashing lights, and the like. The human-machine interface provides means of:

- Input, allowing the users to control the machine;
- Output, allowing the machine to inform the users.

**3.1.18**
**incident**
event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

**3.1.19**
**independent audit**
review of an organization (policies, procedures, processes, equipment, personnel, and the like) by an external group not affiliated with the organization

NOTE This may be required for public companies.

**3.1.20**
**information technology**
computer-related assets of an organization that represent nonphysical assets, such as software applications, process programs and personnel files

NOTE 1 This use of the term information technology is not abbreviated throughout this document.

NOTE 2 Another use of the term information technology (IT) refers to the company's internal organization (for example, the IT department) or the items traditionally maintained by this department (that is, the administrative computers, servers and network infrastructure). This use of the term information technology is abbreviated as IT throughout this standard.

**3.1.21**
**legacy system**
existing industrial automation and control system in a facility that may not be available as a commercial off the shelf (COTS) item

NOTE A legacy system may have been COTS at one time, but it may be no longer available and/or supported.

**3.1.22**
**likelihood**
quantitative estimation that an action, event or incident may occur

**3.1.23**
**local user**
user who is inside the perimeter of the security zone being addressed

NOTE A person in the immediate manufacturing area or control room is an example of a local user.

**3.1.24**
**manufacturing execution system**
production scheduling and tracking system used to analyze and report resource availability and status, schedule and update orders, collect detailed execution data such as material usage, labor usage, operating parameters, order and equipment status and other critical information

NOTE 1 This system accesses bills of material, routing and other data from the base enterprise resource planning system and is typically used for real-time shop floor reporting and monitoring that feeds activity data back to the base system.

NOTE 2 Refer to IEC 62264-1 for additional information.

**3.1.25**
**MAC address**
hardware address that differentiates one device on a network from another

**3.1.26**
**operator**
particular type of user that is usually responsible for the correct operation of the equipment under control

**3.1.27**
**patch management**
area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system

NOTE Patch management tasks include: maintaining current knowledge of available patches, deciding which patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required remotely across heterogeneous environments according to recognized best practices.

**3.1.28**
**process engineer**
person typically responsible for the technical aspects of the industrial operation and who uses the IACS and other tools to oversee and manage the industrial automation in the facility

**3.1.29**
**process information management system**
set of systems that provides supporting information to assist with the operation of the facility

**3.1.30**
**programmable logic controller**
programmable microprocessor-based device that is used in industry to control assembly lines and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant

NOTE Typically programmed as in [14], a PLC is designed for real time use in rugged, industrial environments. Connected to sensors and actuators, PLCs are categorized by the number and type of I/O ports they provide and by their I/O scan rate.

**3.1.31**
**process safety management**
regulation intended to prevent a disaster in chemical and biotechnology systems by addressing sound management and engineering design

**3.1.32**
**remote access**
communication with, or use of, assets or systems within a defined perimeter from any location outside that perimeter

**3.1.33**
**remote user**
user who is outside the perimeter of the security zone being addressed

EXAMPLE A person in an office in the same building, a person connecting over the corporate wide area network (WAN) and a person connecting over public infrastructure networks are all remote users.

**3.1.34**
**risk assessment**
process of identifying and evaluating risks to the organization’s operations (including mission, functions, image, or reputation), the organization’s assets or individuals by determining the likelihood of occurrence, the resulting impact, and additional countermeasures that would mitigate this impact

NOTE Synonymous with risk analysis and incorporates threat and vulnerability analyses.

**3.1.35**
**risk mitigation**
actions to reduce the likelihood and/or severity of an event

**3.1.36**
**risk tolerance**
risk the organization is willing to accept

**3.1.37**
**self-assessment**
review of an organization (that is, policies, procedures, operations, equipment and personnel) by a group inside the organization

NOTE This group may be either directly associated with the organization's business process or may be in another part of the organization, but should be intimately familiar with the risks associated with that business process.

**3.1.38**
**Six Sigma®**
process-focused methodology designed to improve business performance through improving specific areas of strategic business processes

**3.1.39**
**social engineering**
practice of obtaining confidential information by manipulation of legitimate users

**3.1.40**
**stakeholder**
individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services

NOTE Stakeholders influence programs, products and services. In this particular case, stakeholders are personnel in an organization responsible for promoting and overseeing the cyber security process. These personnel include the manager of the cyber security program as well as the cross-functional team of individuals from all of the departments affected by the cyber security program.

**3.1.41**
**system administrator**
person(s) responsible for managing the security of the computer system

NOTE This may include operating system maintenance, network management, account administration and patch management, in accordance with the change management process.

**3.1.42**
**system requirements**
attributes of the desired target security level

**3.1.43**
**ushered access**
**shadowing**
procedure for monitoring the actions of a remotely connected user

**3.1.44**
**vulnerability assessment**
formal description and evaluation of the vulnerabilities in a system

### 3.2 Abbreviated terms and acronyms

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

| | |
|---|---|
| ANSI | American National Standards Institute |
| CFR | U.S. Code of Federal Regulations |
| ChemITC | Chemical Information Technology Center of the American Chemistry Council |
| COTS | Commercial off the shelf |

| | |
|---|---|
| CPU | Central processing unit |
| CSCSP | Chemical Sector Cyber Security Program |
| CSMS | Cyber security management system |
| CSVA | Cyber security vulnerability assessment |
| DCS | Distributed control system |
| DMZ | Demilitarized zone |
| DoS, DDoS | Denial of service, Distributed denial of service |
| FDN | Field device network |
| FTP | File transfer protocol |
| HMI | Human machine interface |
| HSE | Health, safety and environmental |
| HVAC | Heating, ventilation, and air-conditioning |
| IACS | Industrial automation and control system(s) |
| ID | Identification |
| IEC | International Electrotechnical Commission |
| IEEE | The Institute of Electrical and Electronics Engineers |
| IP | Internet protocol |
| ISA | International Society of Automation |
| ISO | International Organization for Standardization |
| IT | Information technology |
| KPI | Key performance indicator(s) |
| LAN | Local area network |
| MAC | Media access control |
| MES | Manufacturing execution system |
| NERC | North American Electric Reliability Council (applies to U.S. and Canada) |
| NIST | U.S. National Institute of Standards and Technology |
| OS | Operating system |
| PC | Personal computer |
| PCN | Process control network |
| PCSRF | NIST Process Control Security Requirements Forum |
| PIM | Process information management |
| PIN | Personal identification number |
| PLC | Programmable logic controller |
| PSM | Process safety management |
| RAID | Redundant array of independent disks |
| RCN | Regulatory control network |
| SANS | SysAdmin, Audit, Networking, and Security Institute |
| SCADA | Supervisory control and data acquisition |
| SI | International System of Units |

| | |
|---|---|
| SIS | Safety instrumented system(s) |
| SoA | Statement of applicability |
| SOC | Standard operating condition |
| SOP | Standard operating procedure |
| SP | Special Publication (by NIST) |
| SSL | Secure socket layer |
| TCP | Transmission control protocol |
| TR | Technical report |
| VLAN | Virtual local area network |
| VPN | Virtual private network |
| WAN | Wide area network |

### 3.3 Conventions

The elements of a CSMS are the following:

- the objective of the element,
- a basic description of the element,
- a rationale to explain why the element is included and
- the requirements for that element.

A tabular presentation is used to provide a description and requirements for each element. The requirements are numbered similar to subclauses (but are not in themselves subclauses), so that the requirements can be referenced individually and selectively.

## 4 Elements of a cyber security management system

### 4.1 Overview

This clause presents the elements that constitute a CSMS for IACS. These elements represent what shall and should be included in the CSMS in order to protect IACS against cyber attacks.

The elements are presented in the following three main categories:

- Risk analysis,
- Addressing risk with the CSMS, and
- Monitoring and improving the CSMS.

Each of these categories is further divided into element groups and/or elements. Figure 1 depicts the relationship between the categories, element groups and elements.

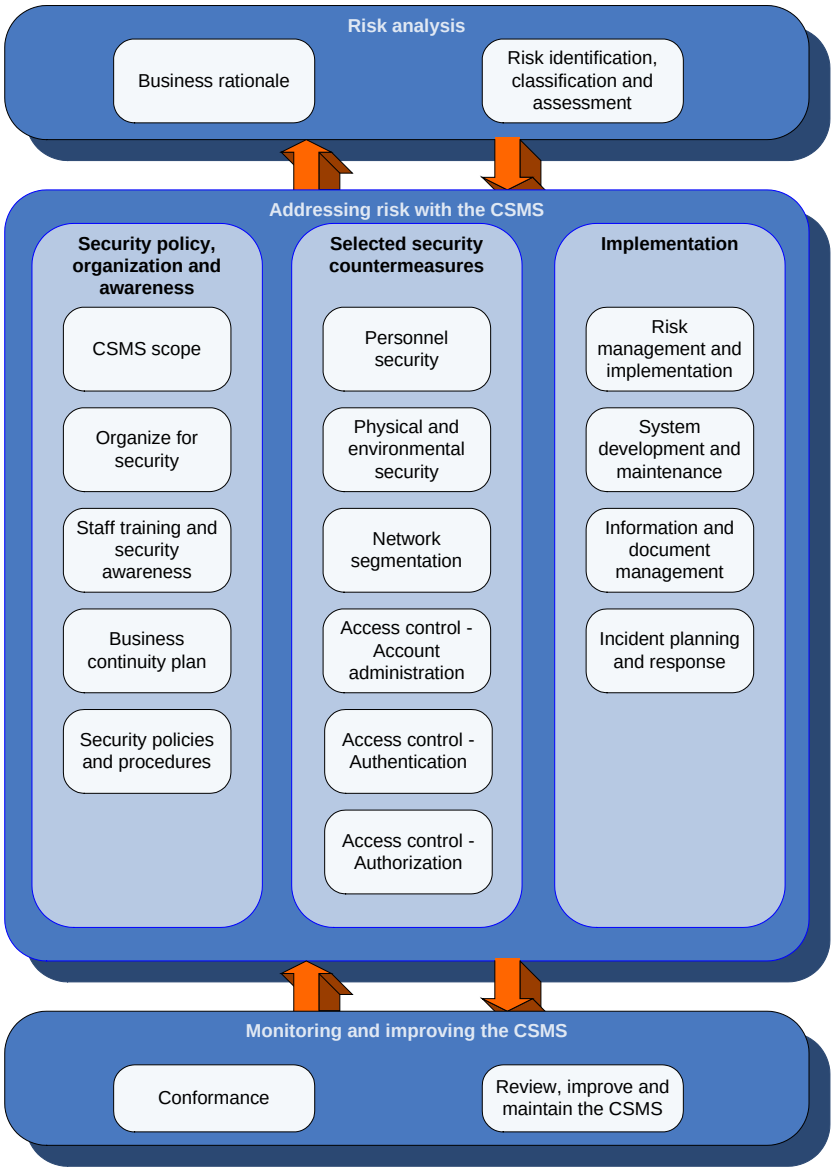



**Figure 1 – Graphical view of elements of a cyber security management system**

Each element in this clause lists the objective of the element, a basic description of the element, a rationale to explain why the element is included and the requirements for that element.

Annex A follows the same basic structure of this clause with categories, element groups and elements. However, the annex provides guidance on how to develop the elements of the CSMS. The reader should read Annex A in order to understand the special needs and issues involved with developing a CSMS for IACS. The guidance discussed in Annex A should be tailored to the special requirements of each organization.

This standard specifies the elements required for a CSMS. It is not the intent of the standard to specify a particular sequential process for identifying and addressing risk that incorporates these elements. Thus an organization will create such a process in accordance with its culture, organization and the current status of its cyber security activities. To assist organizations with this aspect of applying the standard, A.3.4.2 provides an example of a process for identifying and addressing risk. In addition, Annex B offers insights on effective ordering for activities related to all of the elements discussed in this standard.

While a CSMS is an excellent tool for managing risk within a large company it is equally applicable to small companies as well. The CSMS may be more formalized in a large company so it can be used in many different situations and geographies. In a small company, similar CSMS activities need to be conducted, but they may not be as formal. Clause 4 and Annex A provide guidance to help the user better understand the elements and activities of a CSMS.

## 4.2 Category: Risk analysis

### 4.2.1 Description of category

The first main category of the CSMS is Risk analysis. This category discusses much of the background information that feeds into many of the other elements in the CSMS. Figure 2 shows the two elements that are part of the category:

- Business rationale and
- Risk identification, classification and assessment.


**Figure 2 – Graphical view of category: Risk analysis**

### 4.2.2 Element: Business rationale

**Objective:**

Identify and document the unique needs of an organization to address cyber risk for IACS.

**Description:**

A business rationale is based on the nature and magnitude of financial, HSE, and other potential consequences should IACS cyber incidents occur.

**Rationale:**

Establishing a business rationale is essential in order for an organization to maintain management buy in to an appropriate level of investment for the IACS cyber security program.

**Requirements:**

**Table 1 – Business rationale: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.2.2.1** | **Develop a business rationale** | The organization should develop a high-level business rationale, as a basis for its effort to manage IACS cyber security, which addresses the unique dependence of the organization on IACS. |

### 4.2.3 Element: Risk identification, classification and assessment

**Objective:**

Identify the set of IACS cyber risks that an organization faces and assess the likelihood and severity of these risks.

**Description:**

Organizations protect their ability to perform their mission by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. The first set of requirements present the actions an organization takes to carry out both a high-level and detailed risk assessment that incorporates vulnerability assessment, in a typical chronological order. Among these requirements, those related to preparing for high-level and detailed risk assessments are 4.2.3.1, 4.2.3.2 and 4.2.3.8 below. The last few requirements (4.2.3.10 to 4.2.3.14) are general requirements that apply to the overall risk assessment process. Subclause 4.3.4.2 covers the process of taking action based upon this assessment.

**Rationale:**

Since the purpose of investing in cyber security is to lower risk, it is driven by an understanding of level of risk and potential mitigations.

**Requirements:**

**Table 2 – Risk identification, classification and assessment: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.2.3.1** | **Select a risk assessment methodology** | The organization shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets. |
| **4.2.3.2** | **Provide risk assessment background information** | The organization should provide participants in the risk assessment activity with appropriate information including methodology training, before beginning to identify the risks. |
| **4.2.3.3** | **Conduct a high-level risk assessment** | A high-level system risk assessment shall be performed to understand the financial and HSE consequences in the event that availability, integrity or confidentiality of the IACS is compromised. |
| **4.2.3.4** | **Identify the IACS** | The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk and group the devices into logical systems. |
| **4.2.3.5** | **Develop simple network diagrams** | The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types and general locations of the equipment. |
| **4.2.3.6** | **Prioritize systems** | The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system. |
| **4.2.3.7** | **Perform a detailed vulnerability assessment** | The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks. |
| **4.2.3.8** | **Identify a detailed risk assessment methodology** | The organization's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment. |
| **4.2.3.9** | **Conduct a detailed risk assessment** | The organization shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment. |
| **4.2.3.10** | **Identify the reassessment frequency and triggering criteria** | The organization shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, organization, or industrial operation changes. |

| Description | | Requirement |
|---|---|---|
| **4.2.3.11** | **Integrate physical, HSE and cyber security risk assessment results** | The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk. |
| **4.2.3.12** | **Conduct risk assessments throughout the lifecycle of the IACS** | Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement. |
| **4.2.3.13** | **Document the risk assessment** | The risk assessment methodology and the results of the risk assessment shall be documented. |
| **4.2.3.14** | **Maintain vulnerability assessment records** | Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS. |

## 4.3 Category: Addressing risk with the CSMS

### 4.3.1 Description of category

The second main category of the CSMS is Addressing risk with the CSMS. This category contains the bulk of the requirements and information contained in the CSMS. It is divided into the following three element groups:

- Security policy, organization and awareness,
- Selected security countermeasures, and
- Implementation.

### 4.3.2 Element group: Security policy, organization and awareness

#### 4.3.2.1 Description of element group

The first element group in this category discusses the development of the basic cyber security policies, the organizations responsible for cyber security and the awareness within the organization of cyber security issues. Figure 3 shows a graphical representation of the five elements contained in this element group:

- CSMS scope,
- Organizing for security,
- Staff training and security awareness,
- Business continuity plan and
- Security policies and procedures.


**Figure 3 – Graphical view of element group: Security policy, organization and awareness**

#### 4.3.2.2 Element: CSMS scope

**Objective:**

Identify, assess and document the systems, processes and organizations to which the CSMS applies.

**Description:**

The scope includes all aspects of the IACS, integration points with business partners, customers and suppliers.

**Rationale:**

Management should understand the boundaries where the CSMS applies to the organization as well as establish a direction and focus for the CSMS. By developing a clearly defined scope, it is easier for management to convey its goals and purpose for the CSMS.

**Requirements:**

**Table 3 – CSMS scope: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.2.2.1** | **Define the scope of the CSMS** | The organization shall develop a formal written scope for the cyber security program. |
| **4.3.2.2.2** | **Define the scope content** | The scope should explain the strategic goals, process, and timing for the CSMS. |

#### 4.3.2.3 Element: Organizing for security

**Objective:**

Establish the entities responsible for managing, conducting and assessing the overall cyber security of the organization's IACS assets.

**Description:**

Senior leadership establishes an organization, structure or network of people to provide oversight and direction for managing cyber security risks associated with IACS. They also provide the personnel necessary to conduct and assess the cyber security programs throughout the organization over the life of the CSMS. An organization at any level may implement this standard, including a company or other overall enterprise, division, plant or subset of a plant.

**Rationale:**

Commitment to a security program begins at the top of the organization. Because cyber security of IACS involves several different sets of skills not often found in any one particular section or department of an organization, it is imperative that senior leadership formulate an approach to managing security with clear identification of accountability and responsibility that makes good use of skills and labor resources. This may take several different forms from a single organization to a network of people working together to address different security aspects. The particular approach is highly dependent upon an organization's operational culture.

**Requirements:**

**Table 4 – Organizing for security: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.2.3.1** | **Obtain senior management support** | The organization shall obtain senior management support for a cyber security program. |
| **4.3.2.3.2** | **Establish the security organization(s)** | There shall be an organization, structure or network of stakeholders established (or chosen) under management leadership, with the responsibility to provide clear direction and oversight for the cyber aspects of the IACS. |
| **4.3.2.3.3** | **Define the organizational responsibilities** | Organizational responsibilities shall be clearly defined for cyber security and related physical security activities. |
| **4.3.2.3.4** | **Define the stakeholder team makeup** | The core team of stakeholders should be cross-functional in nature to bring together the skills necessary to address security in all parts of the IACS. |

### 4.3.2.4 Element: Staff training and security awareness

**Objective:**

Provide all personnel (including employees, contract employees and third-party contractors) with the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to IACS and to help ensure their own work practices are using effective countermeasures.

**Description:**

All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering.

**Rationale:**

In the area of IACS, the same emphasis should be placed on cyber security as on safety and operational integrity, because the consequences can be just as severe. Security awareness for all personnel is an essential tool for reducing cyber security risks. Knowledgeable and vigilant staff are one of the most important lines of defense in securing a system. It is therefore important for all personnel to understand the importance of security in maintaining the safe operation of the system.

**Requirements:**

**Table 5 – Staff training and security awareness: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.2.4.1** | **Develop a training program** | The organization shall design and implement a cyber security training program. |
| **4.3.2.4.2** | **Provide procedure and facility training** | All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities. |

| Description | | Requirement |
|---|---|---|
| **4.3.2.4.3** | **Provide training for support personnel** | All personnel that perform risk management, IACS engineering, system administration/maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks. |
| **4.3.2.4.4** | **Validate the training program** | The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training. |
| **4.3.2.4.5** | **Revise the training program over time** | The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities. |
| **4.3.2.4.6** | **Maintain employee training records** | Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis. |

### 4.3.2.5 Element: Business continuity plan

**Objective:**

Identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

**Description:**

A business continuity plan should address the recovery objectives for the various systems and subsystems involved based on typical business needs, a list of potential interruptions and the recovery procedures for each, as well as a schedule to test part or all of the recovery procedures. One of the primary recovery objectives should be to maintain maximum availability of the control system.

**Rationale:**

No set of defenses can prevent all disruptions due to cyber security incidents. A detailed Business Continuity Plan ensures that IACS information can be restored and utilized as soon as possible after the occurrence of a significant disruption.

**Requirements:**

**Table 6 – Business continuity plan: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.2.5.1** | **Specify recovery objectives** | Prior to creating a business continuity plan, the organization shall specify recovery objectives for the systems involved based on business needs. |
| **4.3.2.5.2** | **Determine the impact and consequences to each system** | The organization should determine the impact to each system due to a significant disruption and the consequences associated with loss of one or more of the systems. |
| **4.3.2.5.3** | **Develop and implement business continuity plans** | Continuity plans shall be developed and implemented to ensure that business processes can be restored in accordance with recovery objectives. |
| **4.3.2.5.4** | **Form a business continuity team** | A business continuity team should be formed including IACS and other process owners. In the event of a significant disruption, this team should determine the priority of critical business and IACS systems to re-establish operations. |

| Description | | Requirement |
|---|---|---|
| **4.3.2.5.5** | **Define and communicate specific roles and responsibilities** | The business continuity plan shall define and communicate the specific roles and responsibilities for each part of the plan. |
| **4.3.2.5.6** | **Create backup procedures that support business continuity plan** | The organization shall create backup and restore procedures (see 4.3.4.3.9) that support the business continuity plan. |
| **4.3.2.5.7** | **Test and update the business continuity plan** | The business continuity plan shall be tested on a regular basis and updated as necessary. |

### 4.3.2.6 Element: Security policies and procedures

**Objective:**

Address how an organization defines security, operates its security program, defines and addresses its tolerance for risk and reviews its program to make further improvements.

**Description:**

Cyber security policies for the IACS environment should be developed based on existing high-level policies, characterized risks and the risk tolerance levels identified by management. Cyber security procedures are developed from the cyber security policies and identify how the policies are to be implemented.

**Rationale:**

These written policies and procedures allow employees, contractors, third parties, and the like to clearly understand the company perspective of cyber security and their roles and responsibilities in securing the company's assets.

**Requirements:**

**Table 7 – Security policies and procedures: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.2.6.1** | **Develop security policies** | The organization shall develop high-level cyber security policies for the IACS environment which are approved by management. |
| **4.3.2.6.2** | **Develop security procedures** | The organization shall develop and approve cyber security procedures, based on the cyber security policies and provide guidance in how to meet the policies. |
| **4.3.2.6.3** | **Maintain consistency between risk management systems** | Cyber security policies and procedures that deal with IACS risks should be consistent with or extensions of policies created by other risk management systems. |
| **4.3.2.6.4** | **Define cyber security policy and procedure compliance requirements** | Cyber security policies and procedures, for the IACS environment, shall include compliance requirements. |
| **4.3.2.6.5** | **Determine the organization's tolerance for risk** | The organization shall determine and document its risk tolerance as a basis for creation of policy and risk management activities. |
| **4.3.2.6.6** | **Communicate the policies and procedures to the organization** | Cyber security policies and procedures, for the IACS environment, shall be communicated to all appropriate personnel. |

| Description | | Requirement |
|---|---|---|
| **4.3.2.6.7** | **Review and update the cyber security policies and procedures** | The cyber security policies and procedures shall be reviewed regularly, validated to confirm that they are up-to-date and being followed and updated as required to ensure that they remain appropriate. |
| **4.3.2.6.8** | **Demonstrate senior leadership support for cyber security** | Senior leadership shall demonstrate commitment to cyber security by endorsing the cyber security policies. |

### 4.3.3 Element group: Selected security countermeasures

#### 4.3.3.1 Description of element group

The second element group within this category is Selected security countermeasures. The elements within this group discuss some of the main types of security controls that are part of a well designed CSMS. This document does not attempt to describe the full implementation of any of these selected security countermeasures. It discusses many of the policy, procedure and practice issues related to these particular security countermeasures. Figure 4 shows a graphical representation of the six elements in the element group:

- Personnel security,
- Physical and environmental security,
- Network segmentation,
- Access control – Account administration,
- Access control – Authentication and
- Access control – Authorization.

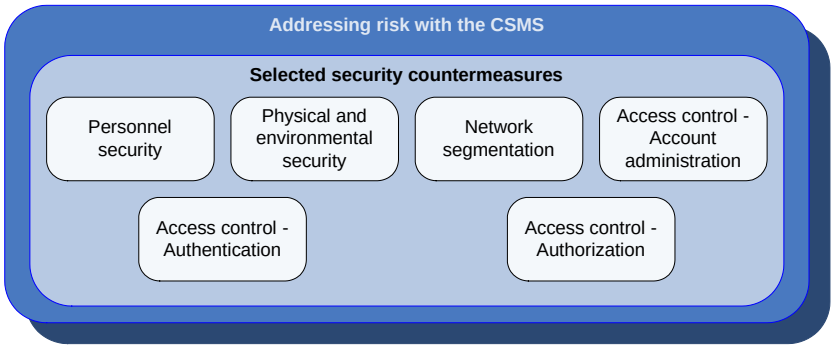



**Figure 4 – Graphical view of element group: Selected security countermeasures**

These particular countermeasures were selected for inclusion because their broad impact on policy and architecture makes it essential to consider them up front when constructing any CSMS. It is not the intent of this standard to specify a complete and sufficient list of countermeasures, since completeness is determined through the process of risk assessment and management described in the standard.

#### 4.3.3.2 Element: Personnel security

**Objective:**

Establish the policies and procedures to determine whether personnel will maintain the IACS security of the organization throughout the lifecycle of their employment.

**Description:**

Personnel security involves looking at new and current personnel to determine if they will maintain the IACS security for the organization. For new personnel, it evaluates them prior to their entry into the organization making sure they demonstrate behaviors consistent with their future security responsibility. For current personnel, it establishes that they continue to demonstrate behavior consistent with their current security responsibilities.

**Rationale:**

In many organizations, personnel security requirements are driven by concerns about insider threats and the possibility of accidents caused by inattention to detail or by personnel unfit for a job due to lack of proper background or the use of substances that might cloud judgment. By implementing personnel security policies it may be possible to reduce these types of problems.

**Requirements:**

**Table 8 – Personnel security: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.2.1** | **Establish a personnel security policy** | There shall be a personnel security policy established, clearly stating the organization's commitment to security and the security responsibilities of personnel. (Personnel include employees, prospective employees, contract employees, and third-party contractors.) |
| **4.3.3.2.2** | **Screen personnel initially** | Unless government regulation prohibits it, all personnel with access to the IACS (both physical and cyber), including new hires and internal transfers to sensitive positions shall be screened, including validation of their identity and background checks, during the job application process. |
| **4.3.3.2.3** | **Screen personnel on an ongoing basis** | Personnel should also be subject to ongoing scrutiny for changes that might indicate a conflict of interest or concern for performing the job in an appropriate manner. |
| **4.3.3.2.4** | **Address security responsibilities** | The personnel security policy should address security responsibilities from recruitment through the end of employment, especially for sensitive positions. |
| **4.3.3.2.5** | **Document and communicate security expectations and responsibilities** | Security expectations and responsibilities shall be clearly documented and regularly communicated to personnel. |
| **4.3.3.2.6** | **State cyber security terms and conditions of employment clearly** | Terms and conditions of employment shall clearly state the personnel's responsibility for cyber security. These responsibilities shall extend for a reasonable period of time after employment ceases. |
| **4.3.3.2.7** | **Segregate duties to maintain appropriate checks and balances** | Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the IACS. |

### 4.3.3.3 Element: Physical and environmental security

**Objective:**

Create a secure environment for the protection of IACS assets. An asset is any physical or logical object owned by, or under the custodial duties of, an organization, having either a perceived or actual value to the organization (see IEC/TS 62443-1-1). IACS assets are those

assets that are a part of the IACS, either physical or cyber or that can affect the operation of the IACS. Physical security measures ensure that all assets, specifically those related to the IACS of an organization, are protected physically from unauthorized access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organization are protected against environmental conditions that would make them unusable or damage the information they contain.

**Description:**

Physical and environmental security measures should be designed to complement the cyber security measures taken to protect assets that are part of the IACS and coordinated with the physical security of the remainder of the plant. When developing a program for physical security of assets, it is important to include all systems in the scope and not just limit the effort to traditional computer room facilities. Practical engineering judgment should be used to balance the risks when determining physical security procedures. Physical segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level.

**Rationale:**

Physical assets are a means to an end as well as the end itself. In modern control systems the physical assets provide the means by which the cyber system operates. Therefore, the asset has value in itself but also has value as an integral part of the control system. Since both the asset and the control system require each other, both shall be protected in order for the system to be secure. The overriding security premise is that the use of security countermeasures should be commensurate with the level of risk. While physical segmentation is an important security countermeasure employed in conjunction with other layers of defense to reduce the risk that may be associated with IACS, it may not be necessary if the security risks are within accepted limits.

**Requirements:**

**Table 9 – Physical and environmental security: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.3.1** | **Establish complementary physical and cyber security policies** | Security policies and procedures that address both physical and cyber security in the protection of assets shall be established. |
| **4.3.3.3.2** | **Establish physical security perimeter(s)** | One or more physical security perimeters shall be established to provide barriers to unauthorized access to protected assets. |
| **4.3.3.3.3** | **Provide entry controls** | Appropriate entry controls shall be provided at each barrier or boundary. |
| **4.3.3.3.4** | **Protect assets against environmental damage** | Assets shall be protected against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion and impact. |
| **4.3.3.3.5** | **Require employees to follow security procedures** | Employees shall be required to follow and enforce the physical security procedures that have been established. |
| **4.3.3.3.6** | **Protect connections** | All connections under the control of the organization shall be adequately protected from tampering or damage. |
| **4.3.3.3.7** | **Maintain equipment assets** | All equipment assets, including auxiliary environmental equipment, shall be properly maintained to ensure proper operation. |
| **4.3.3.3.8** | **Establish procedures for monitoring and alarming** | Procedures shall be established for monitoring and alarming when physical or environmental security is compromised. |

| Description | | Requirement |
|---|---|---|
| **4.3.3.3.9** | **Establish procedures for the addition, removal, and disposal of assets** | Procedures should be established and audited with respect to the addition, removal and disposal of all assets. |
| **4.3.3.3.10** | **Establish procedures for the interim protection of critical assets** | Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster. |

### 4.3.3.4 Element: Network segmentation

**Objective:**

Group and separate key IACS devices into zones with common security levels in order to manage security risks and to achieve a desired target security level for each zone.

**Description:**

Network segmentation is a key security countermeasure designed to compartmentalize devices into security zones where identified security practices are employed to achieve the desired target security level. The zone may be an isolated standalone network segment or a network segment separated from the organization's network by some sort of network barrier device. IACS should be designed in a manner that filters/prevents nonessential communication packets from reaching the IACS devices.

For Transmission Control Protocol / Internet Protocol (TCP/IP) based networks, the most common barrier devices in use are firewalls, routers and layer 3 switches. For non-TCP/IP type networks, the barrier devices may be standalone gateways or integrated into the network interface module of an IACS device.

**Rationale:**

The overriding security premise is that the use of security countermeasures should be commensurate with the level of risk. While network segmentation is an important security countermeasure employed in conjunction with other layers of defense to reduce the risk that may be associated with IACS, it may not be necessary if the security risks are low.

**Requirements:**

**Table 10 – Network segmentation: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.4.1** | **Develop the network segmentation architecture** | A network segmentation countermeasure strategy employing security zones shall be developed for IACS devices based upon the risk level of the IACS. |
| **4.3.3.4.2** | **Employ isolation or segmentation on high-risk IACS** | High-risk IACS shall be isolated from or employ a barrier device to separate it from other zones with different security levels or risks. |
| **4.3.3.4.3** | **Block non-essential communications with barrier devices** | Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment. |

#### 4.3.3.5 Element: Access control – Account administration

**Objective:**

Ensure, on an ongoing basis, that only appropriate entities have accounts that allow access and that these accounts provide appropriate access privileges.

**Description:**

Access control is the method of controlling who or what entities can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

**Rationale:**

The misuse of data and systems may have serious consequences, including harm to human life, environmental damage, financial loss and damaged corporate reputation. These risks are increased when employees, contractors or temporary personnel have unnecessary access to data and systems.

**Requirements:**

**Table 11 – Access control – Account administration: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.5.1** | **Access accounts implement authorization security policy** | Access privileges implemented for access accounts shall be established in accordance with the organization's authorization security policy (see 4.3.3.7.1). |
| **4.3.3.5.2** | **Identify individuals** | As for all cyber security controls, the choice of access accounts for individuals versus access accounts for a crew shall be determined by considering threats, risks and vulnerabilities. In this case, considerations include HSE risks of individual controls, mitigation using complementary physical security controls, requirement for accountability and administrative/operational need. |
| **4.3.3.5.3** | **Authorize account access** | Access shall be granted, changed, or terminated on the authority of an appropriate manager. |
| **4.3.3.5.4** | **Record access accounts** | A record shall be maintained of all access accounts, including details of the individual(s) and devices authorized to use the account, their permissions and the authorizing manager. |
| **4.3.3.5.5** | **Suspend or remove unneeded accounts** | Access accounts shall be suspended or removed as soon as they are no longer needed (for example, job change). |
| **4.3.3.5.6** | **Review account permissions** | All established access accounts shall be reviewed regularly to ensure that the individual(s) and devices have only the minimum required permissions. |
| **4.3.3.5.7** | **Change default passwords** | Default passwords for access accounts shall be changed before the IACS is put into service. |
| **4.3.3.5.8** | **Audit account administration** | Periodic reviews of compliance to the account administration policy should be performed. |

#### 4.3.3.6 Element: Access control – Authentication

**Objective:**

Positively identify network users, hosts, applications, services and resources for computerized transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

**Description:**

Access control is the method of controlling who or what resources can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

There are several types of authentication strategies and each has varying degrees of strength. Strong authentication methods are ones that are quite accurate in positively identifying the user. Weak authentication methods are ones that can be easily defeated to provide unwanted access to information. Physical location of the user may have a significant impact on the risk of accessing the IACS.

**Rationale:**

Authentication requirements are more stringent for administration/configuration users and remote users, than for other users. This is because administration/configuration users have broader privileges and their actions have potentially more impact than other users; and remote users are typically not subject to complementary physical access controls. Automatic account lockout due to failed logins or periods of inactivity increases authentication strength, but is considered carefully in the IACS environment, since failure to authenticate a valid user could have HSE implications if the user is not able to perform tasks in a critical situation. In the IACS environment, there is a great emphasis on combining physical authentication measures with electronic authentication practices.

**Requirements:**

**Table 12 – Access control – Authentication: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.6.1** | **Develop an authentication strategy** | Companies shall have an authentication strategy or approach that defines the method(s) of authentication to be used. |
| **4.3.3.6.2** | **Authenticate all users before system use** | All users shall be authenticated before using the requested application, unless there are compensating combinations of entrance control technologies and administrative practices. |
| **4.3.3.6.3** | **Require strong authentication methods for system administration and application configuration** | Strong authentication practices (such as requiring strong passwords) shall be used on all system administrator access accounts and application configuration access accounts. |
| **4.3.3.6.4** | **Log and review all access attempts to critical systems** | Log files should record all access attempts to critical systems and should be reviewed for successful and failed access attempts. |
| **4.3.3.6.5** | **Authenticate all remote users at the appropriate level** | The organization shall employ an authentication scheme with an appropriate level of strength to positively identify a remote interactive user. |
| **4.3.3.6.6** | **Develop a policy for remote login and connections** | The organization shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity. |

| Description | | Requirement |
|---|---|---|
| **4.3.3.6.7** | **Disable access account after failed remote login attempts** | After some number of failed login attempts by a remote user, the system should disable the access account for a certain amount of time. |
| **4.3.3.6.8** | **Require re-authentication after remote system inactivity** | After a defined period of inactivity, a remote user should be required to re-authenticate before the remote user can re-access the system. |
| **4.3.3.6.9** | **Employ authentication for task-to-task communication** | Systems should employ appropriate authentication schemes for task-to-task communication between applications and devices. |

### 4.3.3.7 Element: Access control – Authorization

**Objective:**

Grant access privileges to resources upon successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

**Description:**

Access control is the method of controlling who or what resources can access premises and systems and what type of access is permitted. There are three key aspects associated with access control: account administration, authentication and authorization. All three aspects shall work together to establish a sound and secure access control strategy.

Authorization explores the controls aimed at protecting information and assets from deliberate and inadvertent destruction, change or disclosure. It focuses specifically on measures designed to ensure that the authenticated agents have access to required information assets. As with authentication, authorization is dependent upon the location of the user.

**Rationale:**

It is important in the IACS environment to make sure that the right people have access to the correct information and systems and are not prevented from doing their job due to lack of authorization. Authorization to perform specific job functions is provided by the application. There is a need to consider safety implications when developing the authorization strategy.

**Requirements:**

**Table 13 – Access control – Authorization: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.3.7.1** | **Define an authorization security policy** | Rules that define the privileges authorized under access accounts for personnel in various job roles shall be defined in an authorization security policy that is clearly documented and applied to all personnel upon authentication. |
| **4.3.3.7.2** | **Establish appropriate logical and physical permission methods to access IACS devices** | The permission to access IACS devices shall be logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras, and other controls that restrict access to an active computer console), or both. |
| **4.3.3.7.3** | **Control access to information or systems via role-based access accounts** | Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications shall be considered when defining roles. |

| Description | | Requirement |
|---|---|---|
| **4.3.3.7.4** | **Employ multiple authorization methods for critical IACS** | In critical control environments, multiple authorization methods should be employed to limit access to the IACS. |

### 4.3.4 Element group: Implementation

#### 4.3.4.1 Description of element group

The third element group in this category is Implementation. This element within this group discusses issues related to implementing the CSMS. Figure 5 shows a graphical representation of the four elements in the element group:

- Risk management and implementation,
- System development and maintenance,
- Information and document management and
- Incident planning and response.

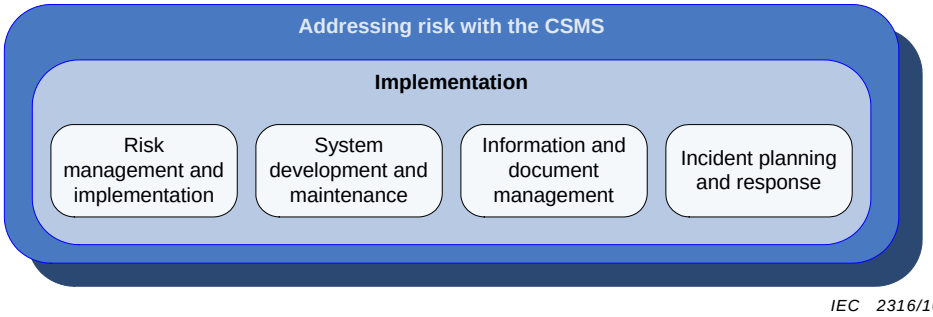



**Figure 5 – Graphical view of element group: Implementation**

#### 4.3.4.2 Element: Risk management and implementation

**Objective:**

Reduce risk to and maintain risk at an acceptable level in the IACS based upon the organization's tolerance for risk.

**Description:**

Risk management and implementation addresses the selection, development and implementation of countermeasures that are commensurate with risks. The countermeasures may take into account the use of products with strong inherent security capabilities, manual and procedural security controls and technology based controls to prevent or reduce security incidents.

**Rationale:**

The risk management and implementation element is used to turn the results from the risk identification classification and assessment element of this standard into effective and concrete actions. Although it can never be eliminated totally, risk can be managed in a manner that balances the cost of risk avoidance against the potential cost of the incident.

**Requirements:**

**Table 14 – Risk management and implementation: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.4.2.1** | **Manage IACS risk on an ongoing basis** | The organization shall adopt a risk management framework that includes selection and implementation of IACS devices and countermeasures to manage risk to an acceptable level over the life of the facility. |
| **4.3.4.2.2** | **Employ a common set of countermeasures** | A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organization wherever a specific risk is identified. |

### 4.3.4.3 Element: System development and maintenance

**Objective:**

Ensure that the organization's desired risk tolerance level is maintained as its IACS assets evolve through the maintenance of existing systems as well as development and procurement of new systems.

**Description:**

This element addresses designing cyber security into systems from the earliest development stages. It also involves the maintenance of those cyber security policies and procedures as the system changes throughout its lifecycle.

**Rationale:**

Organizations have found that maintenance of the CSMS is more challenging than establishing it. For this reason, procedures that proactively address cyber security as part of the natural evolution of the IACS systems are critical.

**Requirements:**

**Table 15 – System development and maintenance: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.4.3.1** | **Define and test security functions and capabilities** | The security functions and capabilities of each new component of the IACS shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile. |
| **4.3.4.3.2** | **Develop and implement a change management system** | A change management system for the IACS environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest. |
| **4.3.4.3.3** | **Assess all the risks of changing the IACS** | Using clearly defined criteria, proposed changes to IACS shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals technically knowledgeable about the industrial operation and the IACS system. |
| **4.3.4.3.4** | **Require security policies for system development or maintenance changes** | The security requirements of a new system being installed in the IACS environment in an existing zone shall meet the security policies and procedures required for that zone/environment. Similarly, maintenance upgrades or changes shall meet the security requirements for the zone. |

| Description | | Requirement |
|---|---|---|
| **4.3.4.3.5** | **Integrate cyber security and process safety management (PSM) change management procedures** | Cyber security change management procedures should be integrated with existing PSM procedures. |
| **4.3.4.3.6** | **Review and maintain policies and procedures** | The operations and change management policies and procedures shall be reviewed and kept current to ensure that security changes do not increase risks to safety or business continuity. |
| **4.3.4.3.7** | **Establish and document a patch management procedure** | A procedure for patch management shall be established, documented, and followed. |
| **4.3.4.3.8** | **Establish and document antivirus/malware management procedure** | A procedure for antivirus/malware management shall be established, documented, and followed. |
| **4.3.4.3.9** | **Establish backup and restoration procedure** | A procedure for backing up and restoring computer systems and protecting backup copies shall be established, used, and verified by appropriate testing. |

### 4.3.4.4 Element: Information and document management

**Objective:**

Classify, manage, safeguard and present the information associated with the IACS and CSMS at the appropriate time to authorized personnel.

**Description:**

Organizations should employ comprehensive information and document management policies for information assets within the scope of their IACS and CSMS. Care should be given to protect this information and verify that the appropriate versions are retained. Information classification systems that allow information assets to receive the appropriate level of protection are the key to meeting this objective.

**Rationale:**

Much of the information about the IACS may be stored electronically or in hardcopy outside the IACS and is not protected by IACS authorization controls. Unauthorized access and use of this information is a threat to IACS security. This information needs to be appropriately controlled and managed.

**Requirements:**

**Table 16 – Information and document management: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.4.4.1** | **Develop lifecycle management processes for IACS information** | A lifecycle document management process shall be developed and maintained for IACS information. |
| **4.3.4.4.2** | **Define information classification levels** | Information classification levels (for example, company confidential, restricted and public) shall be defined for access and control, including sharing, copying, transmitting, and distributing appropriate for the level of protection required. |

| Description | | Requirement |
|---|---|---|
| **4.3.4.4.3** | **Classify all CSMS information assets** | All logical assets within the scope of the CSMS (that is, control system design information, vulnerability assessments, network diagrams and industrial operations programs) shall be classified to indicate the protection required commensurate with the consequence of its unauthorized disclosure or modification. |
| **4.3.4.4.4** | **Ensure appropriate records control** | Policies and procedures should be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements. |
| **4.3.4.4.5** | **Ensure long-term records retrieval** | Appropriate measures should be employed to ensure long-term records can be retrieved (that is, converting the data to a newer format or retaining older equipment that can read the data). |
| **4.3.4.4.6** | **Maintain information classifications** | Information that requires special control or handling should be reviewed on a periodic basis to validate that special handling is still required. |
| **4.3.4.4.7** | **Audit the information and document management process** | Periodic reviews of compliance to the information and document management policy should be performed. |

### 4.3.4.5 Element: Incident planning and response

**Objective:**

Predefine how the organization will detect and react to cyber security incidents.

**Description:**

When developing a program for incident planning and response, it is important to include all systems in scope and not just limit the effort to traditional computer room facilities. Part of the incident response plan should include procedures for how the organization will respond to incidents, including notification and documentation methods, investigations, recoveries and subsequent follow-up practices.

**Rationale:**

Identifying an incident early and responding appropriately can limit the consequences of the event. Incident planning and response provides the organization the opportunity to plan for security incidents and then to respond according to the established company practices. No matter how much care is taken in protecting a system, it is always possible that unwanted intrusions might compromise the system. Technology vulnerabilities continue to exist and external threats are increasing in number and sophistication, therefore requiring a robust strategy for determining the appropriate planning and response. Insight gained from actual incidents is captured because it is critical for evaluating and improving the CSMS.

**Requirements:**

**Table 17 – Incident planning and response: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.3.4.5.1** | **Implement an incident response plan** | The organization shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals. |

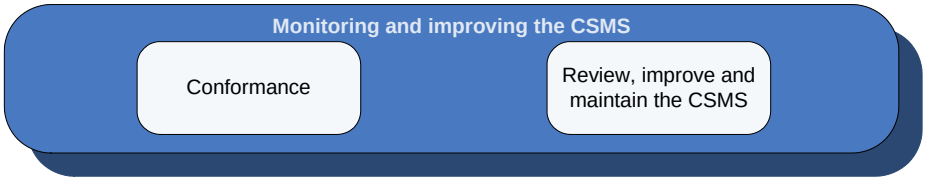
| Description | | Requirement |
|---|---|---|
| **4.3.4.5.2** | **Communicate the incident response plan** | The incident response plan shall be communicated to all appropriate organizations. |
| **4.3.4.5.3** | **Establish a reporting procedure for unusual activities and events** | The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents. |
| **4.3.4.5.4** | **Educate employees on reporting cyber security incidents** | Employees should be educated on their responsibility to report cyber security incidents and the methods of reporting these incidents. |
| **4.3.4.5.5** | **Report cyber security incidents in a timely manner** | The organization should report cyber security incidents in a timely manner. |
| **4.3.4.5.6** | **Identify and respond to incidents** | If an incident is identified, the organization shall promptly respond in accordance with the established procedures. |
| **4.3.4.5.7** | **Identify failed and successful cyber security breaches** | The organization should have procedures in place to identify failed and successful cyber security breaches. |
| **4.3.4.5.8** | **Document the details of incidents** | The details of an identified incident shall be documented to record the incident, the response, the lessons learned, and any actions taken to modify the CSMS in light of this incident. |
| **4.3.4.5.9** | **Communicate the incident details** | The documented details of an incident shall be communicated to all appropriate organizations (that is, management, IT, process safety, automation and control engineering security and manufacturing) in a timely manner. |
| **4.3.4.5.10** | **Address and correct issues discovered** | The organization shall have a business methodology in place to address issues discovered and ensure they are corrected. |
| **4.3.4.5.11** | **Conduct drills** | Drills should be conducted to test the incident response program on a routine basis. |

## 4.4 Category: Monitoring and improving the CSMS

### 4.4.1 Description of category

The third main category of the CSMS is titled Monitoring and Improving the CSMS. It involves both ensuring that the CSMS is being used and also reviewing the CSMS itself for effectiveness. Figure 6 shows a graphical representation of the two elements in the category:

- Conformance and
- Review, improve and maintain the CSMS.




IEC 2317/10

**Figure 6 – Graphical view of category: Monitoring and improving the CSMS**

### 4.4.2 Element: Conformance

**Objective:**

Ensure that the CSMS developed for an organization is followed.

**Description:**

Conformance with a CSMS means the organization is adhering to its stated policies, executing the procedures at the correct time and producing the appropriate reports to allow for future review.

**Rationale:**

Irrespective of the quality of a CSMS, if it is not used, then it does not add any value to the organization and does not help reduce risk.

**Requirements:**

**Table 18 – Conformance: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.4.2.1** | **Specify the methodology of the audit process** | The audit program shall specify the methodology of the audit process. |
| **4.4.2.2** | **Conduct periodic IACS audits** | Validate that the IACS conforms to the CSMS. The CSMS shall include periodic audits of the IACS, to validate that the security policies and procedures are performing as intended and meet the security objectives for the zone. |
| **4.4.2.3** | **Establish conformance metrics** | The organization should define performance indicators and success criteria, which are used to monitor conformance to the CSMS. The results from each periodic audit should be expressed in the form of performance against these metrics to display security performance and security trends. |
| **4.4.2.4** | **Establish a document audit trail** | A list of documents and reports required to establish an audit trail shall be developed. |
| **4.4.2.5** | **Define punitive measures for non-conformance** | The organization shall state what non-conformance with the CSMS means, and any related punitive measures shall also be defined. |
| **4.4.2.6** | **Ensure auditors' competence** | The required competency for auditing the specific systems that are in scope should be specified. The level of independence required should be determined as part of the governance. |

### 4.4.3 Element: Review, improve and maintain the CSMS

**Objective:**

Ensure that the CSMS continues to meet its goals over time.

**Description:**

Reviewing, improving and maintaining the CSMS establishes a continuing oversight of the CSMS to check that it functions effectively and to manage required changes to the CSMS over time.

**Rationale:**

Review and monitoring are required for the CSMS to remain effective, since the CSMS shall respond to changes in internal and external threats, vulnerabilities and consequences, as well as changes in risk tolerance, legal requirements and evolving technical and non-technical approaches to risk mitigation.

**Requirements:**

**Table 19 – Review, improve and maintain the CSMS: Requirements**

| Description | | Requirement |
|---|---|---|
| **4.4.3.1** | **Assign an organization to manage and implement changes to the CSMS** | An organization shall be assigned to manage and coordinate the refinement and implementation of the CSMS changes and use a defined method in making and implementing changes. |
| **4.4.3.2** | **Evaluate the CSMS periodically** | The managing organization shall periodically evaluate the overall CSMS to ensure the security objectives are being met. |
| **4.4.3.3** | **Establish triggers to evaluate CSMS** | The organization should establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS and perhaps a change. These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk and major changes to the IACS. The thresholds should be based on the organization's risk tolerance. |
| **4.4.3.4** | **Identify and implement corrective and preventive actions** | The organization shall identify and implement appropriate corrective and preventive actions that modify the CSMS to meet security objectives. |
| **4.4.3.5** | **Review risk tolerance** | A review of the organization's tolerance for risk should be initiated when there are major changes to the organization, technology, business objectives, internal business and external events including identified threats and changes in social climate. |
| **4.4.3.6** | **Monitor and evaluate industry CSMS strategies** | Management system owners should monitor the industry for CSMS best practices for risk assessment and risk mitigation and evaluate their applicability. |
| **4.4.3.7** | **Monitor and evaluate applicable legislation relevant to cyber security** | The organization shall identify applicable and changing legislation relevant to cyber security. |
| **4.4.3.8** | **Request and report employee feedback on security suggestions** | Employee feedback on security suggestions should be actively sought and reported back to senior management as appropriate on performance shortcomings and opportunities. |

# Annex A
(informative)

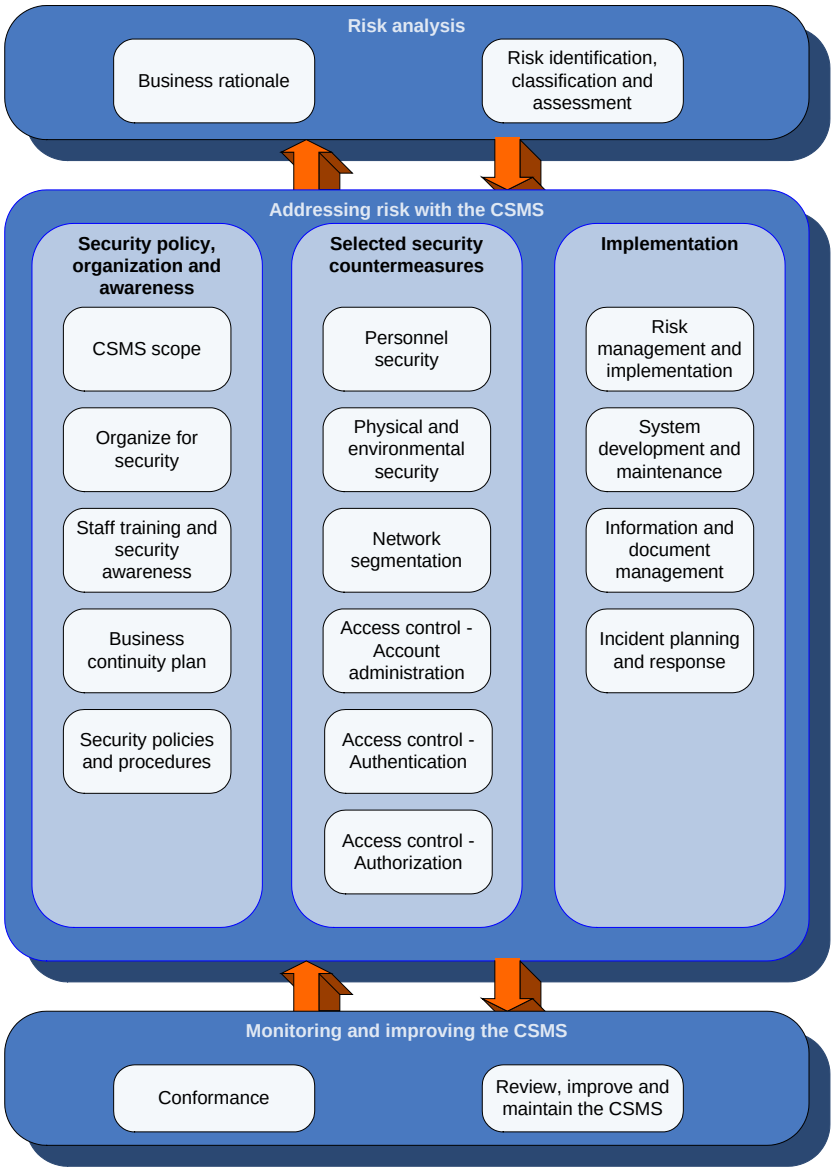
# Guidance for developing the elements of a CSMS

## A.1 Overview

This annex provides informative guidance to the reader on how to develop a CSMS that meets the requirements specified in Clause 4. The guidance presented here provides an overall management system framework that allows organizations adopting the CSMS to tailor it to their own specific needs. It should be thought of as a starting point or baseline for a CSMS. Not all guidance may be applicable and depending on the application, the organization may require more security than what is presented. It is also not meant to be a step-by-step process, as was previously stated in 4.1.

This annex is organized with the same categories, element groups, and elements as those listed in Clause 4 (see Figure A.1). Each element in this annex uses the following organization:

- Description of element – a basic description of the topic;
- Element-specific information – one or more subclauses providing detailed guidance regarding this element. Their structure and content is element-specific;
- Supporting practices:
  - Baseline practices – recommendations for organizations to achieve a baseline level of cyber security. These practices become the building blocks of the requirements for each element.
  - Additional practices – innovative security practices used by some organizations to further enhance cyber security;
- Resources used – sources for additional information as well as documents referenced (in addition to the current document).




IEC 2318/10

**Figure A.1 – Graphical view of elements of a cyber security management system**

## A.2 Category: Risk analysis

### A.2.1 Description of category

The first main category of the CSMS is risk analysis. This category discusses much of the background information that feeds into many of the other elements in the CSMS. Figure A.2 shows the two elements that are part of the category:

- Business rationale and
- Risk identification, classification and assessment.


IEC 2319/10

**Figure A.2 – Graphical view of category: Risk analysis**

### A.2.2 Element: Business rationale

#### A.2.2.1 Description of element

This element establishes that the organization is aware of and understands the importance of cyber security for information technology as used in IACS. This understanding is based upon an understanding of the roles that information technology plays in the mission of the organization, associated risks to this mission and the cost and other business impacts of mitigating this risk.

#### A.2.2.2 Cyber security risk, business rationale and business case

The first step to implementing a cyber security program for IACS is to develop a compelling business rationale for the unique needs of the organization to address cyber risk. An organization may derive the rationale for its IACS CSMS and related individual projects from existing policies related to safety, general risk management or compliance with regulatory requirements. Other organizations may require that the business rationale take the form of a formal or informal business case for cyber security management activities in order to establish that the cost of mitigating cyber risk is justified by its financial benefit. A business rationale or business case for taking the first steps to build a CSMS will depend upon an assessment of risk, generally at a high level. Once risk is acknowledged, an organization is ready to take appropriate steps to mitigate it. An effort to perform more systematic and detailed risk assessment (as described later in this standard) and individual decisions about countermeasures, may themselves require a business rationale, possibly in the form of a business case.

A business rationale captures the business concerns of senior management while being founded in the experience of those already dealing with many of the same risks. This subclause deals with the key components of the resulting business rationale and key resources to help identify those components. A business rationale may have as its scope the justification of a high-level or detailed risk assessment, other specific aspects of a full CSMS as described herein, or implementation of a single countermeasure.

Experience has shown that embarking on a cyber security program without an agreed business rationale often results in eventual loss of program resources in favor of other business requirements. Typically these other business requirements have a more direct business benefit and easily understood rationale.

#### A.2.2.3 Key components of business rationale

There are four key components of a business rationale: prioritized business consequences, prioritized threats, estimated annual business impact and cost of countermeasures.

a) Prioritized business consequences

   The list of potential business consequences needs to be distilled to the particular business consequences that senior management will find the most compelling. For instance, a food and beverage company that handles no toxic or flammable materials and typically processes its product at relatively low temperatures and pressures might not be concerned about equipment damage or environmental impact but might be more concerned about loss of production availability and degradation of product quality. The insight here is based on histories of past incidents as well as knowledge of how IACS are actually used in the business and the potential business impact that unauthorized technical changes could cause. Regulatory compliance might also be a concern.

b) Prioritized threats

   The list of potential threats needs to be refined, if possible, to those threats that are deemed credible. For instance, a food and beverage company might not find terrorism a credible threat but might be more concerned with viruses and worms and disgruntled employees. The insight here is primarily based on histories of past incidents.

c) Estimated annual business impact

The highest priority items shown in the list of prioritized business consequences should be scrutinized to obtain an estimate of the annual business impact preferably, but not necessarily, in financial terms. For the food and beverage company example, it may have experienced a virus incident within its internal network that the information security organization estimated as resulting in a specific financial cost. Because the internal network and the controls network are interconnected, it is conceivable that a virus originating from the controls network could cause the same amount of business impact. The insight here is primarily based on histories of past incidents. Regulatory compliance may entail specific financial or business penalties for non-compliance.

d) Cost

The estimated cost of the human effort and technical countermeasures that this business rationale intends to justify.

NOTE A business impact estimate in financial terms and cost estimates for countermeasures are required to create a business case, but a successful business rationale may not always include this information.

There are a number of resources for information to help form this business rationale: external resources in trade organizations and internal resources in related risk management programs or engineering and operations.

External resources in trade organizations often provide useful tips about factors that most strongly influenced their management to support their efforts and what resources within their organizations proved most helpful. For different industries, these factors may be different but there may be similarities in the roles that other risk management specialists can play.

Internal resources associated with related risk management efforts (that is, information security, HSE risk, physical security, and business continuity) can provide tremendous assistance based on their experience with related incidents in the organization. This information is helpful from the standpoint of prioritizing threats and estimating business impact. These resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might prove the most appropriate or receptive to serving as a champion.

Internal resources associated with control systems engineering and operations can provide insight into the details of how control systems are actually used within the organization. How are networks typically segregated? How are high-risk combustion systems or safety instrumented systems (SIS) typically designed? What security countermeasures are already commonly used? Keeping in mind the organization's history with mergers and acquisitions, it is also important to understand how representative any particular site might be of the entire business unit, region or overall organization.

Remember that in the early stages of the industrial operation, the primary focus will be on identifying one or two high-priority issues that justify continued effort. As the IACS cyber security program develops further, other items may appear on the list and priorities may shift, as the organization applies a more rigorous risk analysis methodology. However, these changes should not detract from the result of this original effort to justify initiating the program.

#### A.2.2.4 Content suggestions for IACS business rationale

Within each organization, the journey to develop an effective cyber security program for IACS starts with individuals who recognize the risks the organization is taking and begin to articulate these risks internally, not just in technical terms, but in business terms that resonate with upper management. A business rationale is not a detailed risk assessment; it is rather a high-level description of risks sufficient to justify the next planned steps in building a CSMS. It may be as brief or detailed as required to support the decision processes in the particular organization.

The negative business consequences of cyber attacks against IACS can include the following:

- reduction or loss of production at one site or multiple sites simultaneously;
- injury or death of employees;
- injury or death of persons in the community;
- damage to equipment;
- environmental damage;
- violation of regulatory requirements;
- product contamination;
- criminal or civil legal liabilities;
- loss of proprietary or confidential information;
- loss of brand image or customer confidence;
- economic loss.

In prioritizing the risk of these consequences occurring, it is also important to consider the potential source or threat that initiates a cyber attack and the likelihood that such an event would occur. Cyber threats could arise from sources inside or outside an organization; threats could be the result of either intentional or unintentional actions; and threats could either be directed at a specific target or undirected. Cyber security incidents can result from many different types of threat agents such as the following:

- Thrill-seeking, hobbyist, or alienated individuals who gain a sense of power, control, self-importance and pleasure through successful penetration of computer systems either via undirected attacks (viruses and worms) or directed attacks (hacking) to steal or destroy information or disrupt an organization's activities.
- Disgruntled employees or contractors who damage systems or steal information for revenge or profit.
- Well-intentioned employees who inadvertently make changes to the wrong controller or operating equipment.
- Employees who break quality, safety or security policies or procedures to meet other urgent needs (for example, production goals).
- Terrorists typically motivated by political beliefs for which cyber attacks offer the potential for low-cost, low-risk, but high-gain attacks especially when linked with coordinated physical attacks.
- Professional thieves (including organized crime) who steal information for sale.
- Adversary nations or groups who use the Internet as a military weapon for cyber warfare to disrupt the command, control and communication capabilities of a foe.

Documented cases provide insight into how and how often one of these threat agents succeeds in inflicting negative business consequences. The rapid adoption of new network technologies has led to the development of new tools to enable cyber attacks. With the lack of a recognized publicly accessible incident reporting system, it will be extremely difficult in the near future to determine a quantitative likelihood of any specific type of event occurring. Likelihood will need to be evaluated qualitatively based on an organization's own internal incident history and on the few cases that have been publicly documented. Several examples of these cases are:

EXAMPLE 1 In January, 2003, the SQL Slammer Worm rapidly spread from one computer to another across the Internet and within private networks. It penetrated a computer network at Ohio's Davis-Besse nuclear power plant and disabled a monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. It occurred due to an unprotected interconnection between plant and corporate networks. The SQL Slammer Worm downed one utility's critical SCADA network after moving from a corporate network to the control center local area network (LAN). Another utility lost its Frame Relay Network used for communications and some petrochemical plants lost human-machine interfaces (HMIs) and data historians. A 911 call center was taken offline, airline flights were delayed and canceled and bank ATMs were disabled.

EXAMPLE 2 Over several months in 2001, a series of cyber attacks were conducted on a computerized waste water treatment system by a disgruntled contractor in Queensland, Australia. One of these attacks caused the

diversion of millions of gallons of raw sewage into a local river and park. There were 46 intrusions before the perpetrator was arrested.

EXAMPLE 3 In September, 2001, a teenager allegedly hacked into a computer server at the Port of Houston to target a female chat room user following an argument. It was claimed that the teenager intended to take the woman's computer offline by bombarding it with a huge amount of useless data and he needed to use a number of other servers to be able to do so. The attack bombarded scheduling computer systems at the world's eighth largest port with thousands of electronic messages. The port's web service, which contained crucial data for shipping pilots, mooring companies and support firms responsible for helping ships navigate in and out of the harbor, was left inaccessible.

The CERT organization has been monitoring and tracking the number of attacks occurring on Internet-connected systems since 1988. None of the reported incidents were for control systems. As of 2004, they have stopped tracking the number of attacks, because the prevalence of automated attack tools has led to attacks becoming so commonplace that the number of incidents reported provides little information with regard to assessing the scope and impact of attacks. A graph of their incident data is shown in Figure A.3 to demonstrate the dramatic increase that has occurred over the last 15 years.

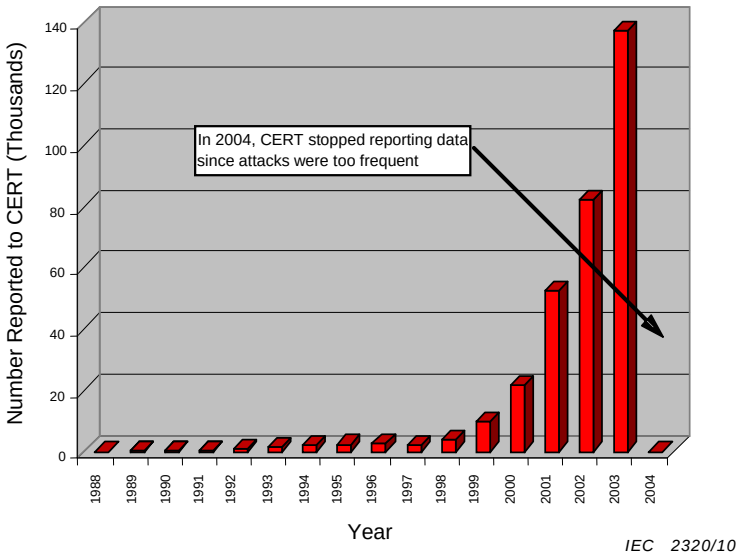



**Figure A.3 – Reported attacks on computer systems through 2004 (source: CERT)**

### A.2.2.5 Supporting practices

#### A.2.2.5.1 Baseline practices

The following six actions are baseline practices:

a) Identifying and documenting the business objectives, critical business processes and critical information technology processes. Include IACS and interfaces with value chain partners where sensitive information is transferred, stored, or processed.

b) Identifying the dependence of the business on information technology systems. Categorize the business dependence low, medium, high, or an alternate ranking system.

c) Identifying various damage scenarios by the loss of confidentiality, integrity or availability of information. Include the manipulation of IACS and the consequences of such actions for those businesses, which use these systems. Include HSE and operational integrity and reliability for drivers of IACS. Capture risks associated with value chain and other third-party business partners. These risks often include the loss or alteration of sensitive information. An example is the interception of information associated with manufacturing products shipments, including types of materials, quantities, shipping routes, mode of transportation, and the like.

d) Developing business impact analyses for IACS security.

e) Developing business impact analyses for value chain or other third-party business partner.

f) Determining the organization's risk tolerance profile defined in terms of:
   1) Safety of personnel (serious injury or fatality);
   2) Financial loss or impact including regulatory penalties;
   3) Environmental/regulatory consequence;
   4) Damage to company image;
   5) Impact to investment community;
   6) Loss of customer base or confidence;
   7) Impact on infrastructure.

NOTE Risk tolerance varies depending on the business. Simply put, the organization's risk tolerance is its threshold of pain. The risk tolerance may be very low (for example, a single serious injury may not be acceptable and must be addressed immediately) when it comes to safety in plant manufacturing or may be very high (for example, in terms of production loss) if the organization has multiple production sites of a commodity product. The financial impact for one business may not be appropriate for other businesses. Organizations with multiple businesses should look at the interdependencies of one business upon another when determining risk tolerance.

IT security managers typically will be familiar with the organization's risk tolerance profile for some, but not all of these consequences. Other managers who are responsible for managing the risks associated with HSE consequences will be familiar with the organization's risk tolerance profile in these areas. The overall risk tolerance profile needs to be determined by integrating information from these sources as well as those from the IACS environment.

#### A.2.2.5.2 Additional practices

The following three actions are additional practices:

a) Identifying and documenting the business objectives, critical business processes, and critical IT processes. This process is best performed with a cross-section of the organization representing the functional areas, as well as the business units of the company. This group typically is chartered either by a senior executive who is responsible for the IT organization, or by a leadership team that includes other senior executives from throughout the organization. This charter specifically includes the risk associated with IACS.

b) Developing a business impact analysis that describes the issues and consequences of inaction and benefits of action. Where practical, these actions are quantified in terms of financial impacts (that is, lost sales or fines), market impacts (that is, loss of confidence or public image), as well as HSE impacts (that is, environmental release, equipment damage and loss of life). Especially when considering consequences like public image, it is important to understand that an incident due to one particular business unit can affect the organization as a whole.

c) Documenting and approving (by the appropriate level of management) the risks outside the scope of the CSMS.

### A.2.2.6 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [24], [26], [27], [30], [42].

## A.2.3 Element: Risk identification, classification and assessment

### A.2.3.1 Description of element

Organizations protect their ability to perform their mission by systematically identifying, prioritizing and analyzing potential security threats, vulnerabilities, and consequences using accepted methodologies. Risk is formally defined as an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence (see IEC/TS 62443-1-1). As described under the related element Risk Management and Implementation (see A.3.4.2), an organization defines its risk tolerance in terms of the characteristics of threats, vulnerabilities and potential consequences it identifies.

The organization then implements this risk tolerance decision by taking action where indicated to reduce the likelihood of a security threat occurring by mitigating vulnerabilities and/or reducing the consequences in case the security threat is realized.

#### A.2.3.2 Cyber risk for IACS

The risk management approach outlined in A.2.2 applies in general for all types of cyber risks as well as other types of risks. This discussion is about the unique aspects of the analysis of cyber risk for IACS.

Although various industries may find certain types of business impact of more concern and may feel that certain types of threats are more likely, all industries that use IACS should be concerned that they are entering a new risk environment. At the same time that IACS have adopted commercial IT operating systems and network technologies and users have interconnected their private networks with their IACS networks, the number of threats has also increased greatly. There are risks associated with traditional information (electronic or paper), classical IT systems and applications, IACS, business partners, joint ventures, outsourcing partners, and the like.

Risks for traditional IT assets focus on the confidentiality, integrity, and availability of information. Risks in IACS are different as the drivers focus more on HSE factors and operational reliability in addition to the traditional protection of information confidentiality, integrity and availability. In IACS the priorities are generally reversed with focus on availability, integrity and confidentiality in that order. This means that cyber risk assessment for IACS should be coordinated with physical security and HSE, wherever practical. Some organizations fully integrate risk assessment efforts related to all of these areas. Risks using outsourcing, third-party contractors or other partners in the manufacturing value chain include sensitive information transmitted, stored or processed. The integration of these business partners into an organization’s operations potentially permits unintentional access into the company’s systems.

In virtually all of these cases, the security-related industrial operations and technologies developed for classical IT applications have not been deployed for IACS partly due to ignorance, but partly due to valid constraints that do not exist in classical IT applications. The objective of this standard is to address both issues.

#### A.2.3.3 Risk assessment process

##### A.2.3.3.1 General

An overview of risks is required to establish the business rationale for a CSMS. The more detailed priorities addressed by this system are determined based upon a methodology that systematically considers risk at a greater level of granularity than typically assessed to establish an initial business rationale.

##### A.2.3.3.2 Risk assessment and vulnerability assessment

In the general literature, the terms vulnerability assessment and risk assessment are sometimes used interchangeably. These two kinds of analyses can be distinguished in accordance with the definitions of vulnerability and risk in this standard. Recall that a vulnerability is defined as a flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's integrity or security policy (see IEC/TS 62443-1-1). As an example, the observation that passwords in a control center are seldom changed is an example of a vulnerability that would be identified in a vulnerability assessment. There may be several risks associated with this vulnerability, for example:

- A low likelihood that the password becomes well known in the plant over time and that a legitimate employee not trained for control system operations uses the password while

pitching in to solve a problem and causes a loss of production for several hours due to input errors.

- A low likelihood that a disgruntled former employee successfully breaks through corporate firewall defences to access the control system network remotely, logs in to an HMI and deliberately takes actions that can cause a loss of production for several days.

Thus as these terms are used in this standard, risk assessment has as its output a set of risks and a vulnerability assessment has as its output a set of vulnerabilities, which have not yet been analyzed in terms of the risks they create. In this way, a vulnerability assessment is an input to a risk assessment. Note that some existing methodologies titled vulnerability assessment methods include risk concepts and others do not.

Returning to the above example of the control room password, it is clear that there are also risks involved in changing the control system password periodically, for example, a low likelihood that an operator may not remember a new password in an emergency situation and will be unable to login to resolve the situation, resulting in serious collateral environmental damage. The tradeoff between the risk addressed by a countermeasure and the risk introduced by a countermeasure such as in this case, is discussed under the Risk Management and Implementation element of this standard (see A.3.4.2).

#### A.2.3.3.3 High-level and detailed risk assessment

Risk assessment can be carried out at several levels. This standard requires risk assessment at two levels of detail, called high-level risk assessment and detailed risk assessment.

High-level risk assessment examines what might be the impact of general types of cyber security vulnerabilities and the likelihood that a threat might exercise these vulnerabilities, but does not consider particular instances of these vulnerabilities or related countermeasures already in place. Thus examples of risks identified in a high-level risk assessment might be:

- A medium likelihood that a malware infestation occurs and causes control network congestion and thus a lack of visibility to the status of the industrial process in the control room, resulting in potential emergency shutdown and resulting costs.
- A low likelihood that a contractor with criminal connections and with physical access to the control system network media taps this media and successfully modifies control commands in a way that causes damage to the facility.

High-level assessment is required because experience has shown that if organizations start out by looking at detailed vulnerabilities, they miss the big picture of cyber risk and find it difficult to determine where to focus their cyber security efforts. Examination of risks at a high level can help to focus effort in detailed vulnerability assessments. The high-level assessment can typically cover all control networks owned by an organization, possibly by dividing them into groups that share common characteristics. Resources may not be available to cover all IACS at the detailed level.

A detailed risk assessment, as defined for this standard, is supported by a detailed vulnerability assessment that includes examining details such as existing technical countermeasures, adherence to account management procedures, patch and open port status by individual host on a specific control system network and network connectivity characteristics such as firewall separation and configuration. Thus an example output from a detailed risk assessment might be:

- Direct connection of process engineering workstations to both the corporate network and the control system network in the South facility, bypassing the control network internal firewall, contribute to risk of malware infection on the control network. In combination with lack of antivirus protection on 50 % of the hosts on the South facility control network, this results in a medium likelihood of a virus-triggered network congestion incident causing a lack of visibility to the status of the industrial operation in the control room and resulting in potential emergency shutdown and resulting costs.

- All control system network media (for example, addresses 192.168.3.x) and connections to other networks are either physically protected by walls, ceilings or floors, or in locked rooms accessible to three authorized control system network administrators. Therefore the risk of a successful attempt at tapping this media is low.

These detailed risk assessment results support related results from a high-level assessment according to the related examples above. However, the detailed risk assessment may in many cases determine that risks are lower or higher than suspected in the high-level assessment. The detailed risk assessment may also uncover risks not considered in the high-level assessment. Finally, since the detailed assessment identifies specific vulnerabilities, it provides direction for how an organization might address risks deemed unacceptable.

#### A.2.3.3.4 Types of risk assessment methodologies

##### A.2.3.3.4.1 General

There are a variety of risk assessment methods that have been developed and marketed by different organizations. In general, these can be classified according to two factors: how they characterize the individual risks (qualitatively versus quantitatively) and how they structure the risk identification exercise (scenario-based versus asset-based).

##### A.2.3.3.4.2 Qualitative versus quantitative

Qualitative risk assessment typically relies on the input of experienced employees and/or experts to provide information regarding likelihood and severity of specific threats impacting specific assets. In addition, different levels of likelihood and severity are identified by general classes such as high, medium and low rather than specific probabilities or economic impacts. Qualitative risk assessment is preferred when there is a lack of reliable information regarding the likelihood of specific threats affecting specific assets or estimating the overall impact of damage to specific assets.

Quantitative risk assessment typically relies on extensive data sets that document the rate at which damage occurs to assets based on exposure to defined combinations of threats and vulnerabilities. If this information is available, it can provide more precise risk estimates than qualitative risk assessment methods. Due to the recent exposure of IACS to cyber security threats, the relative infrequency at which incidents occur and the rapidly evolving nature of the threats, extensive data sets do not yet exist to aid in the assessment of cyber security threats to IACS. At this stage, qualitative risk assessment is the preferred method for evaluating these risks.

##### A.2.3.3.4.3 Scenario-based versus asset-based

In conducting a risk assessment, it is usually helpful to focus the participant's thoughts along one of two lines: the scenarios by which threats take advantage of vulnerabilities to impact assets or the assets themselves. The scenario-based approach tends to take advantage of experience with actual incidents or near-incidents. However, the approach may not penetrate to discover threats or vulnerabilities to sensitive assets that have not been previously threatened. The asset-based approach tends to take advantage of knowledge of an organization's systems and work methods and particular assets whose compromise would lead to high economic impact. However, this approach may not penetrate to discover types of threats or vulnerabilities that would place these assets in jeopardy or scenarios that involve more than one asset. Whichever general approach is used, it is recommended that some aspect of the other approach be included to provide a more thorough risk assessment.

EXAMPLE An organization that has identified assets as devices, applications and data is considered as an example that integrates scenario and asset-based methods. In the next step, the organization lists possible scenarios related to these assets and determines consequences as follows. Application scenarios are very similar to the device scenarios shown.

a) Device scenarios

   1) Scenario: Unauthorized user locally accessing an IACS device

What is the consequence of someone walking up to the device and performing the tasks allowed at this device?

2) Scenario: Remote access of an IACS device by an unauthorized user

What is the consequence of an unauthorized user gaining remote access to this device and performing any of the tasks allowed by this device?

3) Scenario: IACS device disabled or destroyed

What is the consequence of a cyber incident that blocks the device from performing all or a subset of its normal functions?

b) Data scenarios

1) Scenario: IACS data theft

What is the consequence of someone stealing this data set?

- Does the data set have high intellectual property value?
- Is the data set of business value to a competitor?
- If publicly released, would the data set be an embarrassment to the organization?
- Is the data set required for regulatory compliance?
- Is the data set under a litigation hold order?

2) Scenario: IACS data corruption

What is the potential consequence if:

- The data set was intercepted and changed between the source and destination?
- The data set was corrupted at the source?
  - Is the data set required for regulatory compliance?
  - Is the data set under a litigation hold order?

3) Scenario: IACS data denial of service

What is the consequence if the user of the data was not able to access the IACS data set?

NOTE A group might carry out scenario based risk assessment by starting from descriptions of incident scenarios and then determining consequences of the scenario, as shown in this example or start by creating a list of undesirable consequences first, and then work backwards to develop possible incident scenarios that might create these consequences. A combination of these approaches may also be used.

#### A.2.3.3.5 Selecting the risk assessment methodology

Selecting the right risk assessment methodology for an organization is very subjective, based upon a number of issues. Many of these methodologies are commercially available. Some of these are available at no charge; others require a license for use. Assessing these methodologies to find the one most useable for an organization can be a challenging task. Common to most methodologies is the premise that risk is a combination of the likelihood of an event occurring and consequences of that event.

The complication is how to assign quantitative numbers to likelihood, which is typically expressed similar to a probability. Industry experience with process safety and accidents provides a large amount of historical quantitative data on which to base probability values. But, identifying the appropriate numbers for the likelihood of a specific cyber incident is not easy, not only because of a lack of historical data, but also because the past may not predict the future once a vulnerability becomes known to potential attackers. Because of this complication, many companies and trade associations have chosen to develop their own methodology to address the threat and vulnerability concerns of specific importance to their company in a manner consistent with their corporate culture. Also for this reason, this standard uses the term *likelihood*, which has to do with estimations of human capabilities and intent, rather than the expected term *probability*, which has to do with the occurrence of natural events unbiased by human interference.

Some methodologies support high-level risk assessment well. Some support detailed risk assessment well, by allowing input of vulnerability assessment results and they may also directly provide guidance for the associated detailed vulnerability assessment. An organization will find it effective to use a methodology that coherently supports both high-level and detailed risk assessment.

EXAMPLE An example of a trade association helping with the task of selecting the right methodology, the American Chemistry Council's Chemical Information Technology Center (ChemITC) has published a document titled "Report on Cyber Security Vulnerability Assessment Methodologies Version 2.0." [27] This document examines various elements of eleven different methodologies and compares them to a set of criteria important in a general-purpose cyber security risk methodology for assessing business IT systems, IACS and value chain systems. The report offers some sound advice for selecting a methodology. A portion of the guidance is included in the following with permission from CSCSP.

a) Step 1 – Filter

The first step is to review the overview of the selected methodologies. The purpose of this step is to filter the methodologies of interest based on criteria such as ease of use, complexity, scope, resource requirements and type of methodology (see [27], Appendix IV).

b) Step 2 – Select

After identifying the methodologies, select the methodologies that fit the organization's needs (see [27], Attachment II). Attachment II identifies the particular criteria that were used to assess the methodology. The criteria listed there address a much larger IT space beyond IACS. It may be that a methodology to address only a subset of the criteria used in the ChemITC study is necessary. Understanding the difference between the organization's needs and the evaluation criteria will be helpful when reviewing the synopses for the different methodologies. Then review the corresponding synopses to obtain more detailed information for assistance in making an informed methodology choice (see [27], Appendix V).

The synopsis for each methodology addresses the following topics:

- cyber security vulnerability assessment methodology,
- reviewers,
- date,
- web address,
- general observations,
- strengths compared to the common evaluation criteria,
- gaps compared to the common evaluation criteria,
- how this methodology could be used,
- limitations on methodology use, and
- suggested revisions.

c) Step 3 – Validate (optional)

If there is any uncertainty or difficulty choosing the methodology, review the technical criteria spreadsheets shown in the reference document for the methodology to validate the organization's choice(s) (see [27] Attachment II). The technical criteria spreadsheet exists for each methodology. This step is optional because it simply provides even more specific evaluation data.

d) Step 4 – Acquire the selected methodology

After narrowing down the methodology selection to one, obtain the methodology from the provider. The web addresses supplied in the bibliography are a good starting point.

#### A.2.3.3.6 High-level risk assessment – Identifying risks

Once a set of key stakeholders has been identified and provided with some training regarding the nature of IACS, they will perform a high-level risk assessment following the organization's selected methodology. This assessment process clarifies the nature of the individual risks to the organization that arise from the use of IACS. This clarity is needed to ultimately select the most cost-effective countermeasures to be designed or deployed and to help justify the costs of their deployment. While this task is the first step of a risk assessment, it is NOT a detailed vulnerability or threat assessment. It typically involves a risk analysis session to gather input from all stakeholders and takes advantage of high-level business consequences that may have been identified in the business rationale.

The deliverable document from the risk analysis session is a list of scenarios that describe how a particular threat could take advantage of a particular type of vulnerability and damage particular assets resulting in identified negative business consequences. The same session may also address calibration of consequence level and prioritization by risk tolerance level.

Stakeholders, who have experience with IACS applications in the business units and those responsible for the management of related risks, need to participate in the risk assessment effort to leverage their expertise and experience.

In order to make the most efficient use of the participants' time, it is normally necessary to schedule somewhere between a half and a full day to conduct the risk analysis session with all the stakeholder participants in attendance. There are two phases of this risk analysis session: background information and risk identification.

Regardless of which risk assessment method is ultimately used, it is also important to provide the participants in the risk analysis session with appropriate background information before beginning to identify the risks. Typical background information includes an overview of the business rationale and charter, an overview of IACS architectures and functions and an overview of specific types of incidents that occurred within the organization or publicized incidents that occurred in other organizations.

For the session to be successful, it is also important that participants understand the working definitions for risks and vulnerabilities; otherwise, the session is likely to identify vulnerabilities but may not succeed in identifying risks. Examples are useful for this purpose. Thus, as an example, vulnerability might be weak authentication on the control system HMI. The related threat might be that an employee with insufficient experience is able to operate the HMI without supervision and sets unsafe parameters. The consequence might be a stoppage of production due to safety controls being exercised. It is a common pitfall that an organization will list cyber vulnerabilities and then proceed to mitigate them.

#### A.2.3.3.7 High-level risk assessment – Classifying risks

##### A.2.3.3.7.1 General

The list of scenarios produced as an output of the risk analysis session describes a number of different risks posed to organizations by threats to IACS. One of the duties of corporate management is to manage all the risks to their organizations. To facilitate this effort risks need to be identified and prioritized. This subclause describes the three steps required to develop a framework to prioritize individual risks so the appropriate corrective actions can be justified.

##### A.2.3.3.7.2 The risk equation

Before describing the framework for risk prioritization and calibration, it is important to understand a basic concept of risk analysis (for example, the risk equation).

The likelihood of an event occurring takes into account both the likelihood that a threat that could cause an action will be realized and the likelihood that a vulnerability that allows the action will in fact be exploited by the threat. For example, for a virus to cripple a network, it needs to first reach the network and then needs to defeat antivirus controls on the network. If likelihood is expressed similar to a probability, then:

$$Likelihood_{Event\_Occurring} = Likelihood_{Threat\_Realized} \times Likelihood_{Vulnerability\_Exploited} \quad \text{(A.1)}$$

As discussed above, risk is made up of both likelihood and consequence, where consequence is the negative impact the organization experiences due to the specific harm to the organization's asset(s) by the specific threat or vulnerability.

$$Risk = Likelihoo_{dEvent\_Occurring} \times Consequence \quad \text{(A.2)}$$

##### A.2.3.3.7.3 Calibrating likelihood and consequence scales

Risk management systems have been developed within most organizations to deal with a wide variety of risks. In some cases the use of such systems has been mandated by regulatory requirements. These risk management systems make use of the same risk equation to prioritize the risks to the organization by the same type of threats to different assets (for example, information security) or by different threats to the same assets (that is, business continuity, industrial operation safety, environmental safety and physical security). In

most organizations, these risk management systems will already have developed scales for likelihood and consequence.

A typical likelihood scale is shown in Table A.1. This scale is only an example; the organization will need to determine the actual values used in this scale for themselves.

**Table A.1 – Typical likelihood scale**

| Likelihood | |
|---|---|
| **Category** | **Description** |
| High | A threat/vulnerability whose occurrence is likely in the next year. |
| Medium | A threat/vulnerability whose occurrence is likely in the next 10 years. |
| Low | A threat/vulnerability for which there is no history of occurrence and for which the likelihood of occurrence is deemed unlikely. |

Most organizations find it difficult to agree on likelihood, and little information is currently available to help. It is clear that differing opinions about this factor can radically change the investments made by the CSMS. Even though all may not agree with the final assessment on likelihood, the benefit of using it is that the assumptions being used to drive CSMS investment are clear for all to see. Since likelihood is the major factor of risk about which an organization has the least information and control, it is important to track improvements in industry data available to help make this factor more accurate.

To address the issue of lack of agreement, some organizations use the following methods:

- Use a probability of 100 % for likelihood and thus consider only consequences, or do this for certain types of consequences such as HSE
- Agree on a range of probabilities or likelihood categories and then work their prioritization process based on ranges
- Attempt more precision by consulting industry data that is available on attacks to IACS
- Attempt more precision by collecting internal incident data
- Separate likelihood into two factors – the likelihood that an adversary will attempt an attack and the likelihood that they will succeed. Separating these factors can help to clarify the real source of disagreement. If it can be agreed by all that an attempt will succeed and the argument for low risk relies on hoping no attempt happens, that can change the tenor of the discussion.

Consequence is usually measured in different terms for different types of risks. A typical consequence scale is shown in Table A.2. This example illustrates how cyber risk assessment can take process safety and other organizational risks into account. As above, this scale is only an example and will need to be calibrated for the organization.

It is important to follow a high level of intellectual honesty when assessing the consequences. During the assessment, identify assumptions that impact the level of consequence. For example, one might reasonably assume all the safety interlocks and shutdown systems are in place to minimize the impact of an event, since the likelihood of a cyber event in conjunction with an unrelated accident that disables safety systems is very small. However, in making this assumption, one also needs to consider whether there is a risk of an intentional cyber attack taking advantage of an accidental malfunction of safety systems or a coordinated physical or cyber attack causing such a malfunction. Other possible assumptions that may be called out are that operating practices are being followed to the extent typical of normal operation and fundamental lockout procedures are being followed. It is important for sites to honestly assess the risk, keeping in mind the sophistication and state of the control system and related operations and the dependency upon that system to operate the facility.

Calibrating consequences is necessarily performed with respect to the interests and policies of the organization performing the risk assessment. Although the risk of the IACS may be very much impacted by the hazards associated with the industrial operations being controlled by the IACS, it is important to not confuse the risk to the organization with the risk to society. The industrial operations may not employ any hazardous materials but produce a very valuable in-demand product generating high revenues for the company. An IACS security incident resulting in an industrial operations upset, causing several days of off-specification product that cannot be sold, could have very high financial impact to the company. To this company, the IACS has a High-Risk level even though society may view this as a low-risk because there is no health, safety or environmental impact to the general public. Likewise, the same organization might also consider an industrial operation upset on a production facility using hazardous materials as a high-risk consequence even if it did not impact production, due to internal policies and/or external regulations concerning public safety.

Prior to convening a group to calibrate individual risks, clarify the likelihood and consequence scales to provide guidance to the team performing the risk assessment.

**Table A.2 – Typical consequence scale**

| Consequence | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Risk area | | | | | | | | Environmental safety | National impact |
| | Business continuity planning | | | Information security | | | Industrial operation safety | | | |
| Category | Manufacturing outage at one site | Manufacturing outage at multiple sites | Cost (million USD) | Legal | Public confidence | People – on-site | People – off-site | Environment | Infrastructure and services |
| A (high) | > 7 days | > 1 day | > 500 | Felony criminal offense | Loss of brand image | Fatality | Fatality or major community incident | Citation by regional or national agency or long-term significant damage over large area | Impacts multiple business sectors or disrupts community services in a major way |
| B (medium) | > 2 days | > 1 hour | > 5 | Misdemeanor criminal offense | Loss of customer confidence | Loss of workday or major injury | Complaints or local community impact | Citation by local agency | Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community |
| C (low) | < 1 day | < 1 hour | < 5 | None | None | First aid or recordable injury | No complaints | Small, contained release below reportable limits | Little to no impact to business sectors beyond the individual company. Little to no impact on community services |

#### A.2.3.3.7.4 Risk level

The output of a qualitative risk assessment will consist of a list of assets or scenarios with an overall risk level ranking. This is typically developing in a matrix similar to the one shown in Table A.3, which defines three risk levels based upon three levels of likelihood and consequence. Thus each risk identified in the risk assessment is assigned a risk level. Again, this is meant as an example and will require further review by the organization.

**Table A.3 – Typical risk level matrix**

| | | Consequence category | | |
|---|---|---|---|---|
| | | **A** | **B** | **C** |
| **Likelihood** | **High** | High-risk | High-risk | Medium-risk |
| | **Medium** | High-risk | Medium-risk | Low-risk |
| | **Low** | Medium-risk | Low-risk | Low-risk |

The risk levels in each block (High, Medium and Low) each correspond to a particular combination of likelihood and consequence. An organization will define a risk tolerance policy related to each risk level, which will correspond to a particular level of corporate response. The actual approach to resolve the risk may be through the use of identified countermeasures. An initial version of this matrix should be prepared by responsible corporate management before the risk analysis process. This is the recommended method to ensure that the risk assessment effort provides results that directly assist in decision making and are actionable by the organization.

See A.3.4.2 for further information about defining a risk tolerance policy and how the risk tolerance policy and risk assessment results are used to manage risks.

### A.2.3.3.8 Detailed risk assessment

#### A.2.3.3.8.1 General

A detailed risk assessment focuses on individual IACS networks and devices, and takes into account a detailed technical vulnerability assessment of these assets and the effectiveness of existing countermeasures. It may not be practical for all organizations to perform detailed risk assessment for all their IACS assets at once – in this case an organization will gather enough information about their IACS to allow them to prioritize these systems to determine those to be analyzed first by the detailed vulnerability and risk assessment effort.

A detailed risk assessment identifies risks and then prioritizes them. Risks should be identified for each IACS. After identifying the risks, an organization may choose to prioritize all the risks found across all of these systems, prioritize the risks individually for each system or prioritize risks found in subsets of the IACS studied, such as all IACS at a specific site. Since prioritization ultimately drives decisions on what actions will be taken and investments made to improve cyber security, the scope of the prioritization should align with the scope of the budget and the decision authority in place in the organization to make these investments. For example, if all IACS supporting a specific product line are managed and budgeted as a group, risks across those IACS would be prioritized together to support that manager's decision process.

#### A.2.3.3.8.2 Characterizing key IACS

Identifying and prioritizing IACS risks requires that an organization locates and identifies key IACS and their devices and the characteristics of these systems that drive risks. Without an inventory of the IACS devices and networks, it is difficult to assess and prioritize where security measures are required and where they will have the most impact.

The team shall meet with IACS personnel to identify the different IACS used throughout the site and that control remote sites. The focus should be on systems rather than just devices including but not limited to, control systems, measurement systems and monitoring systems that use a central HMI device. Include industrial operations areas, as well as utility areas such as powerhouses and waste-treatment facilities.

As was noted above, the objective is to identify the major devices and kinds of devices that are in use and function collectively to operate the equipment under control. At this point in developing the security program it is not important to develop a comprehensive inventory of every device in the IACS, because the inventory will be used to make judgmental decisions about the relative risk the control devices introduce to the industrial operation. As examples, it is important to understand:

- Whether the field instrumentation and communication from the field transmitter to the controllers is analog-based or digital-based.
- Whether devices/systems are connected to each other and the types of networks used.
- Whether the devices are located within a secured area such as a building or fenced facility, or whether the devices are located remotely.
- Whether the control devices are subject to regulatory control.
- Whether the loss or malfunction of the device/system is significant in terms of their impact on the equipment under control, both in business/financial and HSE terms.

The resulting identification of devices/systems should show the scope of impact on the equipment under control if the devices lose control of the industrial operations they are applied to and their relative security vulnerability (from physical, network, or other factors). This kind of information can be used to understand the relative risk to the industrial operation. Conducting a comprehensive inventory to identify exact quantities of each kind of device is not necessary at this stage.

#### A.2.3.3.8.3 Grouping the devices and systems and developing an inventory

As the team identifies the individual devices/systems, it may be helpful to put the items into a logical grouping of equipment. In modern IACS facilities, this collection of equipment functions as an integrated system to control the various activities of the industrial operation. The number of logical control systems in a company will vary widely. In a medium to large organization, there may be several hundred logical IACS comprised of thousands of individual devices and low-level systems.

For medium to large organizations addressing cyber security on a company-wide basis, it may be very helpful to record the list of logical systems in a searchable database. DCS may be organized by line, unit, cell or vehicle within a local or remote geographical site. SCADA systems may be organized by control center, remote site and associated control equipment. The database will be more effective if the data are collected in a standard format to facilitate comparison of one system to another. Figure 4 is an example of a standard format that can be easily created in the form of a spreadsheet or database. It has been included to spur thinking about the kind of information that may be of use later in the system prioritization and detailed risk assessment activities.

**Industrial automation and control system network characterization**

Business _____
Site _____
Operating unit _____
Site IT contact _____ Phone # _____
Site process control contact _____ Phone # _____
Last updated _____

**PLEASE ANSWER THE FOLLOWING QUESTIONS :**

_____ **Are manufacturing and control systems currently interfaced to site or corporate LANs?**
_____ **Are manufacturing and control systems remotely accessed from outside the IACS domain?**

Process control domain

_____ Total number of IP addressable nodes
_____ Number of IP addressable nodes to be accessed from outside process control domain
_____ Number of concurrent users inside IACS domain
_____ Number of concurrent users inside IACS domain requiring access to external resources
_____ Number of total users outside IACS domain requiring access to process control resources
_____ Number of concurrent users outside IACS domain requiring access to process control resources
IP addressing (check all that apply)
_____ DHCP _____ Public addresses used (i.e. x.x.x.x)
_____ Static _____ Private addresses used (192.168.x.x)

Control platforms

_____ Number of control platforms
_____ Control platform type (PLC, DCS, PC)
Control platform vendor(s) _____ _____
Control platform model(s) _____ _____

Operator consoles and HMI devices

_____ Number of operator consoles
Operator console vendor(s) _____ _____
Operator console model(s) _____ _____
Operator console operating system(s) _____ _____

Application nodes (check all that apply)

_____ Proccess management and control server
_____ SCADA
_____ OPC server
_____ Engineering workstation
_____ Batch server
_____ Other _____

Network security barriers in-use
Type (firewalls, routers, VLANS, etc.) _____

Anticipated network security support (check all that apply)

_____ Site resources
_____ External (3rd party)

Site network (answer yes / no)

_____ Current site network topology diagrams available and up-to-date?
_____ Are process control nodes on isolated LAN segment?
_____ Site information security policy in place?
_____ Security office audit completed (if yes, date completed _____ )
_____ Does site use two-factor authentication?
_____ Security office risk assessment completed (if yes, date completed _____ )

Remote access requirements (check all that apply)

_____ Via site / corporate LAN
_____ Via dial-up modem
_____ Via internet
_____ Via local dial-up modem directly tied to manufacturing and control node(s)

Local egress requirements (check all that apply)

_____ To site applications and resources (document management systems, quality systems, business systems)
_____ To corporate applications and resources (document management systems, quality systems, business systems)
_____ To internet sites

*IEC 2321/10*

**Figure A.4 – Sample logical IACS data collection sheet**

Care should be taken when identifying industrial automation control devices/systems and focus attention beyond the devices that perform direct control. The system or network may be more than the PLC or DCS. In an integrated manufacturing or production facility, the IACS

network is comprised of devices that are directly used to manufacture, inspect, manage and ship product and may include, in addition to others, the following components:

- DCSs and associated devices;
- SCADA systems and associated devices;
- PLCs and associated devices;
- HMI stations;
- SIS and associated devices;
- shop floor (special purpose) computers;
- process information management (PIM) systems and manufacturing execution systems (MES);
- industrial automation control modeling systems;
- expert systems;
- inspection systems;
- material handling and tracking systems;
- analyzers;
- gauging systems;
- batch systems;
- electrical power monitoring and/or management systems;
- remote telemetry systems;
- communication systems used for communication with remote devices;
- standard operating condition (SOC) and standard operating procedure (SOP) systems;
- document management systems;
- program development computers;
- HVAC control systems;
- network communication gateways (that is, switches, hubs and routers);
- network protection devices (that is, firewalls and intrusion detection systems).

Consider including all CPU-based networked devices that are critical to sustaining production. The objective of this inventory step is to discover devices that are vulnerable to network-based attacks so they can be included in the detailed risk assessment.

NOTE This time is not the decision point for deciding which devices should be isolated or separated from the LAN. Err on the side of including more devices rather than fewer. After performing the risk assessment and having a better understanding of the overall vulnerabilities, the assessment team should decide if risk mitigation solutions are truly necessary and where the various devices should be located.

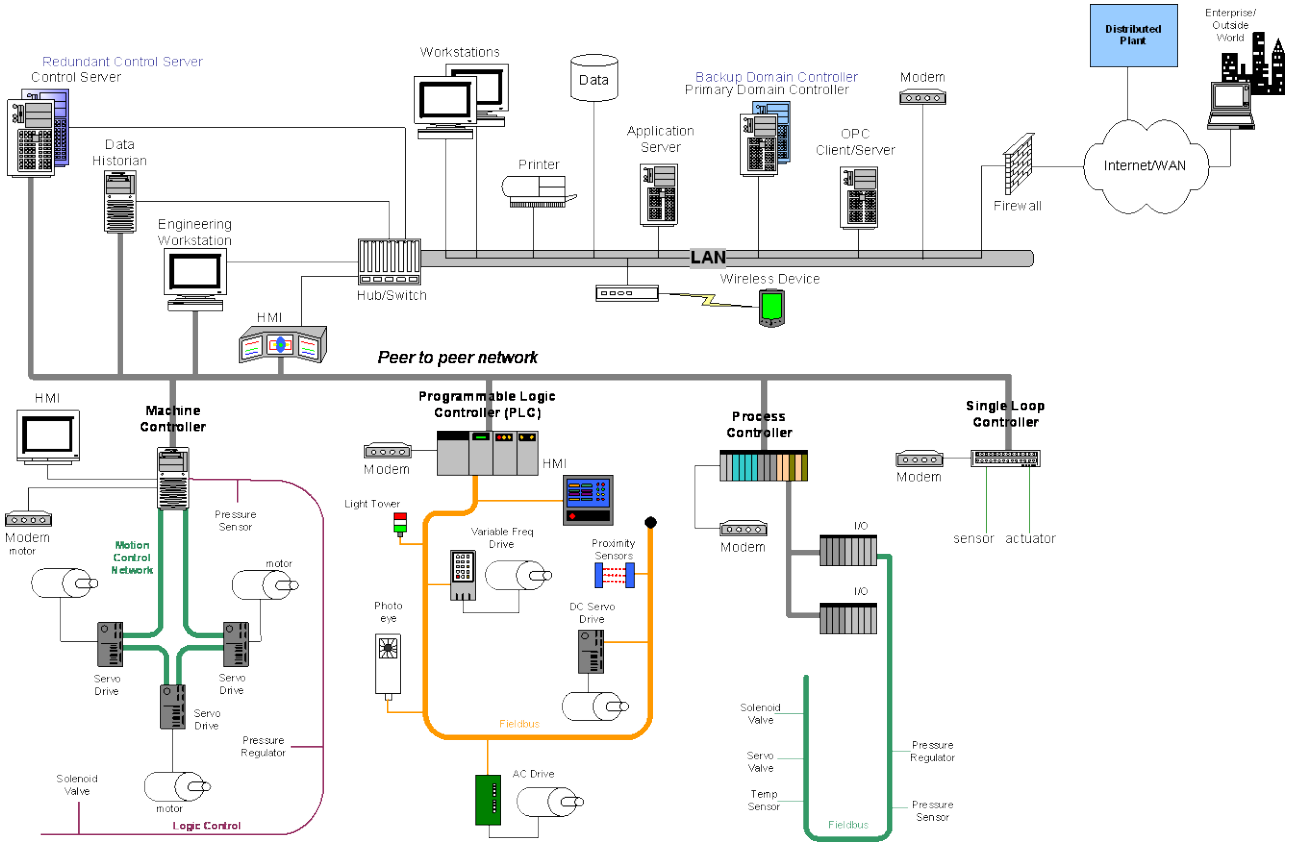
There are several enterprise-wide inventory tools commercially available that will work across networks to identify and document all hardware, systems and software resident on the network. Care shall be taken before using this type of application to identify IACS. Conduct an assessment of how these tools work and what impact they might have on the connected control equipment before using any of them.

Tool evaluation may include testing in similar, off-line, non-production control system environments to ensure the tool does not adversely affect the operation of the control system and interrupt production. While non-production devices may have no impact on production systems, they may send information that could (and has in the past) caused control systems failures or impairment. Impact could be due to the nature of the information and/or the system traffic and loading. Although this impact may be acceptable in IT systems, it is not acceptable in IACS.

### A.2.3.3.8.4 Developing simple network diagrams

A simple network diagram will be beneficial in grouping the various industrial automation and control devices and systems into an identifiable logical control system. It should include the devices identified with the Logical IACS Data Collection Sheet discussed in A.2.3.3.8.2. The diagram should attempt to capture the basic logical network architecture, such as connectivity approaches, combined with some of the physical network architecture basics like location of devices.

Before conducting prioritization of IACS or a detailed risk assessment, it is important that the team has a clear understanding of the scope/boundaries of the system to be assessed. A network diagram is a tool to help visualize the network and aid in performing the risk assessment. It can be a very simple block diagram showing devices, systems, and interface connections or more detailed like the one shown in Figure A.5. Either approach will be beneficial to meeting the objectives. If zones and conduits have been established, simple network diagrams should depict these elements. (More explanation on developing zones and conduits can be found in A.3.3.4.)




IEC 2322/10

**Figure A.5 – Example of a graphically rich logical network diagram**

Simple network diagrams are a starting point and represent a snapshot at one point in time. Experience in detailed vulnerability assessment shows that virtually every assessment turns up connections not identified in the initial diagramming process. Therefore these diagrams should not form the sole basis for assessing connectivity without more detailed physical validation. They are valuable for scoping the risk assessment effort and for defining zones and conduits as described in IEC/TS 62443-1-1.

### A.2.3.3.8.5 Preliminary assessment of overall risk for each identified system

Once the list of IACS devices, assets and networks has been completed, a preliminary assessment needs to be made as to the relative level of risk associated with the systems, so they can be prioritized for detailed risk assessment. If a detailed risk assessment is to be

carried out on all IACS or if the high-level risk assessment has provided sufficient insight to prioritize individual IACS by risk, then this step will not be required.

Each individual system shall be assessed to understand the financial and HSE consequences as identified in the high-level risk assessment, in the event that the availability, integrity or confidentiality of the system is compromised. Also, some measure of scale needs to be assigned to the assessment.

Personnel familiar with the IACS shall conduct the screening assessment activity. IACS and IT personnel typically bring knowledge of the devices and systems in use, while the operations personnel typically bring an understanding of the consequences of a security incident. This team of resources shall work together to accomplish the screening assessment.

The team will develop a high-level scale to quantitatively rate the overall risk associated with each system. The scale could be as simple as high, medium and low or 1 to 10 and shall establish the criteria for each gradation on the risk scale.

The team will make a judgment decision on the level of risk associated with each system by examining the financial and HSE consequences in the event that the availability, integrity, or confidentiality of the system is compromised. The team should record the high-level risk assessment for the logical system in the inventory list developed earlier. Establishing risk tolerance levels helps to prioritize the actual assets in the IACS environment.

The results of this preliminary assessment will be an important input to the decision to perform detailed vulnerability assessment for a particular IACS. A full vulnerability assessment shall be planned if:

- It is determined that the IACS is presently connected to the corporate network or to outside networks (for example, Internet, modems). A detailed risk assessment will help better understand the vulnerabilities and the appropriate mitigation strategy to reduce risk.
- It is determined that the system is currently supported remotely.
- It is anticipated that either of the two criteria above will be met in the near future. In that case, the vulnerability assessment should be performed before taking steps that result in this high-risk position.

#### A.2.3.3.8.6 Prioritizing the systems

The previous subclause suggested assigning a vulnerability/risk rating to each logical IACS identified. This rating scale is a good place to start the prioritization process. However, there are several additional things to consider when deciding where to begin focusing detailed risk assessment efforts, such as:

- risk to the company (for example, HSE or financial);
- places where assessment process is likely to be most successful;
- cost of the potential countermeasures required;
- capital versus non-capital costs;
- skilled support staff available for the particular system;
- geographic region;
- member trade association directives or sensitivities;
- country or local political requirements;
- outsourced or in-house support staff;
- site support to undertake the effort;
- history of known cyber security problems.

There is no right or wrong approach. The values will be different for each company. What is important is to use the same prioritization principles across all the sites. Record the prioritization decisions made and the basis for making them.

#### A.2.3.3.8.7 Identifying vulnerabilities and prioritizing risks

The next step in the risk assessment process is actually conducting the detailed risk assessment on the prioritized systems. Most methodologies employ an approach to break the system down into smaller pieces and examine the risks associated with these smaller elements comprising the overall system.

A detailed risk assessment should address physical and cyber security threats, internal and external threats and consider hardware, software, and information as sources for vulnerabilities.

It is imperative that a team of people performs the assessment to bring a well-rounded perspective to the assessment. The team should be comprised of, at a minimum, a lead site operations person, site IACS person, site IT person and site network person. Others to be considered include experts in physical security, information system security, legal, business (operations, maintenance, engineering, etc), human resources, HSE and hardware vendors. These people are in the best position to recognize vulnerabilities and the consequence of risk for their specific areas.

Although the goal is to understand the threats and consequences associated with a particular system, it is quite likely that a key objective is to be able to compare the assessment results from one system/site to another across the organization. The ability to do this will depend on how consistently the methodology is applied. Some proven approaches include:

- using a key person to lead the assessment process at each site;
- using a small team of people to lead the assessments based upon geography, business unit, and the like, who have participated with each other in other assessments;
- using good training materials with procedure and exercises to level-set the team of individuals who will conduct the assessments at each site;
- using a common form or database to record assessment results;
- centrally reviewing all the assessment results to check if the results seem realistic and comparable to other similar systems.

When conducting the assessment, consider all aspects of the IACS, including unintended changes in system configuration brought about by maintenance, temporary supplier connections to the system for support and even subtle changes in supplier design that could introduce new vulnerabilities through spare parts or upgrades, which should be considered and/or tested in the same manner as the original system components.

The assessment needs to address systems that interface with the IACS as well to ensure that they cannot compromise the IACS security or vice versa. Examples include development systems that provide online development capabilities and environmental and power systems whose compromise could create unacceptable risks.

In some cases, the vulnerability may lie with the vendor. Vendor quality assurance and design control may require a vulnerability assessment. This step is particularly important when ordering spare parts or upgrades.

At this point in the assessment process, a detailed examination of the network from a physical and operational viewpoint should be carried out in order to uncover any connections not shown in the initial simple network diagrams. Many assessments will find such connections.

The following potential sources for vulnerabilities related to network connectivity have been previously identified as weaknesses in certain systems and should be identified and examined:

- wireless access points, particularly poorly secured technologies such as early versions of IEEE 802.11;
- modem connections, particularly those that do not dial back and do not provide encryption;
- remote access software (for example, pcAnywhere®[3] and Timbuktu®) programs that are typically used for access by experts within or outside the entity to support systems or operations. These applications can provide significant control and configuration access to an unauthorized individual;
- remote windowing technologies such as X Windows®;
- Intranet connections;
- Internet connections;
- telemetry networks;
- any network connection to systems that are not a direct part of the IACS;
- any network connections used to couple parts of the SCADA or control system together that are not part of a physically secure, dedicated IACS network. In other words, any network that extends beyond the boundary of a single security zone or across insecure zones or is used for both IACS and other functions at the same time. Equipment included in network connections includes radio telemetry and outsourced services such as frame relay used to communicate between geographically separated areas.

A number of industry resources cover control system security and provide lists of typical vulnerabilities to look for in a detailed vulnerability assessment (see [27] and [29]).

The team's ultimate output is a list of vulnerabilities prioritized by their impact on risk. After vulnerabilities have been identified, the team then associates these vulnerabilities with threats, consequences and associated likelihoods for realization of the threat and exercise of the vulnerability. This analysis takes into account potential mitigation due to physical security measures. Those vulnerabilities that contribute to the highest level risks are typically easy to agree upon. To complete the vulnerability assessment process, the team's methodology should include an agreed method to determine how to prioritize vulnerabilities that contribute to a large number of medium and low-level risks.

Detailed risk assessment results shall be documented and action taken on recommendations resulting from them (see A.3.4.2).

Documentation of the detailed vulnerabilities found during the detailed risk assessment typically includes for each vulnerability found, the date of assessment, identification of assets involved, description of the vulnerability, name of an individual who observed the vulnerability and any tools or methods they used in order to do so. In addition to vulnerabilities found, the documentation of the detailed vulnerability assessment should include vulnerabilities checked for but not found to be present and how this was verified for each asset assessed. This may take the form of a simple checklist. Documentation of vulnerabilities provides great leverage when updating the risk assessment and when specific questions about assets are raised. Prior vulnerability checklists and results form a baseline from which to improve vulnerability assessments in the future and a basis for consistency across an organization. An organization should view them in this light and avoid viewing them as a static definition of the contents of such an assessment.

---

3 pcAnywhere®, Timbuktu® and X Windows® are examples of suitable products available commercially. This information is given for the convenience of users of this standard and does not constitute an endorsement by ISA of these products.

Tasks and documentation related to the high-level and detailed risk assessment processes described in this subclause and the risk management process in A.3.4.2 can be integrated for efficiency to suit the needs of a particular organization.

The detailed risk assessment results should be updated and revalidated on a periodic basis. In addition, since a detailed risk assessment can become out of date due to changes in the environment of a control system, triggers for an updated risk assessment effort should be incorporated into the management of change program. This is a critical point, since most organizations find it easier to establish a cyber security baseline than to maintain it over time (see A.4.3).

#### A.2.3.3.8.8 Pitfalls to avoid

During the assessment, common pitfalls that can derail the risk assessment process should be avoided through the following actions:

a) Designing the solution during the assessment

   The purpose of the assessment is to learn what risks exist, not to design the solution as a team. A lot of time can be wasted by trying to solve the problem and debating one approach versus another while assessing one particular asset. The focus should be on understanding the risks and consequences that currently exist or may occur in the foreseeable future, such as a project currently underway to add a new model device with a network interface.

b) Minimizing or overstating the consequence

   An honest assessment of the consequence of an incident affecting a particular hardware, software or information asset should be provided. Consequences should not be minimized for the purpose of avoiding taking proper security risk mitigation actions to reduce risk. What may be very important to one particular person because it directly impacts his or her job, may have a very different level of consequence to the organization as a whole.

c) Failing to gain consensus on the risk assessment results

   Reaching agreement on the risks and consequences is extremely important. It will be much harder to reach agreement on the countermeasures if the team does not have a common understanding of the risk and agreement on the importance.

d) Assessing the system without considering the assessment results from other similar systems

   It is important to validate that the results are appropriate and consistent with those of similar assessment processes at other sites. The conclusions from previous similar system assessments and the vulnerabilities identified can be very beneficial to the assessment of the system at hand.

#### A.2.3.3.8.9 Interrelationship with physical security measures

Cyber security and physical security may be closely related. In some situations they may function as independent layers of protection and in other situations they are highly dependent upon each other. The loss of one may represent a loss of both layers of protection. During the detailed risk assessment for a system, the potential interaction and how it may affect the consequences should be kept in mind.

In some industries, it is common practice to have a SIS in addition to the IACS. If the SIS is relay based, the likelihood of it being affected by a cyber event that impacts the IACS is small. The SIS can be counted upon to perform its safety function and the consequence of a cyber event may be contained and reduced. However, if the SIS is electronically based and tied to the same network as the IACS (some industries do not recommend this practice), the likelihood of a cyber incident impacting both systems is much higher and the consequence could be greater.

Another example might be a badge access system to a locked control room. Under normal situations, the access control system provides additional security to the control systems.

However, in the event of a denial of service (DoS) flood of the network, the door access control system could fail to function and impede the operator's ability to gain access to the control room operator console. The same DoS network overload could be affecting the operator console as well. In this situation, the single cyber incident serves as a double impediment to responding to the control device and could increase the consequence of the incident.

Eventually, cyber security risk assessment methodologies should be incorporated into physical and site risk assessment methodologies.

#### A.2.3.3.8.10 Risk assessment and the IACS lifecycle

The previous subclauses describe how the process of risk assessment can be carried out on existing IACS when first establishing a CSMS and applied periodically thereafter. Risk assessment is most effective and least disruptive when applied in a similar fashion during the various stages of the lifecycle of the IACS *before* it is running in production mode:

a) During development of a new or updated IACS

Cyber risk should be considered in advance before implementing a new or modified IACS, since experience has shown it will always be easier and less expensive to consider security during the design phase than to add it later. The process for high-level risk assessment proceeds in the same way for a future system as described above for an existing system. The assessment is ideally performed in parallel with high-level design and the results of the proposed design and risk assessment are reviewed together. A detailed risk assessment can also be carried out in parallel with detailed design, though vulnerabilities identified are hypothetical and will not in all cases be as specific as for an already implemented system. In this way, risk assessment during development can drive decisions about what countermeasures should be put in place along with the desired IACS improvements, to minimize surprises after implementation.

b) During implementation of a new or updated IACS

Even with attention to risk during the development phase, implementation details may introduce unexpected vulnerabilities. In the best case, part of the acceptance process for a new or updated IACS includes not only testing, but also a detailed vulnerability analysis as previously described. Thus, for example, an organization may need to determine whether to turn on a new or updated system before a patch to a recently discovered vulnerability is available for the underlying operating system.

c) During retirement of an IACS

The decision to retire or retain an IACS or components of an IACS is based upon many factors, including cost, desire for new functionality or capacity, ongoing reliability and availability of vendor support. Impact on cyber security is also a factor to be weighed in this decision. New components and architectures may improve security functionality and/or introduce new vulnerabilities that need to be addressed. Hence a cyber risk assessment that analyzes a retirement decision examines both the scenario in which the old system is replaced and the scenario in which the old system is retained for some period of time.

High-level and detail risk assessments are updated upon the retirement of an IACS for two reasons: 1) the removal of the IACS may impact the vulnerability of some IACS that remain in place and 2) if the IACS is replaced by a new system, new vulnerabilities may be introduced as discussed earlier. An example of this is that network connectivity to an IACS that remains in place may have always taken place through the IACS being removed. This means that a new connectivity design is put in place for the remaining IACS and this configuration should be assessed for vulnerabilities and associated risks.

### A.2.3.4 Supporting practices

#### A.2.3.4.1 Baseline practices

The following ten actions are baseline practices:

a) Establishing the criteria for identifying which devices comprise the IACS.

b) Identifying devices that support critical business processes and IACS operations including the IT systems that support these business processes and IACS operations.

c) Classifying the logical assets and components based on availability, integrity, and confidentiality, as well as HSE impact.

d) Prioritizing risk assessment activities based on consequence (for example, industrial operations with known high hazards are addressed with a high priority).

e) Scoping the boundaries of the system to be assessed, identifying all assets and critical components.

f) Developing a network diagram of the IACS (see A.2.3.3.8.4).

g) Understanding that risks, risk tolerance and acceptability of countermeasures may vary by geographic region or business organization.

h) Maintaining an up-to-date record of all devices comprising the IACS for future assessments.

i) Conducting a risk assessment through all stages of the technology lifecycle (development, implementation, updating and retirement).

j) Identifying reassessment frequency or triggering criteria based on technology, organization or industrial operation changes.

#### A.2.3.4.2 Additional practices

The following four actions are additional practices:

a) Identifying and classifying assets to aid in defining the company's risk. Important focus areas should be people involved and technologies used. The creation of a checklist helps group the assets into categories (see A.2.3.3.8.3).

b) Classifying individual assets based on the safety implications of availability, integrity, and confidentiality. An asset could have different levels of classification for each of the categories.

EXAMPLE Classification for a specific type of data:

- Availability: low – the system does not require continuous operation. The system is not part of a hazardous operation. A delay of up to one or two days would be acceptable.
- Integrity: medium – the data is verified at various stages and changes to it would be detected.
- Confidentiality: very high – the business critical data should be maintained at the highest confidential level.

c) Establishing the likelihood (that is, probability or estimated frequency) that a particular threat will be successful, in view of the current level of controls. It is important to look at other typical controls that may be in place in manufacturing/operations that would supplement cyber security controls to reduce the likelihood of the consequence occurring. These include independent SIS and other PSM techniques such as passive, auxiliary, independent back-up devices. The estimated frequency is directly related to the overall vulnerability and threats and could be expressed quantitatively as a percentage or more subjectively as high, medium or low.

d) Defining the consequences or impact of a successful threat attempt based on the business or IACS risk evaluation.

### A.2.3.5 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [24], [26], [27], [28], [29], [30], [33], [42].

## A.3 Category: Addressing risk with the CSMS

### A.3.1 Description of category

The second main category of the CSMS is Addressing Risk with the CSMS. This category contains the bulk of the requirements and information contained in the CSMS. It is divided into three element groups:

- Security policy, organization and awareness,
- Selected security countermeasures, and
- Implementation.

### A.3.2 Element group: Security policy, organization and awareness

#### A.3.2.1 Description of element group

The first element group in this category discusses the development of the basic cyber security policies, the organizations responsible for cyber security and the awareness within the organization of cyber security issues. Figure A.6 shows a graphical representation of the five elements contained in the element group:

- CSMS scope,
- Organizing for security,
- Staff training and security awareness,
- Business continuity plan, and
- Security policies and procedures.


**Figure A.6 – Graphical view of element group: Security policy, organization, and awareness**

#### A.3.2.2 Element: CSMS scope

##### A.3.2.2.1 Description of the element

With the business rationale established and management support obtained, the next step is to develop a formal scope or charter for the effort. This scope should explain what is to be accomplished (in business terms) and when. It defines the specific entity of focus.

This scope statement should be owned by a senior executive program champion, or by a management team who will be responsible for guiding the team during program development. The champion will ultimately be responsible for making sure that the program is executed, including communications, funding, enforcement and auditing.

Ultimately, the CSMS shall encompass all business units and all geographic parts of the organization. If leadership commitment cannot be obtained initially for this scope of work,

define a smaller scope of work and use this as an opportunity to build credibility and demonstrate the value of the CSMS.

#### A.3.2.2.2 Developing the CSMS scope

Management needs to understand the boundaries where the CSMS apply to the organization as well as establish a direction and focus for the CSMS. By developing a clearly defined scope, it is easier for management to convey its goals and purpose for the CSMS.

The scope should include all aspects of the IACS, integration points with business partners, customers and suppliers. A management framework (for example, organization) should be established to initiate and control the implementation and ongoing operations of cyber security within the company.

An organization responsible for determining and communicating corporate policies as they relate to cyber security is important to protect corporate assets from a cyber security perspective. Companies need to recognize that in today's Internet-driven business world, electronic information connectivity is an integral part of doing business and thus cyber security is essential. Business transactions are not only contained within the organization's Internet firewall, but are extended to customers, vendors, third-party contractors and outsourcing partners.

The overall scope of work needs to be clarified from three different perspectives: business, architectural and functional.

From a business perspective the scope of work needs to answer questions similar to:

- Which corporations are included?
- Which business units are included?
- Which geographical regions are included?
- Which specific sites are included?

From an architectural standpoint, the scope of work needs to answer questions similar to:

- Which computer systems and networks will be addressed?
- Will SCADA and distribution monitoring systems be included?
- Will non production-related computer systems (both those supported and unsupported by the IT organization) in manufacturing be included?
- Will manufacturing execution systems (MES) be included?
- Will burner management systems and SIS be included?
- Will robotic systems be included?
- Will connections to suppliers or customers be included?

From the functional standpoint, the scope of work can be divided into the following two categories:

a) Direct risk management activities

   These are activities that involve the evaluation, communication and prioritization of risk. Examples include designation of local cyber security owners, collecting and maintaining an asset inventory, developing and maintaining the network architecture, completing internal or external audits and reporting these results on a business unit or corporate basis.

b) Risk management related projects

These are activities funded on the basis of reducing the risks identified by the risk management activities. These indirect risk management solutions take the form of projects that are bounded in time and the development and deployment of ongoing services.

In clarifying the functional scope, questions similar to the following should be considered:

- How does the scope of this work relate to existing risk management systems?
- How does the scope of this work relate to information security policies that already apply to these systems and organizations?
- How does the scope of this work relate to technical standards and procedures that already apply to specific architectural components (that is, basic process control systems, SCADA systems, SIS, burner management systems and robotic systems)?
- How does the scope of this work relate to projects that are already funded?
- How does the scope of this work relate to existing services?

Leadership support provides the endorsement of the effort by managers who are responsible for assigning resources to manage and implement the tasks to reduce risks to the IACS.

The scope should be owned by a senior executive program champion who will be responsible for guiding the team during program development. The champion will ultimately be responsible for making sure that the program is executed, including communications, funding, enforcement and auditing.

With support and commitment from senior leadership, stakeholders should be identified and their time to work on improving security should be allocated. The stakeholders are responsible for moving the security initiative forward. With support from senior leadership the stakeholders initiate the next activities and engage the right resources to accomplish the tasks. Form an integrated team that involves traditional desktop and business computing systems, IACS and systems that interact with customers, suppliers and transportation providers. The charter and scope mentioned earlier bring focus on who needs to be involved to meet the objectives of the initiative.

It is likely that senior leadership may identify a project leader whose job it is to round up the right people to work on the security effort. This person shall have a high-level understanding of the current state of cyber security procedures in the company. Assuming that the goal is to improve the cyber security policies and procedures for IACS, the project leader should look for the areas that could be affected by IACS cyber security incidents and identify the key people that are recognized as responsible/accountable for these areas. The focus should be on identifying people in the right role, independent of the organization to which they are assigned.

It is important to note that different company organizational structures may have these people in different organizations. The goal is to develop a cost-effective CSMS that leverages existing business processes and organizations rather than create a whole new organization. People who are already in the right role and with the right experience should be selected when possible. Breaking down turf issues may be an important activity of this stakeholder team.

The core team of stakeholders should be cross-functional in nature and bring together skills not typically found in any single person. The team should include people with the following roles:

- IACS person(s) who may be implementing and supporting the IACS devices;
- operations person(s) responsible for making the product and meeting customer orders;
- process safety management person(s) whose job it is to ensure that no HSE incidents occur;

- IT person(s) who may be responsible for network design and operation, support of desktops and servers, and the like;
- security person(s) associated with physical and IT security at the site;
- additional resources who may be in the legal, human resources and customer support or order fulfillment roles.

The set of stakeholders may change over time or specific individuals may take on higher-profile roles during different phases or activities while developing the CSMS. It is not important which organization leads the effort, but rather that the leader exhibits the right set of behaviors that foster working together as a team with a unified purpose. The parent organizations to which the above individuals are aligned each have something to offer and have a stake in decisions and outcome of the CSMS.

#### A.3.2.2.3 Suggested practices

##### A.3.2.2.3.1 Baseline practices

The following three actions are baseline practices:

a) Describing the organization(s) responsible for establishing, communicating, and monitoring cyber security within the company.

b) Stating the scope of the CSMS, including:
   - information systems – including all operating systems, databases, applications, joint ventures and third-party business activities;
   - IACS – including all process control systems, SCADA systems, PLCs, DCSs, configuration workstations and plant or lab information systems for both real-time and historical data;
   - networks, local area networks (LANs), wide area networks (WANs) – including hardware, applications, firewalls, intrusion detection systems, and the like;
   - integration points with support and service providers;
   - user responsibilities – including policies to address authentication and auditability;
   - information protection – including access requirements and individual accountability;
   - risk management – including processes to identify and mitigate risks and document residual risk;
   - disaster recovery – including identification of critical software/services;
   - training requirements;
   - conformance, compliance and audit;
   - asset identification.

c) Characterizing the organization responsible for the CSMS, including:
   - organization structure;
   - location;
   - budget;
   - roles and responsibilities associated with the CSMS processes.

##### A.3.2.2.3.2 Additional practices

The following five actions are additional practices:

a) Having management endorse the scope and responsibilities of the CSMS.

b) Having a clear understanding of the roles and responsibilities associated with the organization(s) responsible for some aspect of the CSMS.

c) Documenting the scope of the CSMS with separate subclauses addressing specific components.

d) Addressing business, legal (for example, Data Privacy), and regulatory requirements and responsibilities.

e) Identifying and documenting the dependency of process safety on cyber security and physical security practices and procedures including a framework for organizational interaction.

#### A.3.2.2.4 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [24], [26].

### A.3.2.3 Element: Organizing for security

#### A.3.2.3.1 Description of element

Companies should establish an organization, structure, or network of people with responsibility for overall security recognizing there are physical as well as cyber components that should be addressed.

It is important to establish accountability to provide direction and oversight to an organization's cyber security. Cyber security in the broadest sense covers not only data, but also the systems (hardware and software) that generate or store this information and includes elements of physical security as well. IACS, value-chain partners, third-party contractors, joint venture partners, outsourcing partners and physical security specialists should be considered by the organization as part of the overall security structure and hence included in the scope of responsibility.

#### A.3.2.3.2 Building an organizational framework for security

The commitment to a security program begins at the top. Senior management shall demonstrate a clear commitment to cyber security. Cyber security is a business responsibility shared by all members of the enterprise and especially by leading members of the business, manufacturing, IT and risk management teams. Cyber security programs with visible, top-level support and buy-in from organization leaders are more likely to gain conformance, function more effectively and have earlier success.

A management framework should be established to initiate and control the implementation of an overall security program. The scope and responsibilities of cyber security for organizations should include physical security and cyber security for IT systems, IACS suppliers, third party contractors, outsourcing partners and the value-chain components of the organization. An overall security program should be extended to include joint venture operations.

Organizations should establish a framework with management leadership to approve the cyber security policy, assign security roles and coordinate the implementation of cyber security across the organization. The framework may face some interesting organizational challenges. Many companies are organized in a three-dimensional matrix where one dimension is by business line, a second dimension is by function or discipline and a third dimension is by geographical region. Individual managers typically have responsibilities for some part of this overall organization. Because a system is only as secure as its weakest link, a cyber security system will ultimately need to be developed that spans the entire geographical reach of the organization.

Cyber security deals with a number of different risks that can generally be classified into concerns about availability, integrity or confidentiality. Concerns about availability would typically be managed by a business continuity planning program or network security program. Concerns about integrity in a manufacturing context are typically managed by a process safety or quality assurance program. Concerns about confidentiality are typically managed by an information security program. Because cyber security affects so many different risk areas,

it is likely that no one single manager will have the necessary scope of responsibility to authorize a cyber security program for all IACS. It will often be necessary to convene and convince a small group of senior managers who, quite possibly, have never had to work closely together before to make a consensual decision.

Either an overall enterprise (for example, a corporation) or individual sub-organizations within the enterprise may work toward conformance with this standard. If the overall enterprise is to conform, risk is assessed across the total enterprise. In this case, for example, individual plants within the corporation may carry out risk assessments, but will use a common risk assessment methodology that allows compilation of these assessments at the corporate level. Thus if an overall enterprise has a goal to achieve conformance, it will find it necessary to set guidelines to support this, even if individual sub-organizations such as plants do much of the work.

Other possibilities are that the overall enterprise is not attempting to meet the standard, but is requesting its sub-organizations at some level to do so individually or that some sub-organizations are attempting to meet the standard on their own initiative. In either of these cases the enterprise will still need to support these sub-organizations in meeting any specific requirements in the standard that are handled at the enterprise level, such as securing corporately provided architectures, employee screening and wording of contracts with service suppliers. Under these scenarios, for example, an individual plant site could have its own risk assessment methodology, determine its own mitigation priorities and have plant level senior management supporting the effort. And in these cases the enterprise is not evaluating its own overall conformance with the standard, although it potentially might evaluate conformance of individual plants. This strategy would make the most sense for a highly decentralized diverse corporation or other enterprise.

#### A.3.2.2.3.3 Getting started and gaining support

For senior managers to effectively champion a cyber security program they must be convinced that the costs of the program they will pay out of their budgets will be less than the impact of the threat on their areas of responsibility. It may be necessary to develop a business rationale or a business case for managing cyber security risks to convince leadership to support the program. Budgetary responsibilities and scopes of responsibility will need to be clarified amongst the senior leadership.

Due to the constraints of time, many senior managers have trusted advisers they use to filter the important issues they need to address from the issues that others are more suited to address. These individuals are gatekeepers. In large organizations, there are frequently staff organizations that senior managers use to generate recommendations for technically complex issues. It may be necessary to work with these staff organizations initially to collect sufficient information to make the business case. These organizations may also be able to provide insight into which senior managers typically handle specific types of risks.

It is likely that senior leadership may identify a project leader whose job it is to round up the right people to work on the security effort. This person shall have a high-level understanding of the current state of cyber security procedures in the company. It is important to recognize that a truly integrated CSMS involves traditional desktop and business computing systems, IACS and value chain systems that interact with customers, suppliers and transportation providers. The charter and scope mentioned earlier bring focus on who needs to be involved to meet the objectives of the initiative.

The project leader should look for the areas that could be affected by IACS cyber security incidents and identify the key people that are recognized as responsible/accountable for these areas. The focus should be on identifying people in the right role, independent of the organization to which they are assigned.

It is important to note that different company organizational structures may have these people in different organizations. The goal is to develop a cost-effective CSMS that leverage existing business processes and organizations rather than create a whole new organization. People

who are already in the right role and with the right experience should be selected where possible. Breaking down turf issues may be an important activity of this stakeholder team.

The core team of stakeholders should be cross-functional in nature and bring together skills not typically found in any single person. The team should include people with the following roles:

- IACS person(s) who may be implementing and supporting the IACS devices;
- operations person(s) responsible for making the product and meeting customer orders;
- process safety management person(s) whose job it is to ensure that no health, safety and environmental incidents occur;
- IT person(s) who may be responsible for network design and operation, support of desktops and servers, and the like;
- security person(s) associated with physical and IT security at the site;
- additional resources who may be in the legal, human resources and customer support or order fulfilment roles.

The set of stakeholders may change over time or specific individuals may take on higher profile roles during different phases or activities in the life of developing the CSMS. It is not important which company organization leads the effort, but rather that the leader exhibits the right set of behaviors that foster working together as a team with a unified purpose. The parent organizations to which the above individuals are aligned each have something to offer and have a stake in decisions and outcome of the CSMS.

One common practice to convince senior managers is to test new programs in a small geographic region or at a particular site to prove that new procedures/programs work prior to devoting a large amount of resources. This can be another effective approach to either get access to senior managers or actually make the business case to senior managers.

Once the appropriate senior managers have been identified, it is important to decide whether to present the CSMS to them all as a group or to approach them sequentially. It is more efficient to convince them all simultaneously, but they may not all be receptive to the discussion simultaneously. If there is a need to persuade a leadership team, it is helpful to identify an ally on the leadership team to review the presentation and offer input before making the presentation to the whole team. Due to the number of different risk areas that are affected by cyber security, it is not uncommon to require persuasion of more than one leadership team.

If the costs of the cyber security program cannot be determined initially due to lack of a computer inventory or lack of standard countermeasures, a second round of presentations may be required once these costs are determined more precisely. The emphasis at this early stage needs to be on putting a system in place to balance the costs of the countermeasures with the costs of the risks. Usually there is inadequate information at this stage to request a specific budget for implementing countermeasures.

#### A.3.2.3.4 Supporting practices

##### A.3.2.3.4.1 Baseline practices

The following five actions are baseline practices:

a) Obtaining executive management commitment for setting up an organizational framework to address security.

b) Assigning responsibility for cyber and physical security to personnel with an appropriate level of funding to implement security policies.

c) Initiating a company-wide security team (or organization) to provide clear direction, commitment and oversight. The team can be an informal network, organizational or

hierarchical structure spanning different company departments or organizations. This team assigns responsibilities and confirms that business processes are in place to protect company assets and information.

d) Establishing or modifying contracts to address cyber and physical security policies and procedures of business partners, third-party contractors, outsourcing partners, and the like, where the security policies and procedures of those external partners affect the security of the IACS.

e) Coordinating or integrating the physical security organization where an overlap and/or synergy between physical and cyber security risks.

#### A.3.2.3.4.2 Additional practices

The following four actions are additional practices:

a) Establishing the responsibility for IACS cyber security:

- A single individual from any of several functions is responsible for cyber security for the entire organization. This individual chairs a cross-functional team representing the various business units and functional departments. The team demonstrates a commitment to cyber security and sets a clear direction for the organization. This includes asset and industrial operation ownership as well as providing the appropriate resources for addressing security issues.
- A separate team is responsible for the security of IACS under either a manufacturing or engineering organization. While this approach has the advantage of having leadership knowledgeable of the risks associated with IACS, the benefits of such an approach can be lost if this team does not coordinate closely with those responsible for traditional IT assets and physical security.
- An overall security team is responsible for both physical and logical assets. In this hierarchical structure, security is under a single organization with separate teams responsible for physical and information systems. This approach is useful in smaller organizations where resources may be limited.

b) Coordinating efforts with law enforcement agencies, regulators, and Internet service providers along with other relevant organizations, as it relates to terrorist or other external threats. Organizations that have established relationships with local emergency response personnel expand these relationships to include information sharing as well as responding to cyber security incidents.

c) Holding external suppliers that have an impact on the security of the organization to the same security policies and procedures to maintain the overall level of IACS security. Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cyber security policies and procedures if they will impact IACS security:

- companies should consider the increased security risk associated with outsourcing as part of the decision making process to determine what to outsource and outsourcing partner selection;
- contracts with external suppliers governing physical, as well as logical access;
- confidentiality or nondisclosure expectations and intellectual property rights should be clearly defined;
- change management procedures should be clearly defined.

d) Removing external supplier access at the conclusion/termination of the contract. The timeliness of this is critical and is clearly detailed in the contract.

#### A.3.2.3.5 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [26], [30], [43].

### A.3.2.4 Element: Staff training and security awareness

#### A.3.2.4.1 Description of the element

Security awareness for all personnel is an essential tool for reducing cyber security risks. Knowledgeable and vigilant staff is one of the most important lines of defense in securing any system. In the area of IACS, the same emphasis shall be placed on cyber security as on safety and operational integrity, because the consequences can be just as severe. It is therefore important for all personnel (employee, contract or third-party) to understand the importance of security in maintaining the operation of the system. Staff training and security awareness programs provide all personnel (employees, contractors, and the like) with the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to IACS and to help ensure their own work practices include effective countermeasures. All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering. Cyber security training and security awareness programs are most effective if they are tailored to the audience, consistent with company policy and communicated regularly. Training provides a means to communicate key messages to personnel in a timely fashion. An effective training program can help employees understand why new or updated security controls are required and generate ideas they can use to reduce risks and the impact on the organization if control methods are not incorporated.

#### A.3.2.4.2 Developing a staff training program and building security awareness

Training of one sort or another is an activity that spans almost the entire period during which a CSMS is developed and implemented. It begins after the scope of the effort is clarified and the team of stakeholders is identified. The objective of the training program is to provide all personnel with the information they need so that they will be aware of any possible threats to the system and their responsibilities for the safe and secure operation of the production facilities.

The organization should design and develop a cyber security training program in conjunction with the organization's overall training program. Training should be in two phases: 1) general training for all personnel and 2) role-based training aimed at specific duties and responsibilities. Before beginning the development of the training program it is important to identify the scope and boundaries for the training and to identify and define the various roles within the organization.

The general training program should be developed for all personnel. Users should be trained in the correct security procedures, the correct use of information processing facilities and the correct handling of information in order to minimize risks. Training should also include legal responsibilities, business controls and individual security responsibilities.

Role-based training should focus on the security risks and responsibilities associated with the specific role a person fills within the organization. These individuals will need more specific and intensive training. Subject matter experts should be employed to contribute to this training. Role-base training may be conducted in the classroom, may be web-based or hands-on. This training may also leverage training provided by vendors for in-depth discussion of tools and associated exposures.

The program should include a means to review and revise the program, as required and a means to evaluate the effectiveness of the program. Also, there should be a time defined for periodic retraining.

Management's commitment to training and ensuring adequate cyber security awareness is critical to providing a stable and secure computing environment for both IT and IACS. In particular for the IACS environment, a stable and secure computing environment aids in maintaining the safe operation of the equipment under control and reducing HSE incidents. This should be in the form of resources for developing and organizing the training and making staff available to attend.

Following the development of a cyber security training program, the organization should provide the appropriate training for all personnel. Training programs should be provided in a place and at times that allow personnel to be trained without adversely affecting their other responsibilities.

General training should be provided as part of a new employee's orientation and as a part of the orientation for contract, temporary or third-party personnel. The training required should be appropriate for the level of contact which they will have with the organization. Specialized training may be provided as follows:

a) Training for stakeholders

   Training is appropriate for the team of stakeholders as well as the community of individuals in the IACS community who will ultimately be impacted. The team of stakeholders will need specific training on the type of risks that are being considered, the scope and charter of work that management has approved, any background information on incidents that have occurred to these systems either within the organization or within the industry in general and on the types of architectures and systems that are in use within the organization. Formal classroom training is not necessary to share this information. Presentations at business meetings, communication sessions and e-mail announcements are examples of ways to share the information.

b) Training employees preparing for new roles

   Training will be needed for employees as they prepare to assume new roles either within the direct risk management system or within the risk management related projects. Virtually all members of the IACS community will receive a certain amount of training during this phase. Some of the direct risk management roles will include responsibilities for self-assessments or internal audits.

c) Training of auditors

   Training will be needed for auditors to help them understand the nature of the systems and networks they will be auditing as well as the specific policies that have been created.

d) Ongoing training

   There will be an ongoing need for training at all levels due to the addition of new employees and third-party personnel, the need to provide updates as policies and services are modified over time and to provide refresher training to ensure that personnel remain competent in their roles and responsibilities.

It is important to validate that personnel are aware of their roles and responsibilities as part of the training program. Validation of security awareness provides two functions: 1) it helps identify how well the personnel understand the organization's cyber security program and 2) it helps to evaluate the effectiveness of the training program. Validation can come through several means including written testing on the content of the training, course evaluations, monitored job performance or documented changes in security behavior. A method of validation should be agreed upon during the development of the training program and communicated to the personnel.

Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis. Documenting training can assist the organization to ensure that all personnel have the required training for their particular roles and responsibilities. It can also help identify if additional training is needed and when periodic retraining is required.

Over time, the vulnerabilities, threats and associated security measures will change. These changes will necessitate changes to the content of the training program. The training program should be reviewed periodically (for example, annually) for its effectiveness, applicability, content and consistency with tools currently used and corporate practices and laws and revised as needed. Subscriptions to security alert services may help ensure up-to-date knowledge of recently identified vulnerabilities and exposures.

#### A.3.2.4.3 Supporting practices

##### A.3.2.4.3.1 Baseline practices

The following seven actions are baseline practices:

a) Addressing the various roles associated with maintaining a secure systems environment within the cyber security training curriculums.

b) Having classroom courses or on-the-job training to address the requirements for each role.

c) Validating a user's understanding via course evaluations and/or examinations.

d) Having subject matter experts for each course who can provide additional information and consulting.

e) Reviewing and validating the training curriculum periodically and evaluating its effectiveness.

f) Communicating key messages to all personnel in a timely fashion via a security awareness communication program.

g) Training all personnel initially and periodically thereafter (for example, annually).

While none of these baseline practices are specific to IACS security training, the emphasis and content for the training programs needs to show the relationship between IACS security and HSE consequences.

##### A.3.2.4.3.2 Additional practices

The following seven actions are additional practices:

a) Establishing cyber security training as a component of the company's overall training organization for all employees.

b) Tailoring the cyber security training curriculums with a progression of material for a given role in the organization.

c) Maintaining and reviewing records of employee training and schedules for training updates on a regular basis depending on their position/role.

d) Leveraging cyber security training provided by vendors.

e) Establishing the timing, frequency and content of the security awareness communication program in a document to enhance the organizations' understanding of cyber security controls.

f) Including an overview of the security awareness communication program for all personnel to ensure they are aware of the security practices on their first day.

g) Reviewing the training and the security awareness program annually for its effectiveness, applicability, content and consistency with tools currently used and corporate practices.

#### A.3.2.4.4 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [2], [23], [24], [26].

### A.3.2.5 Element: Business continuity plan

#### A.3.2.5.1 Description of the element

A business continuity plan identifies procedures for maintaining or re-establishing essential business operations while recovering from a significant disruption. The purpose of the business continuity plan is to provide a course of action to respond to the consequences of disasters, security failures and loss of service to a business. A detailed business continuity plan ensures that business critical IACS systems can be restored and utilized as soon as possible after the occurrence of a significant disruption.

#### A.3.2.5.2 Scope of the business continuity plan

Before developing the business continuity plan, it is important to understand when the plan should be used and what kinds of situations apply. Unplanned interruptions may take the form of a natural disaster (that is, hurricane, tornado, earthquake or flood), an unintentional man-made event (that is, accidental equipment damage, fire or explosion or operator error), an intentional man-made event (that is, attack by bomb, firearm, vandalism, hacker or virus) or an equipment failure. From a potential outage perspective, this may involve typical time spans of minutes or hours to recover from many mechanical failures to days, weeks or months to recover from a natural disaster. Because there is often a separate discipline that deals with reliability and electrical/mechanical maintenance, some organizations choose to define business continuity in a way that excludes these sources of failure. Since business continuity also deals primarily with the long-term implications of production outages, some organizations also choose to place a minimum interruption limit on the risks to be considered. For the purposes of IACS cyber security, it is recommended that neither of these constraints be made. Long-term outages (disaster recovery) and short-term outages (operational recovery) should both be considered. The plan also includes other aspects of disaster recovery, such as emergency management, human resources, and media or press relations.

Because some of these potential interruptions involve man-made events, it is also important to work collaboratively with the physical security organization to understand the relative risks of these events and the physical security countermeasures in place to prevent them. It is also important for the physical security organization to understand which areas of a production site house IACS that might pose higher-level risks.

#### A.3.2.5.3 The business continuity planning process

Prior to creating a plan to deal with potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. System recovery involves the recovery of all communication links and IACS capabilities and is usually specified in terms of a recovery time objective or the time to recover these links and capabilities. Data recovery involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a recovery point objective or the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential interruptions should be created and the recovery procedure developed and documented. For most of the smaller scale interruptions, repair and replace activities based on a critical-spares inventory may prove adequate to meet the recovery objectives. In other cases, contingency plans need to be developed. Due to the potential cost of these contingency plans, these should be reviewed with the managers responsible for business continuity planning to verify they are justified.

The requirements for a business continuity team should be identified and a team should be formed. The team should include IACS and other industrial operations owners. In the event of a significant disruption, this team should determine the priority of critical business and IACS systems to re-establish operations.

A schedule to test all or part of the recovery procedures should be developed. Often the procedures for a specific subsystem are tested annually and the specific subsystem is rotated so the overall system procedures are eventually tested over a 5-10 year period. These frequencies are only examples and shall be determined by the organization as part of the planning process.

Particular attention should be given to verifying backups for system configuration data and product or production data. Not only should these be tested when they are produced, the procedures followed for their storage should also be reviewed on some frequency to verify that the backups and the supporting data are usable and accurate. These backups should be kept under environmental conditions that will not render them unusable and in a secure location where they can be quickly obtained by authorized individuals when needed.

In the event that an incident occurs, the organization may be required to provide forensic data about the incident to investigators, whether inside or outside the organization.

Over time, the business continuity plan will need to be reviewed and revised to reflect changes in the management structure, organization, business model, industry, and the like.

#### A.3.2.5.4 Supporting practices

##### A.3.2.5.4.1 Baseline practices

The following nineteen actions are baseline practices:

a) Forming a business continuity team involving the key stakeholders in the organization (that is, business owners, IT personnel and IACS personnel) to develop the plan.

b) Determining the priority of critical business and IACS based on the nature of the system and the time required for restoration. This depends on the organization's risk tolerance and recovery objectives.

c) Determining the amount of time/resources required for system restoration, location of backup files, hardware, frequency of backups, need for hot spares, and the like, to ensure critical systems can be restored in the event of a disaster situation.

d) Requiring that the records related to the document management and backup/recovery procedures be readily available in multiple ways from multiple locations (that is, electronic copies stored in a vault and paper copies on-site and in a protected facility) so that there is no single point of failure.

e) Considering the possible impact on third parties such as joint ventures and supply chains.

f) Determining the need for additional business insurance.

g) Defining the specific roles and responsibilities for each part of the plan. Some organizations divide the team into sub-teams reporting to a coordinating committee. Examples of sub-teams include damage assessment, restoration and recovery, communications (internal and external) and emergency response.

h) Assigning the responsibility for initiating the business continuity plan and clearly define the circumstances under which to activate the plan.

i) Detailing under what circumstances to take specific emergency measures. The choice of measures varies according to the specific scenario. Consider the consequences of an IT or IACS disaster having physical impact to production facilities.

j) Defining the type, number and identity of the resources needed and their assignments.

k) Detailing the communications methods for the team members along with contingencies for loss of email, phone disruption, and the like in the event of a large-scale disaster.

l) Defining the frequency and method to test, validate and assess the continuity plan and using these results to improve and update the plan for increased effectiveness.

m) Detailing the risks associated with operating under the continuity plan and how they are going to be addressed and/or mitigated.

n) Identifying data that requires special handling and protection, as well as the information that is critical to continued operation.

o) Establishing interim procedures to continue minimum business operations. A reduced product slate may be appropriate during this interim period.

p) Identifying and storing backup systems (hardware, software and documentation) in a safe location.

q) Testing backup systems on a predefined schedule for proper operation of the system and correct restoration of the data.

r) Identifying and/or storing supplies to support the emergency response team and aid in restoring business operations (for example, bottled water, detoxification showers and emergency air packs or respirators).

s) Defining the process for resuming normal operations.

#### A.3.2.5.4.2 Additional practices

The following nine actions are additional practices:

a) Prioritizing IT systems and IACS by their consequence to the business or operation based on the organization's risk tolerance. The IACS may have impact on the business IT systems that might be overlooked without collectively examining and prioritizing the systems as a whole. Disaster planning and recovery plans should address the interrelationship of these systems.

b) Locating critical system backups in different geographic areas. If this is not feasible, storing backup data and equipment in an area not subject to the same physical disaster as the primary system (that is, high ground for floods or concrete bunker for tornadoes).

c) Testing and updating business continuity plans periodically or as needed.

d) Tying business continuity plans to a management of change system ensuring an update to the business continuity plan in the event of significant changes in system or business consequence.

e) Testing communications plans periodically or as needed and assigning responsibility to keep call lists up-to-date.

f) Providing critical contact information to the core team (a card carried by each team member).

g) Having each person of the team keep written copies of the plan at home.

h) Having procedures and/or contracts in place to purchase additional hardware, software and supplies if needed. It is important that the continuity plan balances the replacement times for IACS with the replacement times for the equipment being controlled. In some cases, this equipment may have long lead times for repair/replacement that greatly exceed the replacement time of the control systems.

i) Establishing advance service level agreements with providers of a disaster recovery service.

#### A.3.2.5.5 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [37], [48], [51].

### A.3.2.6 Element: Security policies and procedures

#### A.3.2.6.1 Description of element

Within each management system, there are sets of overall requirements to be met by the system and lists of the organizations that are subject to these requirements. In this standard, those requirements are referred to as policies. There are also descriptions of how individuals and organizations meet the requirements in the management system. In this standard, these descriptions are referred to as procedures.

For a CSMS, policies provide high-level guidance on requirements for cyber security within the organization. They contain directives that address how an organization defines cyber security, operates its cyber security program and addresses its tolerance for risk. The policies for the CSMS are created from higher-level corporate policies from which they derive their authority. Policies carry with them negative consequences for lack of compliance, possibly including termination of employment or even criminal prosecution.

Procedures provide the detail on how the CSMS policies are implemented within the organization. They may not be as strict as policies and may include provisions to obtain exceptions since it is very difficult to craft procedures to deal appropriately with every possible situation or contingency.

The CSMS policies and procedures written by the organization should give personnel a clear understanding of their roles and responsibilities in securing the organization's assets.

#### A.3.2.6.2 Developing security policies

Developing security policies for the organization should not be approached as a linear task. After the initial stages of policy development have been completed, it is necessary for the organization to review and analyze the effectiveness of those policies, then refine them as necessary. These policies should not be developed in isolation from other risk management systems in the organization.

Developing and implementing security policies involves senior leadership commitment from all areas of the organization with responsibility for these types of systems. By defining and endorsing a security policy, senior leadership can demonstrate a commitment to continuous improvement. Leadership commitment relating to security policies involves organization leadership recognizing security policy as a business responsibility shared by all members of the management team and as a policy that includes physical and cyber components. The security procedures need to be incorporated into the overall business strategies and have management support.

Many IACS organizations have existing policies in place for systems such as safety, physical security, IT and employee behavior. When beginning the process of developing a CSMS, it is important to try and integrate the cyber security policies in that system with existing policies and procedures. This may and often does, require the modification of policies within those other risk management systems. For example, existing risk management systems may have already characterized the risks or established risk tolerance levels that need to be understood when developing the new CSMS. An explanation of combining policies and risk management systems can be found in IEC/TS 62443-1-1, 5.6. Security policies that deal with IACS risks will also deal with a wide range of issues from organizational leadership requirements to technically detailed system configuration requirements. It is recommended that these policies be separated into appropriate subgroups to make them more accessible to readers who may only be interested in specific topics.

In many circumstances the security policies and procedures can be thought of as countermeasures to address risk. These can take several forms from administrative procedures to automated security tools. The objective is to make the overall cost of the countermeasures less than the overall impact of the risk. Reducing the cost to implement the countermeasures while still achieving the same level of risk reduction provides more value to the organization. In cases where this economy of scale exists, the IT discipline will manage the technologies where the scale can be leveraged. Thus, the detailed security policies of the IT discipline shall be examined for potential reapplication in the IACS space.

When developing cyber security policies, it is important to consider the conformance and compliance requirements and the audit process as well. Since the IACS will need to be evaluated for its compliance with the security policies, it is necessary to make sure that the policies defined do not conflict with other, possibly more important risk management policies. For example, a security policy is created requiring all desktop computers to be password protected at a certain nuclear facility. This blanket policy also requires all operator stations in the control room to be password protected, but these operator stations are required to be open due to safety regulations. The password policy for desktop computers would cause the system to be out of conformance to HSE policies. The cyber security policy should have originally been written considering the effect it would have on all the different systems at a particular facility. A better approach would be to define a policy that states that desktop computers to be protected from unauthorized use and then have procedures that may require password protection in some instances while providing physical isolation in other situations.

#### A.3.2.6.3 Determining the organization’s tolerance for risk

An organization should define a Risk Tolerance policy related to risk levels, corresponding to a particular combination of likelihood and consequence. This policy can be based on a qualitative risk assessment consisting of a list of assets or scenarios with an overall likelihood and a consequence ranking, which are defined and assigned as part of the organization’s risk assessment process (see A.2.3).

In the typical risk level matrix example shown in Table A.3, likelihood and consequence have both been broken down into three levels. The risk level has also been broken down into three levels. The risk levels in each block (High, Medium and Low) correspond to a particular combination of likelihood and consequence. An organization defines a Risk Tolerance policy related to each level, which will correspond to a particular level of corporate response to the risk. For example, risks that merit a High might be resolved within 6 months; risks that only merit a Low will not have any effort devoted to them; and Medium Risk Level items will deserve intermediate effort. In other words, the organization has stated it can tolerate a High-level risk for 6 months and no longer.

#### A.3.2.6.4 Reviewing and revising cyber security policies

The cyber security policies should be reviewed regularly, validated to confirm that they are up-to-date and being followed and revised as required to ensure that they remain appropriate. Where the cyber security policies are at a higher level, they should not need to be updated as often since they describe what instead of how. While the how of the procedure may change with new threats or techniques, the reason for protecting the system will remain relatively constant.

#### A.3.2.6.5 Deploying cyber security policies

During the creation of cyber security policies, the method for deploying them should be defined. For example, security policies could be published on the corporate Intranet and users could be trained on how the policy affects them. The policies are the bedrock of the CSMS, so the system for deployment should be consistent with the implementation of the management system.

#### A.3.2.6.6 Supporting practices

##### A.3.2.6.6.1 Baseline practices

The following five actions are baseline practices:

a) Establishing management commitment, involvement and support while creating and enforcing cyber security policies.

b) Requiring review and approval by all affected business units and departments, including operations management.

c) Publishing written documents that describe the cyber security policies.

d) Reviewing, validating and revising the policies regularly to confirm that they are up-to-date and being followed.

e) Communicating and disseminating cyber security policies to all personnel.

##### A.3.2.6.6.2 Additional practices

The following ten actions are additional practices:

a) Creating consistent policies with an organization-determined lifecycle. The policies are neither changed constantly, nor are they changed in reaction to hot topics.

b) Creating supporting policies that pertain to specific roles or groups that define how the higher-level policy is implemented for each of these groups. For example, physical access control and password restrictions may not be appropriate in certain industrial control situations. Exceptional procedural safeguards may be required to compensate.

c) Creating security policies to address a number of security concerns, including the mitigation of risks and the changing of staff attitudes towards cyber security.

d) Aligning the security policies with overall organizational policies and strategies.

e) Integrating the cyber security policies with or as a part of an overall security policy that addresses physical elements too.

f) Identifying how the policies are enforced and by whom.

g) Identifying how users need to conform to the provisions of the policies.

h) Providing a consistent policy management framework.

i) Establishing which policies apply to specific users or user groups.

j) Identifying how to measure conformance requirements for the policies.

#### A.3.2.6.7 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [26], [30], [43].

### A.3.3 Element group: Selected security countermeasures

#### A.3.3.1 Description of element group

The second element group within this category is Selected Security Countermeasures. The elements within this group discuss some of the main types of security controls that are part of a well designed CSMS. This document does not attempt to describe the full implementation of any of these selected security countermeasures. It discusses many of the policy, procedure and practice issues related to these particular security countermeasures. Figure A.7 shows a graphical representation of the six elements in the element group:

- Personnel security,
- Physical and environmental security,
- Network segmentation,
- Access control – Account administration,
- Access control – Authentication, and
- Access control – Authorization.

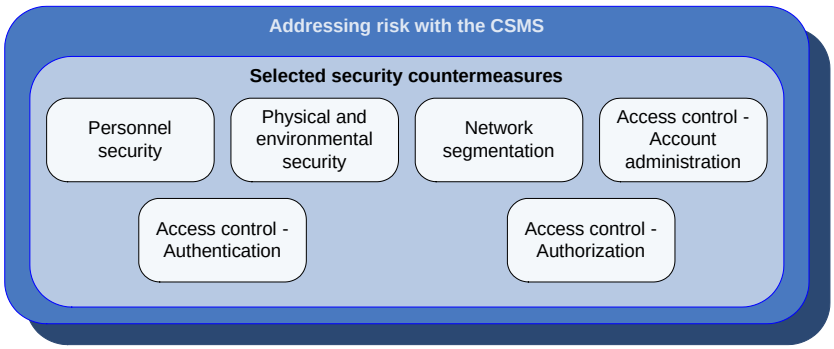



**Figure A.7 – Graphical view of element group: Selected security countermeasures**

A CSMS is the system via which an organization's security countermeasures are selected and maintained. Therefore particular countermeasures are considered as a result of this system rather than as a part of the CSMS itself. However, the countermeasures discussed in this subclause have been included in this standard because their application is fundamental to the formulation of security policy and architecture. For this reason, they should be considered up front during the creation of a CSMS.

### A.3.3.2 Element: Personnel security

#### A.3.3.2.1 Description of element

Personnel security involves looking at potential and current personnel to determine if they will carry out their responsibilities for IACS security in the organization and establishing and communicating their responsibilities to do so. Employees, contractors or temporary personnel that have access to industrial operation sensitive information or the IACS networks, hardware

and software create a potential exposure if sensitive information is revealed, modified or if unauthorized access to IT systems or IACS is granted.

#### A.3.3.2.2 Requirements for personnel security

In many organizations, the personnel security requirements have been driven by concerns about insider threats and the possibility of accidents caused by inattention to detail or by personnel unfit for a job due to lack of proper background or use of substances that might cloud judgment. By implementing personnel security policies it may be possible to reduce these types of problems.

When developing a program for personnel security, it is important to include personnel that can access all systems in scope and not just limit the effort to personnel using traditional computer room facilities.

Computers in IACS operations are tools used to operate the facility productively and safely. It is the personnel that operate the systems that are the heart of the operations and every care should be taken to ensure that these people are qualified and fit for these positions. This process begins at the recruitment phase and continues through termination. It requires constant attention by management and co-workers to ensure that the system is operated in a secure manner.

A personnel security policy should clearly state the organization's commitment to security and the security responsibilities of personnel. It should address security responsibilities of all personnel (both individual employees and the organization) from recruitment through the end of employment, especially for sensitive positions. (This includes employees, prospective employees, contract employees, third-party contractors and company organizations such as human relations.)

All personnel, including new hires and internal transfers to sensitive positions (for example, those requiring privileged access) should be screened during the job application process. This screening should include identity, personal and employment references and academic credentials. Background screenings may also include credit history, criminal activity and drug screening as this information may be useful in determining the applicants' suitability (subject to local Privacy Laws). Third-parties, contractors, and the like are subject to background screening at least as rigorous as employees in comparable positions. Employees and contractors may also be subject to ongoing scrutiny, such as for financial, criminal and drug activities. Due to the amount of industrial operation sensitive data and potential HSE risks in some IACS environments, it may be necessary to screen a wide group of employees who have access to the IACS. Plant-floor employees may need the same level of background checks and scrutiny as a typical IT system administrator. The terms "screening" and "background checks" are left intentionally vague so that the organization can determine the level of screening to be performed on personnel. "Sensitive positions" is also left to be defined by the organization because it is realized that some positions can have little or no effect on the security of the system.

During the hiring process, the terms and conditions of employment should clearly state the employees' responsibility for cyber security. These responsibilities should extend for a reasonable period of time after employment ceases. While hiring contractors or working with third-party personnel, their security responsibilities should be documented and included in any agreements. Where possible, the responsibilities should be specific and measurable.

Personnel should be made aware of the organization's security expectations and their responsibilities through clearly documented and communicated statements by the organization. Personnel need to accept their mutual responsibility to ensure safe and secure operation of the organization. Organizations may consider having all personnel of information processing facilities sign a confidentiality or nondisclosure agreement. Any confidentiality agreements should be reviewed with and signed by employees as part of the initial employment process. Third-party contractors, casual staff or temporary employees not

covered by a formal nondisclosure agreement should also sign a confidentiality agreement prior to beginning work.

Organizations should create job roles based on the segregation of duties to ensure that access to information is on a need-to-know basis and high-risk operating steps require more than one person to complete. These duties should be segregated amongst personnel to maintain the appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the IACS. The security roles and responsibilities for a given job should be periodically reviewed and revised to meet the changing needs of the company.

All personnel should be expected to remain vigilant for situations that may lead to safety or security incidents. Companies need to train managers to observe personnel behavior that may lead to theft, fraud, error or other security implications. A disciplinary process for cyber security violations should be established and communicated to personnel. This should be tied to the legal and punitive measures against such crimes in the country.

#### A.3.3.2.3 Supporting practices

##### A.3.3.2.3.1 Baseline practices

The following eight actions are baseline practices:

a) Screening personnel during the recruitment phase, such as background checks prior to hiring or movement to sensitive jobs, especially for sensitive positions.

b) Scrutinizing personnel, especially those in sensitive positions, on a regular basis to look for financial problems, criminal activity or drug problems.

c) Communicating the terms and conditions of employment or contract to all personnel stating the individual's responsibility for cyber security.

d) Documenting and communicating the organization's security expectations and personnel responsibilities on a regular basis.

e) Requiring personnel to accept their mutual responsibility to ensure safe and secure operation of the organization.

f) Segregating duties amongst personnel to maintain the appropriate checks and balances.

g) Requiring all personnel to sign a confidentiality or nondisclosure agreement.

h) Establishing a disciplinary process for personnel who have violated the security policies of the organization.

##### A.3.3.2.3.2 Additional practices

The following two actions are additional practices:

a) Creating job roles based on the segregation of duties to ensure that access to information is on a need-to-know basis and high-risk processing steps require more than one person to complete.

b) Documenting the security responsibilities and including them in job descriptions, contracts or other third party agreements.

#### A.3.3.2.4 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [2], [23], [26], [30], [43].

#### A.3.3.3 Element: Physical and environmental security

##### A.3.3.3.1 Description of the element

Physical and environmental security relates to creating a secure environment for the protection of tangible or physical assets (that is, computers, networks, information and operations equipment) from damage, loss, unauthorized access or misuse. Physical and environmental security of information systems is a well-established discipline that draws knowledge and experience from other areas of physical or facilities security. Physical and environmental security measures should be designed to complement the cyber security measures taken to protect these assets.

Physical and environmental security measures are different, but linked since they both try to protect the assets of an organization from threats. Physical security measures ensure that the assets of an organization are protected physically from unauthorized access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organization are protected against environmental conditions that would make them unusable or damage the information they contain.

Although cyber security policies and procedures are important for the proper protection of information and control systems, in order to have truly effective protection, they should be complemented by the appropriate level of physical security. For example, maintaining tight controls such as authentication and access control does little to protect system integrity if it is possible to enter a facility and physically remove or damage electronic media.

##### A.3.3.3.2 Considerations for physical and environmental security

###### A.3.3.3.2.1 General

In many organizations, the environmental and physical perimeter security requirements have been driven by concerns about only the physical assets of the organization and may not fulfill the cyber security requirements. Due to the integration of multiple organizations within specific sites (that is, business partners, contractors and third-parties), additional physical security protection for IACS assets may be required. In IACS facilities, physical security is focused more at protecting IACS assets than it is to the operations information itself. The concern is not so much the actual theft or corruption of the computing and control devices, but rather the impact this would have on the ability to sustain production in a safe manner.

When developing a program for physical security of assets, it is important to include all systems in scope and not just limit the effort to traditional computer room facilities. IEC/TS 62443-1-1 discusses criteria that can be used to determine which physical assets should be considered in the scope of the CSMS.

Computers comprising the IACS are tools used to operate the facility productively and safely. They are a means to the end as well as the asset that is to be protected. In some cases, safety and/or productivity is threatened by locking equipment behind doors because the response time to access the equipment may be increased.

Practical engineering judgment balancing all risks should be used to determine the physical security procedures for the assets to be protected. Although it is common practice to locate routers and other network equipment in locked environments, it may be of limited value to expand this practice much beyond this level. Field devices (that is, valve actuators, motor starters and relays) are usually given the ability to be actuated directly in the field without control signals over the IACS network. It can be cost-prohibitive to protect each field device individually, so strong physical perimeter access procedures are usually needed in facilities that involve a high risk.

The following list contains items that should be considered when creating a secure environment for the protection of tangible assets from physical damage due to physical intrusion or environmental conditions.

#### A.3.3.3.2.2 Security policy

A written security policy contains directives that define how an organization defines security, operates its security program and reviews its program to make further improvements. These written policies allow personnel to clearly understand their roles and responsibilities in securing the organization's assets. The organization needs to establish a physical and environmental security policy that is complementary to both the organization's cyber security policy and its physical security policy. The primary objective is to bridge any gaps that might exist between these two policies. The physical and environmental security policy should be consistent with and follow the same policies, as discussed earlier, as other security policies dealing with the security of the control system. A physical security detailed risk assessment is used to determine the appropriate physical security procedures to be implemented.

#### A.3.3.3.2.3 Security perimeter

Critical information or assets should be placed in a secure area protected by security perimeters and entry controls. These physical security controls work in conjunction with cyber security measures to protect information. One or more physical security perimeters should be established to provide barriers for unauthorized access to facilities. Multiple perimeters may be nested to provide successively tighter controls. An example may be locked cabinet inside a control room with key card access within a facility with a guarded perimeter fence.

#### A.3.3.3.2.4 Entry controls

At each barrier or boundary, appropriate entry controls should be provided. These entry controls may be things like locked gates, doors with appropriate locks or guards. The entry controls should be appropriate to the level of security required in the area secured by the entry controls and relative for the need for quick access.

#### A.3.3.3.2.5 Environmental damage protection

Assets need to be protected against environmental damage from threats such as fire, water, smoke, dust, radiation and impact. Special consideration should be given to fire protection systems used in areas affecting the IACS to make sure that the systems responsible for protecting the facility offer protection to the IACS devices without introducing additional risk to the industrial operation.

#### A.3.3.3.2.6 Security procedures

Personnel need to be required to follow and enforce the physical security procedures that have been established to reinforce the entry and other physical controls. Personnel should not circumvent any of the automated entry and other physical controls. An example of an employee circumventing a physical control would be to have an entry door to a protected control room propped open with a chair.

#### A.3.3.3.2.7 Single points-of-failure

Single points-of-failure should be avoided when possible. Redundant systems provide a more robust system that is capable of handling small incidents from affecting the plant or organization, for example, using a redundant power supply in a critical system to ensure that if one power supply is damaged, the critical system will remain functioning.

#### A.3.3.3.2.8 Connections

All connections (that is, power and communications, including I/O field wiring, I/O bus wiring, network cables, inter-controller connection cables, modems, and the like) under the control of the organization should be adequately protected from tampering or damage. This may include putting connections in locked cabinets or within fenced enclosures. The level of physical security for these connections should be commensurate with the level of security for the systems to which they connect. In considering physical security, the consequences of environmental damage should also be considered. These connections should also be

protected against natural factors such as heat, fire, dust, and the like that could cause failures.

#### A.3.3.3.2.9 Equipment maintenance

All equipment, including auxiliary environmental equipment, should be properly maintained to ensure proper operation. Maintenance schedules should be established and preventive maintenance performed. Equipment maintenance should be tracked and trends noted to determine if maintenance schedules should be adjusted.

#### A.3.3.3.2.10 Alarms

Proper procedures should be established for monitoring and alarming when physical and environmental security is compromised. Personnel should be required to respond to all alarms with the appropriate response measures. All facilities, commensurate with their security level, should be alarmed for both physical and environmental intrusions. These may include motion detectors, cameras or door alarms for physical intrusions and fire alarms, water detectors or temperature sensors for environmental concerns.

#### A.3.3.3.2.11 Equipment lifecycle

Proper procedures should be established and audited with respect to the addition, removal and disposal of all equipment. Proper asset tracking is a good practice. These procedures would include workstation disposal, format, clean drive, and the like. The procurement of hardware would also take into account how the equipment can be tracked and how it can be sanitized and disposed when the time comes that it is no longer needed.

#### A.3.3.3.2.12 Physical information

All information, expressed in a physical form (that is, written or printed documents, magnetic storage media and compact disks), needs to be adequately protected against physical threats. This may include placing these items in locked rooms or cabinets to prevent unauthorized access. Consideration should also be given to protecting the information from environmental damage such as magnetic fields, high humidity, heat or direct sunlight, and the like that could damage the information. Like those for equipment, procedures should be in place to securely dispose of physical media when no longer needed.

#### A.3.3.3.2.13 Use of assets outside controlled environments

Special care should be taken when using assets that affect the IACS outside of the IACS network. This includes staging the assets at a system integrator facility prior to installation. Also, assets like laptop computers with access to the IACS network used off-site should be handled as an extension of the IACS network with all of the appropriate physical and environmental security procedures being followed. Consideration should be given to using the same level of security for assets that are temporarily outside of the normal security boundaries. This may require special planning or facilities to protect these assets against unauthorized access or use or from environmental damage.

#### A.3.3.3.2.14 Interim protection of critical assets

During and following either a physical or environmental event, power or other service may be lost to critical systems. Provisions should be made to protect these critical systems. This could include such things as supplying backup power, covering or damming to prevent water damage, and the like.

### A.3.3.3.3 Supporting practices

#### A.3.3.3.3.1 Baseline practices

The following nine actions are baseline practices:

a) Establishing physical security perimeters to provide barriers for unauthorized access to facilities. At each barrier or boundary, appropriate entry controls are provided.

b) Protecting assets against environmental damage from threats such as fire, water, smoke, dust, radiation and impact.

c) Requiring personnel to follow and enforce the physical security procedures that have been established to reinforce the entry and other physical controls.

d) Requiring redundant sources of power to prevent single points-of-failure.

e) Protecting all external connections from tampering or damage.

f) Maintaining all equipment, including auxiliary environmental equipment, to ensure proper operation.

g) Establishing procedures for monitoring and alarming when the physical and/or environmental security is compromised.

h) Establishing and auditing procedures with respect to the addition, removal and disposal of all assets.

i) Using special procedures to secure assets that affect the IACS outside of the IACS network.

#### A.3.3.3.3.2 Additional practices

The following seven actions are additional practices:

a) Using security cables, locked cabinets, protected entrances at the home office, keeping equipment out of sight and labeling and tagging assets.

b) Using password settings for boot and login commands on computers not in the control room, encrypted file system, laptops using thin-client techniques, and the like.

c) Protecting computer equipment not in control rooms such as routers or a firewall by placing them in a locked environment.

d) Having control rooms staffed continuously. This can often be the first line of defense in physical protection. Use control rooms to house information and technology assets.

e) Requiring personnel who are leaving the organization to return the equipment in good working order.

f) Using an equipment tracking system to determine where equipment is located and who has responsibility for the equipment.

g) Requiring environmental protection for assets including proper housing for equipment that is located where it may be subjected to dust, temperature extremes, moisture, and the like.

#### A.3.3.3.4 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [2], [23], [27], [31].

### A.3.3.4 Element – Network segmentation

#### A.3.3.4.1 Description of element

Network segmentation involves separating key IACS assets into zones with common security levels in order to manage security risks to achieve a desired target security level for the zone. Network segmentation is an important security countermeasure employed in conjunction with other layers of defense to reduce the risk that may be associated with IACS.

Today's IACS are connected to and integrated with business systems both within and between partner companies. Despite the need for connectivity and tight integration, IACS do not need to utilize the vast majority of data traversing corporate networks. Exposing the IACS devices to all this traffic increases the likelihood of a security incident within the IACS. In keeping with the principle of least privilege and need to know, IACS should be architected in a

manner that filters/removes unnecessary communication packets from reaching the IACS devices. Network segmentation is designed to compartmentalize devices into common security zones where identified security practices are employed to achieve the desired target security level. The goal is to minimize the likelihood of a security incident compromising the functional operation of the IACS. Compartmentalizing devices into zones does not necessarily mean isolating them. Conduits connect the security zones and facilitate the transport of necessary communications between the segmented security zones.

The overriding security premise is that the use of security countermeasures should be commensurate with the level of risk. Network segmentation of an IACS may not be necessary if the security risks are low. The risk management and implementation element provides additional information on the subject of managing risk. It should be reviewed prior to implementing a network segmentation countermeasure strategy discussed in this element of the CSMS.

#### A.3.3.4.2 Network segments and zones

##### A.3.3.4.2.1 General

IEC/TS 62443-1-1, Clause 6 introduces reference models and provides the context for discussing this countermeasure. Networks are segmented through the use of some sort of a barrier device that has the ability to control what passes through the device. On Ethernet based networks running TCP/IP, the most common barrier devices in use are firewalls, routers and layer 3 switches. Frequently, IACS are comprised of several different networks employing different physical and application layer technologies. These non-TCP/IP networks also employ barrier devices to separate and segment communications. The barrier devices may be standalone gateways or integrated into the network interface module of an IACS device.

While placing a barrier device into the network may create a new network segment and security zone, a security zone also may encompass multiple network segments. Figure A.8 below illustrates a possible segmented architecture for a generic IACS. This figure attempts to depict how functional equipment levels may translate into the physical world of an IACS and the logical world of a zone. (The figure is fairly high level and does not include all the network devices required in an actual installation.)

It is important to not confuse the functional levels of the reference model with security levels associated with security zones. While it is generally true that the lower level equipment plays a greater role in the safe operation of the automated industrial operation, it may not be practical or possible to employ a segmentation strategy aligned one-for-one with the equipment levels.

In this figure, the control zone contains equipment with a common target security level. The figure depicts a TCP/IP-based process control network (PCN) segment, a proprietary regulatory control network (RCN) segment and a proprietary field device network (FDN) segment. These networks link the Level 0, 1, 2 and 3 equipment shown in the reference models of IEC/TS 62443-1-1, 5.2. The barrier devices for each of these network segments regulate the communication entering and leaving their segment.

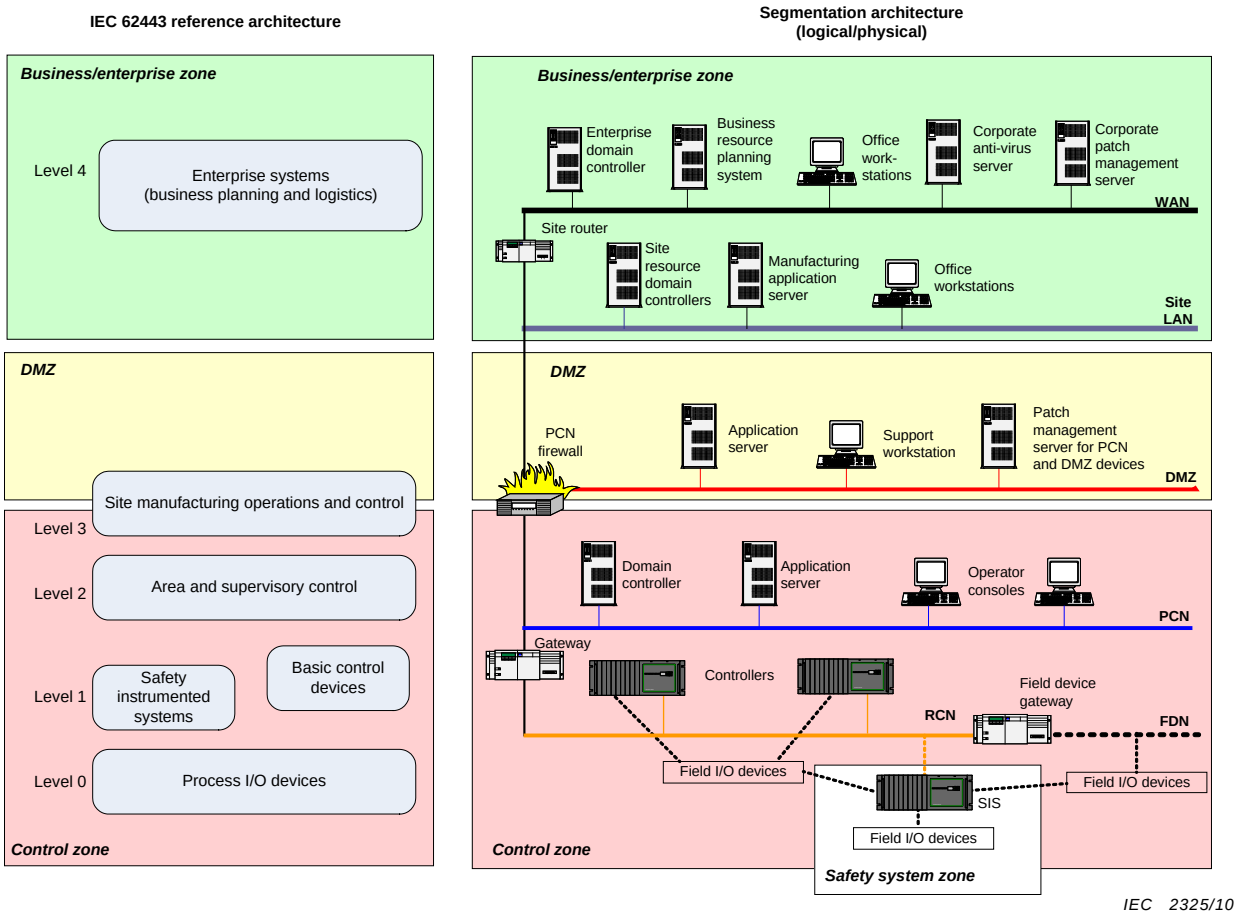



**Figure A.8 – Reference architecture alignment with an example segmented architecture**

### A.3.3.4.2.2 Control zone

For low-risk IACS, it may not be necessary to employ network segmentation as a countermeasure, which would require creation of a distinct control zone. However for medium- to high-risk IACS, network segmentation is a countermeasure providing very significant risk reduction.

The generally accepted good practice is to use a barrier device such as a firewall to manage the communication across the conduit that links the control zone to the business zone, as shown in Figure A.8.

Common filtering strategies at the barrier device include:

a) The base configuration of the barrier device should be to *deny all* communication by default and only allow communication by exception to meet a critical business need. This applies to both intermittent, interactive user communication across the conduit and continuous, task-to-task communication between devices in these two zones. Whenever possible, communications should be filtered by ports and services between matched IP pairs for the devices communicating over the conduit.

b) Ports and services frequently used as attack vectors should not be opened through the barrier device. When the service is required due to business justification, extra countermeasures should be employed to compensate for the risk. As an example, inbound http, which is a common attack vector, may be necessary to support an important business function. Additional compensating countermeasures such as blocking inbound scripts and the use of an http proxy server would help lessen the risk of opening this high risk port and service.

c) The fewer the number of ports and services open through the barrier device the better. Communication technologies that require a large number of ports to be open should be avoided.

The barrier device can serve as a good automated tool to enforce that security practices be followed in the control zone, such as not allowing inbound email or communications to/from the Internet.

#### A.3.3.4.2.3 Demilitarized zone (DMZ)

For high risk IACS, the use of a DMZ in conjunction with a Control zone offers additional risk reduction opportunities between the low-security level Business zone and the high-security level control zone. The security level for the DMZ is higher than the Business zone but less than the control zone. The function of this zone is to eliminate or greatly reduce all direct communication between the control zone and the business zone.

Devices should be located in the DMZ that function as a bridge or buffer between devices in the business zone and control zone. Communication is setup between a device in the business zone and the DMZ. The device in the DMZ then passes along the information to the recipient device in the control zone. Ideally the ports and services employed between the device in the business zone and the DMZ are different from the ports and services used between the DMZ device and the destination control zone device. This reduces the likelihood that malicious code or an intruder would be able to negotiate the combined conduits connecting the business zone to the control zone.

The filtering strategies listed above for the control zone are also applicable for the DMZ. However, some riskier protocols like telnet may be allowed to facilitate management of devices in the DMZ and control zones.

There are several use cases where a DMZ can be of benefit. These are included here to illustrate the security concepts. They are not meant to be an exhaustive or detailed list of how to implement a DMZ:

a) Minimizing the number of people directly accessing control zone devices.

   Historian servers are often accessed by people located on the site LAN in the business zone. Rather than locating the historian server in the control zone and allowing direct access to this device from the business zone by a large number of users, the security level of the control zone can be maintained at a higher level if the historian server is located in the DMZ.

b) Providing greater security for important IACS devices.

   In the case of the historian server mentioned above, an option would be to locate the historian on the site LAN where the majority of the users are located. This would reduce the number of people needing to access the PCN. However, since the business zone is a low-security level zone, the historian server would be subjected to a less secure environment. The potential for compromise of the server would be greater.

c) Compensating for patching delays.

   The DMZ offers additional security protection to important IACS devices that cannot be patched as quickly while waiting for patch compatibility testing results from the application vendor.

d) Providing improved security for the control zone by moving management devices to a higher security level.

   The DMZ is a good place to locate devices like anti-virus servers and patch management servers. These devices can be used to manage deployment of security modules to the control zone and DMZ devices in a more controlled manner without subjecting the high-security level control zone to direct connection to servers that may be communicating to hundreds of devices.

#### A.3.3.4.2.4 Safety system zone

Some IACS may employ a set of safety interlocks that are relay-based or microprocessor-based. A microprocessor-based logic solver SIS may require a slightly different set of security practices from that employed in the control zone. The target security level for this zone should be determined and appropriate actions taken to ensure appropriate countermeasures are employed to meet the target security level.

#### A.3.3.4.2.5 Isolated IACS

The risk associated with the IACS may be too great to allow any opportunity for compromise by an external agent. A facility may choose to disconnect all conduits between the control zone and any other zone. This is a very valid network segmentation strategy for consideration.

Facilities choosing to adopt this isolation approach are not automatically eliminating all risk. There may still be much vulnerability that could be exploited locally. Appropriate layers of cyber and physical protection should be employed to address the residual risk remaining after isolation of the IACS from the business zone.

### A.3.3.4.3 SCADA segmentation architecture

The above discussion described a segmented architecture for an IACS typically found in a single operating facility. Segmentation is a countermeasure that has equal applicability for a SCADA-type IACS. Figure A.9 illustrates one possible segmentation approach for this type of architecture. Although not shown due to space constraints, the DMZ and safety system zone described in the single operating facility IACS can also be employed in a SCADA architecture.

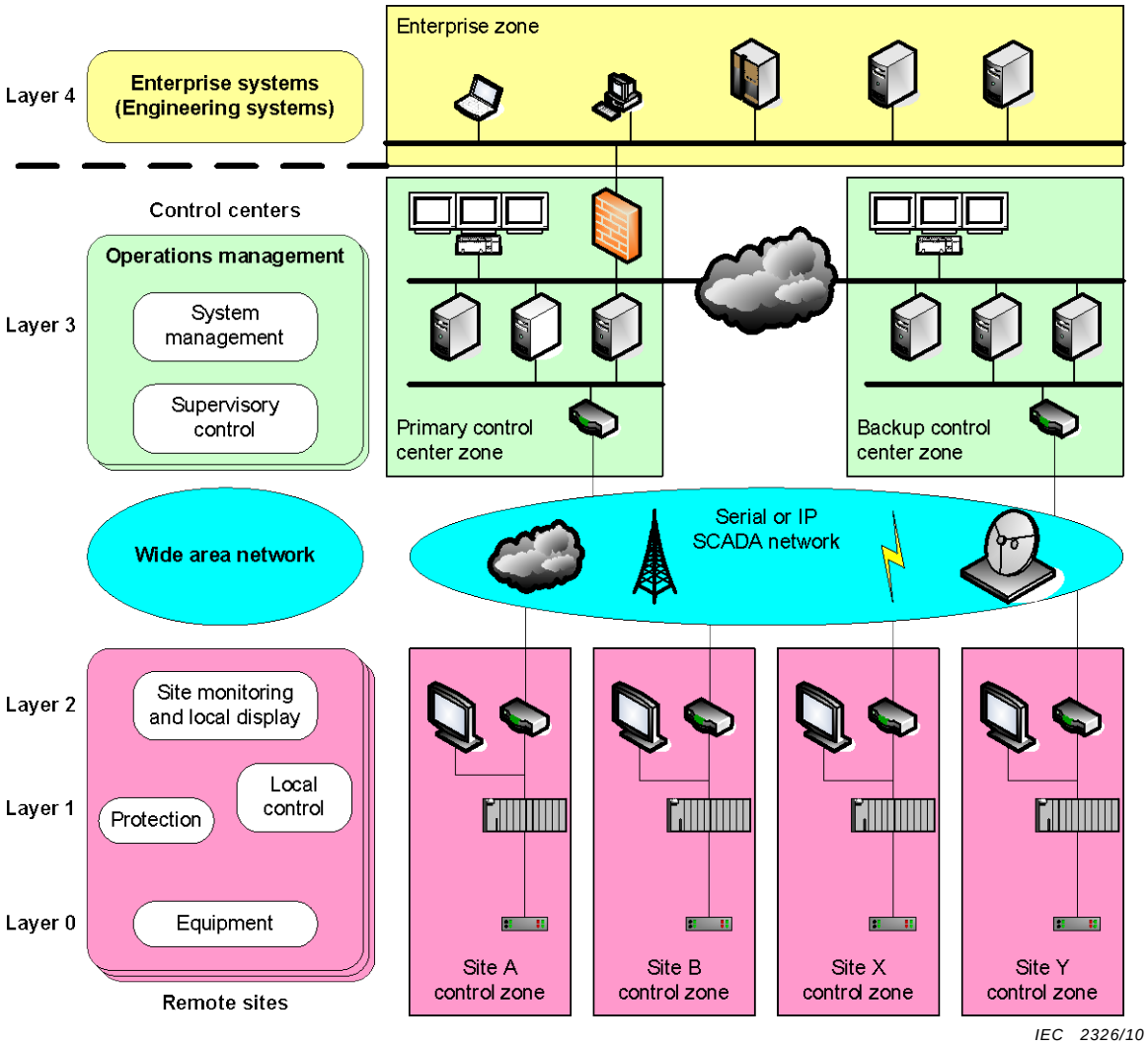



**Figure A.9 – Reference SCADA architecture alignment with an example segmented architecture**

#### A.3.3.4.4 Suggested practices

##### A.3.3.4.4.1 Baseline practices

The following four actions are baseline practices:

a) Employing barrier devices such as firewalls to segment high-risk IACS devices into control zones.

b) Employing gateways or internal barrier devices within the IACS device to separate regulatory control networks from the PCN.

c) Employing sound change management practices on the barrier device configuration.

d) Disconnecting high-risk IACS from the business zone.

##### A.3.3.4.4.2 Additional practices

The following four actions are additional practices:

a) Employing add-on, supplemental barrier devices within the control zone to further segment the network.

b) Employing a common and centrally managed security profile on all control zone barrier devices.

c) Employing a DMZ segmentation architecture.

d) Performing automated assessment tests to verify that the barrier device configuration has been correctly implemented per the design specification.

#### A.3.3.4.5 Resources used

This element was based in part on material found in the following reference, which is listed in the Bibliography: [1].

### A.3.3.5 Element: Access control: Account administration

#### A.3.3.5.1 General description of access control

Access control is the method of controlling who or what resources can access premises and systems and what type of access is permitted. The misuse of data and systems may have serious consequences, including harm to human life, environmental damage, financial loss and damage to the corporate reputation. These risks are increased when personnel have unnecessary access to data and systems. It is very important that the security policy that defines the access control rules and procedures is clearly documented and communicated to all personnel (that is, employees, joint ventures, third-party contractors and temporary employees).

One of the most important security elements for any computer system is having a sound and appropriate set of access control procedures. There are three key aspects associated with access control: Account administration; Authentication; and Authorization.

Each of these is described separately in their own element subclause of this standard. However, all three aspects need to work together to establish a sound and secure access control strategy.

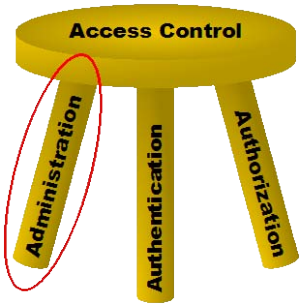
Within each of the three aspects of access control, rules should be established to confirm that a user's access to systems and data is controlled. The rules generally should be applied to roles or groups of users. They should have access to systems and data that are required to meet defined business requirements but should not have access if there is no defined business purpose for it.

There are rules that are enforced administratively and those that are enforced automatically through the use of technology. Both kinds of rules need to be addressed as part of the overall access control strategy. An example of an administrative rule that an organization might have is the removal of employee's or contractor's account after their separation from the organization. An example of a technology enforced rule is requiring remote users connecting to the corporate network to utilize a VPN.

In addition to rules, there are both physical security procedures and cyber security procedures that work together to establish the overall security framework for the system. Physical security procedures include such measures as locking rooms where user interface equipment is located. This standard provides a basic description of the parts of physical security that relate to cyber security in A.3.3.3.

There is both a real-time aspect to access control and an off-line aspect. Quite often, insufficient attention is paid to the off-line activities of access control for IACS. The off-line activity, here described as Account administration, is the first step in the process and includes defining the user privileges and resource needs for the user. These are based upon the role of the user and the job to be performed. The off-line method also includes an approval step by a responsible party before the access account is configured to provide the proper access.

#### A.3.3.5.2 Description of element




IEC 2327/10

**Figure A.10 – Access control: Account administration**

Account administration, one of the three legs of access control as shown in Figure A.10, is the method associated with initially setting up permission and privileges to access specific resources on the network or system and to review those permissions and privileges on a periodic basis. It may be linked in some way to the physical access to resources. Account administration in the IACS environment goes beyond the traditional IT definition of operating system account access for a particular user. In the IACS environment, access accounts are more role-based for the functions they can perform on a particular machine rather than the data they can access. A user's role may change in an organization over time, so the administration process may be used more frequently on IACS accounts. Privileges often include access to file directories, hours of access and amount of allocated storage space. The role assigned at the application level for the access account shall be identified and understood during the administration phase. Several steps are involved which include identification of the resources needed to perform that person's job function, independent approval by a trusted person and setup/configuration of the computer account that automatically assigns the resources when requested.

In addition to the task of creating access accounts and assigning users to roles at the operating system level, many manufacturing applications require additional role assignments. System administrators for IACS shall be skilled and trusted to perform these account administrative functions on live equipment control applications. The change management process for making these account changes should clearly identify any timing constraints that shall be followed due to the safety risks during certain sequences of the control operation.

#### A.3.3.5.3 Considerations for account administration

##### A.3.3.5.3.1 General

When developing a program for account administration, it is important to include all systems in scope and not just limit the effort to traditional computer room facilities.

##### A.3.3.5.3.2 Rules to control a user's access to systems, data and specific functions

Each organization should establish rules to control a user's access to the systems, data and functions. These rules should be based on the risk to the system and the value of the information. These rules should be conveyed to all personnel.

##### A.3.3.5.3.3 Standard administration process

A standard administrative process should be followed for the creation of access accounts. Although it may be more cost efficient for a single organization to provide the account administration function for all computer systems in a company, IACS and IT systems may have different sets of people providing administrative control of the account creation and maintenance process. This is often due to the different set of risks associated with these systems. Account approvals may also require approval by a supervisor familiar with the IACS tasks and operations.

#### A.3.3.5.3.4 Role based access accounts

A standard administrative process should be followed for the creation of access accounts. The accounts should be role based and grant the user only those privileges and access to resources that are needed to perform their particular job function.

#### A.3.3.5.3.5 Minimum privileges

Users should be assigned the minimum privileges and authorizations necessary to perform their tasks. Access should be granted based on the need to support a particular job function. The role-based privileges should consider special requirements for installing software, requirements for configuring services, file-sharing needs and remote access needs.

#### A.3.3.5.3.6 Separation of duties

The account administration process includes principles of separation of duties with separate approvers and implementers of account configuration. This principle provides an additional layer of protection so that one person cannot compromise a system alone.

#### A.3.3.5.3.7 Identify individuals

Every user should be identifiable with separate access accounts unless there are HSE risks for such accounts. In such cases, other physical security controls should be employed to limit access. Access needs to be controlled by an appropriate method of authentication (that is, user ID and password, personal identification numbers (PINs) or tokens). These personal credentials should not be shared except in certain special situations. One special case is in a control room where the operators function as a single work team or crew. In this situation, everyone on the work team may use the same credentials. (Additional discussion is provided on this subject in A.3.3.6.). An alternate identification process should exist in the event of a forgotten password.

#### A.3.3.5.3.8 Authorization

Access should be granted on the authority of an appropriate manager (either from the responsible company or a partner organization). Approvals should be made by supervisors familiar with the manufacturing/operations tasks and the specific training a person has had for that role.

#### A.3.3.5.3.9 Unneeded access accounts

Access accounts are the means of controlling access to the system, therefore, it is important that these accounts be inactivated, suspended or removed and access permissions revoked as soon as they are no longer needed (for example, job change, termination, and the like). This action should be taken by the appropriate manager as soon as possible after the access account is no longer needed.

#### A.3.3.5.3.10 Review access account permissions

The need for access to critical systems is explicitly reconfirmed on a regular basis. All established access accounts should be reviewed periodically to ensure that the account is still in use, their role and access needs are still correct, the user is still authorized and only has the minimum required permissions. Inactive or unneeded accounts should be removed. If an access account remains unused for an extended period, the need for it is explicitly confirmed by the account owner and account sponsor.

#### A.3.3.5.3.11 Record access accounts

One of the primary functions of account administration is the recording of the individual access accounts. Records should be maintained of all access accounts, including details of the individual, their permissions and the authorizing manager.

#### A.3.3.5.3.12 Change management

The change management process for account administration should clearly identify any timing constraints that shall be followed due to the safety risks of making changes during certain industrial operation sequences. These changes are treated with as much importance as are process, software and equipment changes. The access account administration process should integrate with standard process safety management (PSM) procedures and include approval and documentation steps. The approvers of access accounts for manufacturing/operations functions may be a different set of people than are approving users for the IT systems. Approvals should be made by supervisors familiar with the manufacturing/operations tasks and the specific training a person has had for that role.

#### A.3.3.5.3.13 Default passwords

Many control systems come with default passwords that are used in getting the system set up and ready for operation. These access account passwords are often widely known or easily determined from published literature or other sources. These default passwords should be changed immediately upon setup and before connection to the system.

#### A.3.3.5.3.14 Audit account administration

Periodic reviews for compliance of access account administration information should be conducted. This ensures that the owners of the information or documents are compliant with the appropriate policies, standards or other requirements set down by the organization.

### A.3.3.5.4 Supporting practices

#### A.3.3.5.4.1 Baseline practices

The following nine actions are baseline practices:

a) Assigning the minimum privileges and authorizations to users necessary to perform their tasks. Access should be granted on the basis of the need to perform a particular job function.

b) Controlling identification and access for each individual user by an appropriate method of authentication (for example, user ID and password). These personal credentials (that is, passwords, PINs and/or tokens) are not shared except in certain special situations.

c) Establishing an alternate identification process in the event of lost credentials or a forgotten password.

d) Granting, changing, or terminating access on the authority of an appropriate manager (from the organization, contracting organization, or third-party). A record is maintained of all access accounts, including details of the individual, their permissions, and the authorizing manager.

e) Suspending or removing all access accounts and revoking permissions as soon as they are no longer needed (for example, job change).

f) Reviewing all established access accounts on a regular basis to ensure that they are still in use and they still require access to critical systems.

g) Reconfirming the need for access accounts with the appropriate manager if the accounts are unused for an extended period of time.

h) Requiring default passwords to be changed immediately.

i) Requiring all personnel (that is, employees, joint ventures, third-party contractors, and temporary employees) to agree in writing to conform to the security policy, including access control policies.

#### A.3.3.5.4.2 Additional practices

The following five actions are additional practices:

a) Using tools (that is, provisioning and identity management) to manage the process of access account creation, suspension, and deletion. A provisioning system also manages the approval workflow by which the business owner approves access, including logging. It may also automate the process of account creation/suspension on the target systems.

b) Linking the account administration process to the human resources process so that employee changes trigger reviews and updates to access accounts.

c) Defining and documenting the application roles/user privileges (that is, job functions mapped to application roles and access entitlements for each role) by the application information owner or delegate.

d) Paying special attention to users with privileged access (that is, more frequent reviews and background checks).

e) Allowing users to have more than one access account, based on their particular job-role at that particular time. A person would use a system administrator access account to perform an application update on a particular machine but would also need an operator access account to run and test the application.

#### A.3.3.5.5 Resources used

This element was based in part on material found in the following reference, which is listed in the Bibliography: [6].

### A.3.3.6 Element: Access control: Authentication

#### A.3.3.6.1 Description of element

NOTE For additional information about the overall topic of Access control, see the introductory material in A.3.3.5.1.

Authentication, another of the three legs of access control as shown in Figure A.11, is the method of positively identifying network users, hosts, applications, services, and resources for some sort of computerized transaction so that they can be given the correct authorized rights and responsibilities. The method uses a combination of identification factors or credentials. Authentication is the prerequisite to allowing access to resources in a system.

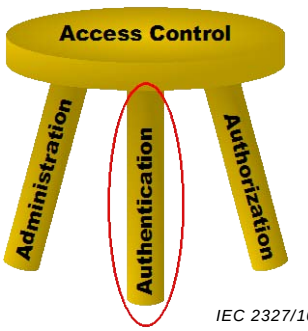



**Figure A.11 – Access control: Authentication**

Authentication in the IACS environment has several challenges not typically found in normal IT situations. Current IT authentication technologies have several limitations that are not well suited for the IACS environment and could actually result in increased HSE risks at the expense of decreased cyber security risks.

It is important in the IACS environment to make sure that the right people have access to the correct information and systems and are not prevented from doing their job via authentication. Failure to authenticate a valid user could have HSE implications if the user is not able to perform tasks in a critical situation. In the IACS environment, there is a great emphasis on combining physical authentication measures with electronic authentication practices.

The physical location of the user may have a significant impact on the risk level of the access. For example, the user connecting to a system from inside a building that employs a guard and badge-reader system at the door is less of a risk than a user connecting from some other region in the world. The authentication strategy addresses the combined physical and cyber security controls to be used to control overall risk. The strategy clearly defines the authentication requirements for special situations.

There are several types of authentication strategies and each has varying degrees of strength. Strong authentication methods are ones that are quite accurate in positively identifying the user. Weak authentication methods are ones that can be easily defeated to provide unwanted access to information.

The physical location of the user may have a significant impact on the risk of accessing the IACS. Authentication for these cases will be discussed in the following subclauses.

#### A.3.3.6.2 Authentication for local users

It is very important that only trained and designated resources take actions on industrial control HMI stations, such as operator control stations. Many industries control their equipment from control rooms staffed by several operators. These operators often function as a team and perform actions on multiple HMI stations as part of their normal job function. Common access accounts shared by the team of operators are frequently employed. Until cost-effective, robust, strong authentication schemes are available on the HMI stations, the recommended practice is to use physical controls to ensure that only designated individuals are performing actions on control room HMI stations. Access to control rooms should be managed by appropriate combinations of entrance control technologies and administrative procedures. Consider the HSE implications when developing the access control procedures.

#### A.3.3.6.3 Authentication for remote users

A remote user is anyone who is outside the perimeter of the security zone being addressed.

EXAMPLE A remote user might be a person in an office in the same building, a person connecting over the corporate wide area network (WAN) or a person connecting over public infrastructure networks.

Physical and administrative controls that rely on visual authentication do not work for remote interactive users. However, there are numerous technology-based authentication schemes that can be used. It is important to employ an authentication scheme with an appropriate level of strength to positively identify the remote interactive user. Industrial operations with a low potential to create HSE incidents and that have low financial impact may be protected using weak authentication methods such as a simple user ID and password. However, industrial operations where there is a large financial or HSE stake should be protected using strong authentication technologies. For these types of operations, it is recommended that the system be designed in a way that the remote access user is not allowed to perform control functions, only monitoring functions.

#### A.3.3.6.4 Authentication for task-to-task communication

The discussion above focused on interactive users. It is just as important to employ appropriate authentication schemes for task-to-task communication between application servers or between servers and controlled devices. The communications interface should employ methods to verify that the requesting device is indeed the correct device to perform the task. Some ways in which critical interfaces could authenticate task-to-task communications between devices are checking the internet protocol (IP) address, checking the media access control (MAC) address, using a secret code or using a cryptographic key to verify that the request is coming from the expected device. Interfaces with low risk may use less secure methods for authentication. An example of insecure communications is an anonymous file transfer protocol (FTP) for program upload/download/compare between the control HMI and a data repository.

#### A.3.3.6.5 Considerations for authentication

##### A.3.3.6.5.1 General

When developing a program for access control, it is important to include all systems in scope, and not just limit the effort to traditional computer room facilities.

a) Defining an authentication strategy

Companies should have an authentication strategy or approach that defines the method of authentication to be used.

b) Authenticating all users before system use

All users should be authenticated before using the requested application. This authentication may be a combination of physical and cyber authentication practices.

c) Requiring strong secure accounts for system administration and/or application configuration

Strong account user ID and password practices should be used on all system administrator and application configuration access accounts. The system administrator does not typically need quick access to perform system-level tasks on the computers. It is more important that untrained users be prevented from performing system-level functions than it is to provide quick access.

d) Requiring local administration

On highly critical systems, it is a good practice to perform all system administrator or application configuration functions locally at the device to reduce the potential for a network interruption causing a problem with the control of the equipment. The system administrator or application manager should coordinate all changes with the operator for the area so that production is not impacted during a configuration change.

##### A.3.3.6.5.2 Authentication for local users

If a practice introduces the potential to delay an operator's ability to locally make quick corrective action to the industrial operation from the HMI control station, normal IT authentication practices may not be appropriate. To achieve security in control system operation while still providing for rapid response, a combination of physical and cyber controls have been found to produce the best results. Some of these controls include but are not limited to:

- manual locks (for example, key and combination) on doors to rooms or cabinets containing control system components;
- automated locks (for example, badge and card readers);
- control rooms staffed continuously;
- individual accountability by control room personnel to keep access limited to designated personnel and ensure that only trained personnel perform actions on operator control stations.

Some examples of common IT practices that may *not* be applicable in an IACS environment are:

a) Individual user IDs and passwords for each operator for work-team environments

Many industries control their operations from control rooms staffed by several operators. These operators often function as a team and perform actions on multiple HMI stations as part of their normal job function. Requiring each operator to log in and be authenticated and authorized each time they use a new HMI could compromise quick response to an operation event.

b) Access to non-local domain controllers and active directory servers for access account authentication

Network issues may interfere with timely login under this architecture.

c) Automatic access account lockout after some number of failed login attempts

Under some conditions that require rapid response by an operator, the operator may become flustered and enter the wrong password. If the operator is then locked out, it could compromise the operator's ability to resolve the situation.

d) Robust long passwords that contain a mix of alpha, numeric and special characters

Although robust passwords provide an increased measure of security, in the control room environment, the requirement to enter such passwords could slow response time for an operator. A similar level of security could be achieved by physical means such as locked doors or continuous staffing of the control room by those that know cleared operators.

e) Password changes after a specified number of days

The impact of changing passwords is much like that of robust passwords, it may slow response to a situation when a quick response is needed. Passwords should be changed when there is a change in personnel, but changing after a set number of days may not be productive.

f) Screen savers with password protection

Many HMI stations are designed to report by exception. The operator may not need to take any action on the operator station until an alert occurs. Screen savers have the potential to interfere with the operator by blocking the view to the operation under control and delaying response to an emergency situation.

#### A.3.3.6.5.3 Authentication for remote users

Remote users do not normally need to rapidly respond to situations common to operators. In addition, for remote users, accountability becomes more important than availability. Therefore, some of the practices common to IT security are also of benefit for remote users. These include:

a) Authenticate all remote users at the appropriate level

The organization should employ an authentication scheme with an appropriate level of strength to positively identify a remote interactive user.

b) Log and review all access attempts to critical systems

The system should log all access attempts to critical systems and the organization should review these attempts whether they were successful or failed.

c) Disable access account after failed *remote* login attempts

After some number of failed login attempts by a *remote* user, the system should disable the user's access account for a certain amount of time. This helps deter brute force password cracking attacks on the system. Although remote users do not normally need to respond rapidly to operation situations, there may be instances, such as unmanned control rooms or remote facilities (for example, SCADA systems controlling an electrical distribution system) where rapid access is required from a remote location. In these cases, disabling the access account may not be appropriate. Each organization should address authentication of remote users in a manner appropriate to their situation and tolerance for risk.

d) Require re-authentication after *remote* system inactivity

After a defined period of inactivity, a remote user should be required to re-authenticate before the system can be accessed again. This makes sure that the access account is not left open and accessible from the remote device. Although remote users do not normally need to connect to the control system for long periods of time, there may be instances, such as unmanned control rooms or remote facilities (for example, SCADA systems on an electrical distribution system) where a remote operator may need to monitor the system over an extended period of time. In these cases, requiring re-authentication may not be appropriate. Each organization should address authentication of remote users in a manner appropriate to their situation and tolerance for risk.

For remote users, the level of authentication required should be proportional to the risk to the system being accessed. Weak authentication may be appropriate if the system does not have

control over operations with a high HSE risk. For systems with HSE risks, strong authentication may be more appropriate.

Examples of weak authentication include:

- connecting modems directly to industrial operation control devices or networks that employ simple user ID and password authentication;
- connecting industrial operation control devices or networks from the corporate LAN or WAN that employ simple user ID and password authentication;
- using Microsoft Windows® user ID and password authentication at the application level on industrial operation control devices.

Examples of strong authentication include:

- using Physical token or smart card two factor authentication that requires both a physical device and unique knowledge (for example, a Personal Identifier Number, PIN) in the possession of the user;

  NOTE Security is enhanced by using secure PIN entry, for example, when the PIN is entered using a secure reader to prevent keylogging.
- authenticating using smartcards or biometrics;
- authenticating users based on their location;
- connecting modems to industrial operation control devices or networks that employ a dial-back feature to a predefined phone number;
- connecting industrial operation control devices or networks to the corporate LAN or WAN and using smartcards or biometric authentication;
- connecting home computers to industrial operation control devices or networks using a VPN connection and two-factor authentication with a token and PIN.

#### A.3.3.6.5.4 Authentication for task-to-task communication

Task-to-task communications will not usually be monitored directly like user interactive sessions. Authentication of task-to-task communications will typically happen at the startup of an industrial operation and at regular intervals afterwards. Systems should employ some technical solution to authenticate each device or network.

NOTE IEC/TR 62443-3-1 [6] provides an explanation of these and other technologies. It discusses their strengths and weaknesses and their applicability to the IACS environment.

### A.3.3.6.6 Supporting practices

#### A.3.3.6.6.1 Baseline practices

The following five actions are baseline practices:

a) Establishing a strategy or approach that defines the method of authentication to be used. The method may vary depending on the risks, the consequences associated with the business process and the sensitivity of the data.

b) Employing different strategies for users connecting from different geographical locations (including remote facilities) or for devices with special security requirements. This issue takes into account the physical security characteristics that interact with the cyber security characteristics to establish the overall security level for the user.

c) Authenticating all users prior to being allowed use of a particular application. This requirement may be waived when there are compensating physical controls.

d) Requiring at least a manually entered user ID and password as the minimum level of electronic authentication.

e) Authenticating task-to-task communication by knowing the MAC and/or IP address for the device, a specific electronic key, the device name, and the like.

#### A.3.3.6.6.2 Additional practices

The following action is an additional practice:

a) Authorizing users inside a locked facility that employs guards and badge-readers to access systems having a greater level of risk than a remote user would be allowed.

#### A.3.3.6.7 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [6], [23].

### A.3.3.7 ELEMENT – Access Control: Authorization

For additional information about the overall topic of Access control, see the introductory material in A.3.3.5.1.


**Figure A.12 – Access control: Authorization**

Authorization, the third leg of access control is shown in Figure A.12, is the automated procedure performed by the computer system to grant access to resources upon successful authentication of the user and identification of their associated access account. The privileges granted are determined by the access account configuration set up during the account administration step in the procedure.

Some standard authorization procedures employed in the general IT work space may be inappropriate or inadequate for IACS. For example, access accounts in a typical IT system are primarily user-based with a limited number of roles assigned (that is, standard user or system administrator). Each user is usually only assigned one role. Access accounts in a typical IACS system will primarily be role-based with a greater granularity of roles (that is, operator, engineer, application specialist, vendor and system administrator). Users may be assigned multiple roles based on a particular job function they need to perform at a particular time. The user may have to login to a particular device and separately into an application to be authorized to make changes to industrial automation control variables. Or, a user may have to log off a system and re-login to perform system administration tasks on that same device.

This subclause explores the controls aimed at protecting information and assets from deliberate and inadvertent destruction, change or disclosure. It focuses specifically on measures designed to ensure that the authenticated agents (that is, personnel, applications, services and devices) have access to required information assets.

Information that is sensitive to disclosure needs to be properly protected both to maintain competitive advantage and to protect employee privacy.

The authorization rules desired by an organization will determine how it assigns roles to specific users or groups of users and how privileges for these access accounts are configured. The capability to implement a desired authorization policy depends upon features in underlying systems to distinguish the functions and data required for different job roles.

Thus the definition of an authorization policy is an iterative procedure where the organization defines an ideal policy and then determines how closely that can be implemented using the capabilities of their systems and network. If procuring a new system, support for a desired authorization policy can be an element of the procurement specification. When designing a new network configuration, technologies like firewalls for remote users can be added to create an additional layer of authorization for critical devices, as described in the following paragraphs.

#### A.3.3.7.1 Considerations for authorization

##### A.3.3.7.1.1 General

When developing a program for access control, it is important to include all systems in scope, and not just limit the effort to traditional computer room facilities.

a) Authorization security policy

   Rules that define the privileges authorized under access accounts for personnel in various job roles need to be defined in an authorization security policy that is clearly documented and applied to all personnel upon authentication.

b) Logical and physical permission methods to access IACS devices

   The permission to access IACS devices should be logical (rules that grant or deny access to known users based on their roles), physical (locks, cameras and other controls that restrict access to an active computer console) or both.

c) Access to information or systems via role-based accounts

   Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications are a critical component of role definition.

##### A.3.3.7.1.2 Authorization for local users

Many process industries control their operations from control rooms staffed by several operators. These operators often function as a team and perform actions on multiple HMI stations as part of their normal job function. Authorization to perform specific job functions is provided by the application. The local user is granted access to certain devices or operational displays based upon a role-based access account. The actual login user ID and password are typically common for everyone in the job role. This work-team approach to control room operation may conflict with standard IT authorization policy and practice.

Safety implications shall be considered when developing the authorization strategy. For high-vulnerability industrial operations, authorization privileges should be set at the local process control device level and should not require access to devices at the LAN or WAN level to assign privileges. This supports the basic control principle of minimizing the potential points of failure.

Access accounts should be configured to grant the minimum privileges required for the job role. Training needs to be employed to establish common levels of skills for each of the job roles. Customizing individual access accounts to match skill levels of personnel should be avoided. All users in the same job function should utilize access accounts configured for the same role.

##### A.3.3.7.1.3 Authorization for remote users

The authorization process discussed thus far places the authorization function at the end-node device and application level. In critical control environments, an additional destination authorization strategy should be employed at a barrier device (firewall or router) for the IACS network. Once a user is authenticated at the barrier device, role-based destination access rights should be assigned to the user so that the user can only attempt to connect to pre-assigned devices on the IACS network. The end-node login should establish the user's final privileges for performing functions on the device. Facilities with high-vulnerabilities should take advantage of this additional level of destination authorization.

Role-based access accounts should take into account geographic location. A person may utilize one access account when working on-site and a different one when dialing in from home to assist local personnel. This practice should be clearly defined in the administrative procedures. Compliance with administrative procedures should be based on individual accountability.

#### A.3.3.7.2 Supporting practices

##### A.3.3.7.2.1 Baseline practices

The following two actions are baseline practices:

a) Permitting access to IACS devices with logical controls (rules that grant or deny access to known users based on their roles), physical controls (locks, cameras, and other controls that restrict access to an active computer console) or both.

b) Logging and reviewing all access attempts to critical computer systems, both successful and failed.

##### A.3.3.7.2.2 Additional practices

The following six actions are additional practices:

a) Protecting network connections between the organization and other organizations through use of a managed firewall.

b) Using an authenticating proxy server for all outbound access to the Internet.

c) Granting access to a remote user by enabling a modem on an industrial operations control device only when needed.

d) Using ushered access when high-risk tasks are performed (for example, industrial operations that have HSE consequences or that constitute critical business risks).

e) Segregating data with high sensitivity and/or business consequence from other internal information so that existing authorization controls can restrict access to that information.

f) Separating the business network from the IACS network with an access control device and limiting user access to critical assets on both sides.

#### A.3.3.7.3 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [6], [23], [27], [30], [43].

### A.3.4 Element group: Implementation

#### A.3.4.1 Description of element group

The third element group in this category is Implementation. This element within this group discusses issues related to implementing the CSMS. Figure A.13 shows a graphical representation of the four elements in the element group:

- Risk management and implementation,
- System development and maintenance,
- Information and document management and
- Incident planning and response.

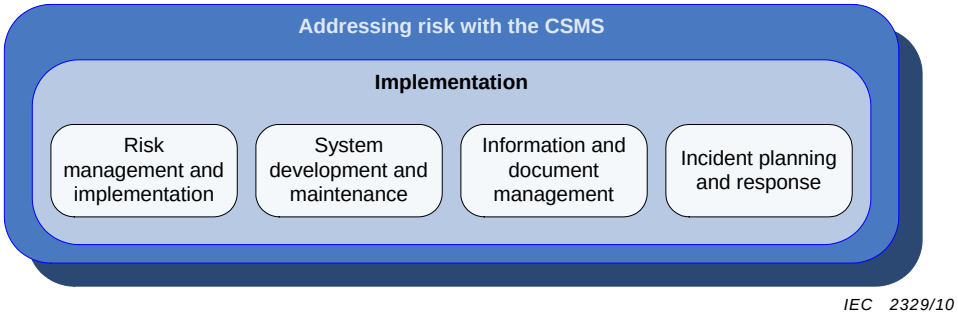



**Figure A.13 – Graphical view of element group: Implementation**

### A.3.4.2 Element: Risk management and implementation

#### A.3.4.2.1 Description of element

The foundation of any CSMS or security program is to maintain risk at an acceptable level. Risk management and implementation addresses the selection, development and implementation of security measures that are commensurate with the risks. The security measures may take into account inherently safer industrial operation design, use of products with strong inherent security capabilities, manual and procedural security countermeasures, and technology based countermeasures to prevent or reduce security incidents.

Although risk will never be totally eliminated, it can be managed. This subclause describes a framework to measure risk and then manage it through the implementation of various security countermeasures to reduce the likelihood of an incident occurring or reduce the consequence of the resulting event.

In most cases risk is measured in terms of cost and or social conscience. While it may be easy to put a price on a production outage due to a cyber security incident, it is not possible to assign an exact cost to an event resulting in the injury or death of a person. Companies shall determine their risk tolerance to certain kinds of events and use this to drive the strategy for managing risk.

#### A.3.4.2.2 Building a risk management and implementation framework

Because the elimination of all risk is usually impractical or impossible, organizations should focus on the most critical applications and infrastructures to decrease risk to an acceptable level. Deciding what cyber security countermeasures to implement is a matter of balancing risk and cost. Decisions should be based on a risk assessment and be documented to serve as a basis for future planning and action.

Organizations should analyze the detailed risk assessment, identify the cost of mitigation for each risk, compare the cost with the risk of occurrence and select those countermeasures where cost is less than the potential risk. Because it may be impractical or impossible to eliminate all risks, focus on mitigating the risk for the most critical applications and infrastructures first. The same risks are often found at more than one location. It makes sense to consider selecting a standard set of countermeasures that may be applicable in more than one instance and then defining when to use them. This approach will allow the organization to leverage common solutions and reduce the design and implementation costs to improve the security posture of the organization. One possible way to approach this is to develop an overall framework for implementation that incorporates risk assessment, the organization's tolerance for risk, countermeasure assessment and selection and the strategy for implementing risk reduction activities.

Each organization will likely have a different risk tolerance that will be influenced by regulations, business drivers and core values. The organization's risk tolerance for IACS incidents determines the amount of effort an organization is willing to spend to reduce the level of risk to an acceptable level. If the organization has a low risk tolerance it may be

willing to commit a greater amount of financial and/or personnel resources to the task of improving the security level of the IACS.

Table A.2 identifies the organization's sensitivity to different types of risk and aggregates the various consequences into categories of high, medium, or low. When these categories of consequences are combined with the likelihood of an incident occurring, as in Table A.1, the result is a matrix of consequence category versus likelihood. In the absence of an analytical method to quantitatively measure likelihood and consequence, it may be practical to simply assign qualitative risk levels of low, medium and high to the points of intersection in the matrix. These risk levels reflect the organization's sensitivity to risk, as shown in Table A.3. These risk levels imply thresholds of tolerance which will drive the risk reduction implementation strategy. This is a clear way to communicate the organization's position on risk.

The risk reduction strategy may employ different countermeasures, architecture practices, IACS device selection and the decisions of when and where to employ them based upon the risk level shown in Table A.3. Systems with a high risk warrant employing more extensive countermeasures to achieve a higher level of security.

One way to capture the organization's decisions on countermeasure selection is to develop a chart listing specific countermeasures to be used for IACS devices based upon the risk-level of the IACS. An example of a possible countermeasure chart is shown in Table A.4.

The table defines the common solution set of countermeasures to be employed to try to reach the target security level. These countermeasures are to be employed unless there is some unique constraint that makes this solution undesirable for a given IACS. The organization's risk reduction strategy may also use the risk-level ratings to establish priorities and timing for implementing the identified countermeasures shown in Table A.4. IACS with high-risk ratings should probably be addressed with greater urgency than lower risk IACS.

The countermeasures to address a specific risk may be different for different kinds of systems. For example, user authentication controls for an advanced application control server associated with a DCS may be different than the authentication controls for the HMI on the packaging line. Formally documenting and communicating the selected countermeasures, along with the application guidance for using the countermeasures, is a good strategy to follow.

**Table A.4 – Example countermeasures and practices based on IACS risk levels**

| Countermeasure and architecture practices | High-risk IACS | Medium-risk IACS | Low-risk IACS |
|---|---|---|---|
| Two-factor authentication to control access to the device | Required | Required | Optional |
| Hardening of the operating system | Required | Recommended | Optional |
| Employ network segmentation | Required | Required | Optional |
| Employ antivirus application | Required | Required | Required |
| Use of WLAN | Not allowed | May be allowed | Allowed |
| Strong password authentication at the application level | Required | Recommended | Recommended |
| Other countermeasures | … | … | … |

There are many different information technology risk mitigation countermeasures that can and should be applied to IACS devices. Guidance on specific countermeasures is addressed in other parts of the IEC 62443 series that are still in development, such as IEC 62443-3-2 [7] and IEC 62443-3-3 [8], which provide an in-depth look at different available countermeasures and their application to the IACS environment.

Most organizations will have a limited set of financial and personnel resources to apply to CSMS activities. As a result, it is important to use these resources in a manner that yields the greatest returns. A risk management framework begins with understanding vulnerabilities that exist within the IACS and the potential consequence that could occur should that vulnerability be exploited. Once risks are understood, the company needs to develop an implementation framework to reduce risk or keep it at an acceptable level. Several of the security models discussed in IEC/TS 62443-1-1 will be used in creating the implementation framework. The models include the Security Level Model along with the Zone and Conduit Model.

NOTE This subclause discusses one possible way to approach this key CSMS element using the IEC/TS 62443-1-1 security models. There is no one right approach to this element. Alternate approaches can result in a very functional framework for managing risk.

The detailed discussion and example that follows on the topic of risk management and implementation describes the framework process as it is applied to reduce cyber security risks to an existing system in a single industrial operating area. The framework is equally applicable to many new IACS in multiple locations around the world.

No matter what detailed risk management and implementation approach is employed, a good quality framework shall address four main sets of tasks over the life of an IACS:

- Assessing the risk of the IACS;
- Developing and implementing countermeasures;
- Documenting countermeasures and residual risk;
- Managing residual risk over the life of the IACS.

These tasks are covered in detail in A.3.4.2.3 through A.3.4.2.5 and are graphically represented in the security lifecycle models discussed in IEC/TS 62443-1-1, 5.11.

#### A.3.4.2.3 Assessing the risk of the IACS to determine the IACS cyber security risk level

##### A.3.4.2.3.1 General

The zone and conduit model, security level lifecycle model, and reference model are described in detail in IEC/TS 62443-1-1. The use and integration of these models will be discussed in this subclause.

A.2.3 provides guidance on a procedure to be followed in order to analyze the risk of the IACS. This is one of the earliest activities in the assess phase of the security level lifecycle model. An organization needs to develop and document a risk analysis process so that it can be used on multiple IACS at different locations throughout the organization with repeatable results.

This subclause explains how the assessment phase fits into the overall risk management strategy. This is illustrated by walking through the scenario of examining an existing IACS and improving the cyber security position of this system to reduce risk. Figure A.14 shows the Security level lifecycle model's Assess phase.

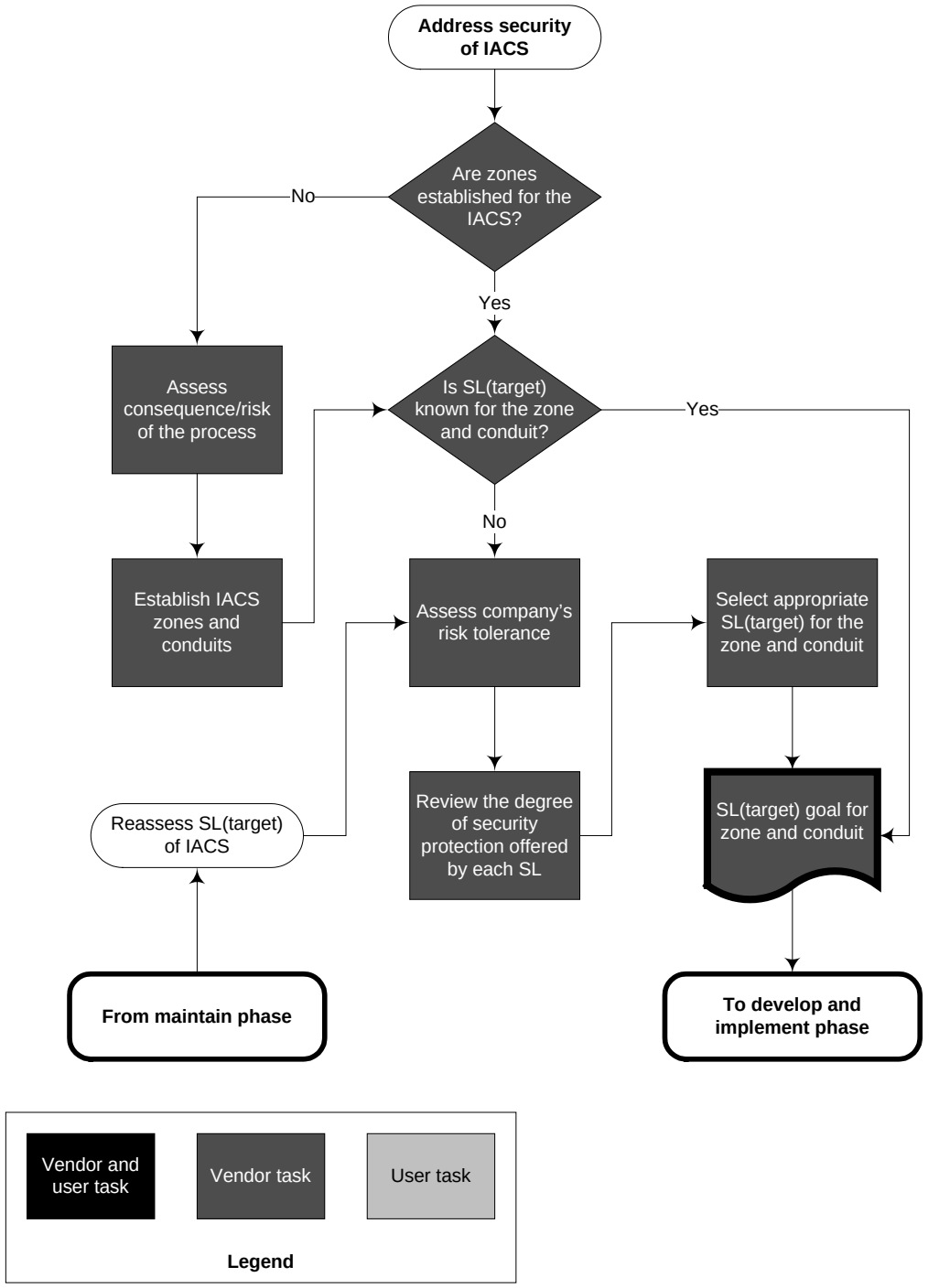



**Figure A.14 – Security level lifecycle model: Assess phase**

For an existing IACS that has never undergone a risk assessment and has not yet employed the Zone model, the activity begins with the box labeled “Assess consequence/risk of the process.”

The purpose of the assessment is to understand the risk impact to the business in the event the IACS is compromised by a cyber incident and is not able to perform its intended control functions or performs unintended functions. Once the risk associated with the IACS has been documented the activities associated with managing and mitigating the risk should be performed.

The output of the risk analysis will be a table listing the consequence rating and likelihood rating for each IACS asset or some collection of assets. Table A.5 is an example output of a

detailed risk assessment and results from combining Table A.1, Table A.2 and Table A.3 of this standard. The likelihood rating is assigned based upon the detailed vulnerability assessment of each of the assets listed, and the likelihood of related threats being realized.

**Table A.5 – Example IACS asset table with assessment results**

| IACS device asset | Consequence rating | Likelihood rating |
|---|---|---|
| Operator control room console | A | Medium |
| Remote operator console | C | High |
| Engineering configuration station | A | High |
| Historian server | B | Medium |
| Controller | A | Medium |
| Gateway | B | Medium |
| Other devices | C | Low |

#### A.3.4.2.3.2 Determining the IACS risk level

Table A.3 above is a simplified example model for translating a company's sensitivity to risk into qualitative levels of risk for the IACS. It should be prepared by the organization's responsible leadership before the risk analysis is conducted.

The intersection of the Consequence and the Likelihood ratings yields the Risk Level.

EXAMPLE An IACS device with a consequence rating of B and a likelihood of High would represent a high-risk device.

The risk postures in Table A.3 can be applied to the IACS device assets in Table A.5 resulting in an overall rating for the IACS as shown in Table A.6. This table provides a priority ordering for particular vulnerabilities.

Each device has a cyber security risk level associated with it. In a tightly integrated IACS, the control functions provided by each device are highly dependent upon the integrity of the other devices in the IACS. The functional integrity of the control system will be impacted by the integrity of the weakest device.

A simplifying security assumption is that the device with the highest IACS risk level establishes the inherent risk level for the entire IACS. In the example IACS listed in Table A.6, the inherent risk level for the IACS is High-risk because several of the IACS devices have a risk level identified as High-risk.

**Table A.6 – Example IACS asset table with assessment results and risk levels**

| IACS device asset | Consequence rating | Likelihood rating | IACS device risk level |
|---|---|---|---|
| Operator control room console | A | Medium | High-risk |
| Remote operator console | C | High | Medium-risk |
| Engineering configuration station | A | High | High-risk |
| Historian server | B | Medium | Medium-risk |
| Controller | A | Medium | High-risk |
| Gateway | B | Medium | Medium-risk |
| Other devices | C | Low | Low-risk |

Understanding this base inherent risk level is a key to carrying out a risk management plan. It establishes the target security level needed to reduce risk. This establishes the justification for implementing a risk reduction and management plan, if the IACS is not already operating

at that target level. Various security countermeasures will be employed to reduce the risk to the IACS to a tolerable level. However, a failure of these countermeasures to mitigate the risk could result in an incident with a consequence of the magnitude identified during the risk analysis task.

#### A.3.4.2.3.3 Establishing security zones and associating IACS devices to the zones

The reference model discussed in IEC/TS 62443-1-1 identifies several different operational or equipment levels of an IACS. Although there may be different operational levels within an IACS, the cyber security requirements may be similar for several of these operational or equipment levels. It may be possible to incorporate several operational/equipment levels into a single logical security zone.

The security level model introduces the concept of employing zones assigned to one of three or more security levels. For illustration purposes in this example, assume there are three security levels qualitatively described as Low, Medium and High. The task at hand is to examine the security needs of the various IACS device assets and assign them to these different zones.

Table A.6 lists the IACS cyber security risk level for each of the assets. Assets with a High-risk level share a need for a high level of cyber protection to reduce risk. These assets should be assigned to a common security zone. Assets with lower risk levels should be assigned to a lower security zone. At this point in the risk management process, it is appropriate to superimpose the identified security zones onto the system physical network diagram developed for conducting the risk analysis.

Given today's security countermeasure technologies, security zones will typically align with physical network segments. An IACS device may not be currently located on the proper network segment based upon the risk analysis results for that device. If this is the case, the device may need to be relocated to a different network segment. An asset with a Low-risk level may be assigned to a higher risk security zone, but assets with a High-risk level should not be placed into a lower risk security zone. To do so would raise the risk of an unacceptable consequence in the event of a cyber security incident.

During the implementation phase of the security level lifecycle model, the devices with security needs that do not match with the zone the devices are physically located in should be relocated to the appropriate network segments to meet the security requirements.

An organization may choose to establish a common approach to security zones in an effort to improve the efficiency of managing risk. One way to do this is to adopt a corporate template architecture incorporating network segmentation strategies and security zones for the various kinds of devices and systems employed in the enterprise. Figure A.15 shows an example of a security zone template architecture for an organization. Figure A.16 shows how the IACS assets in the example are mapped to the zones in the template architecture that employs a three-tier zone approach.

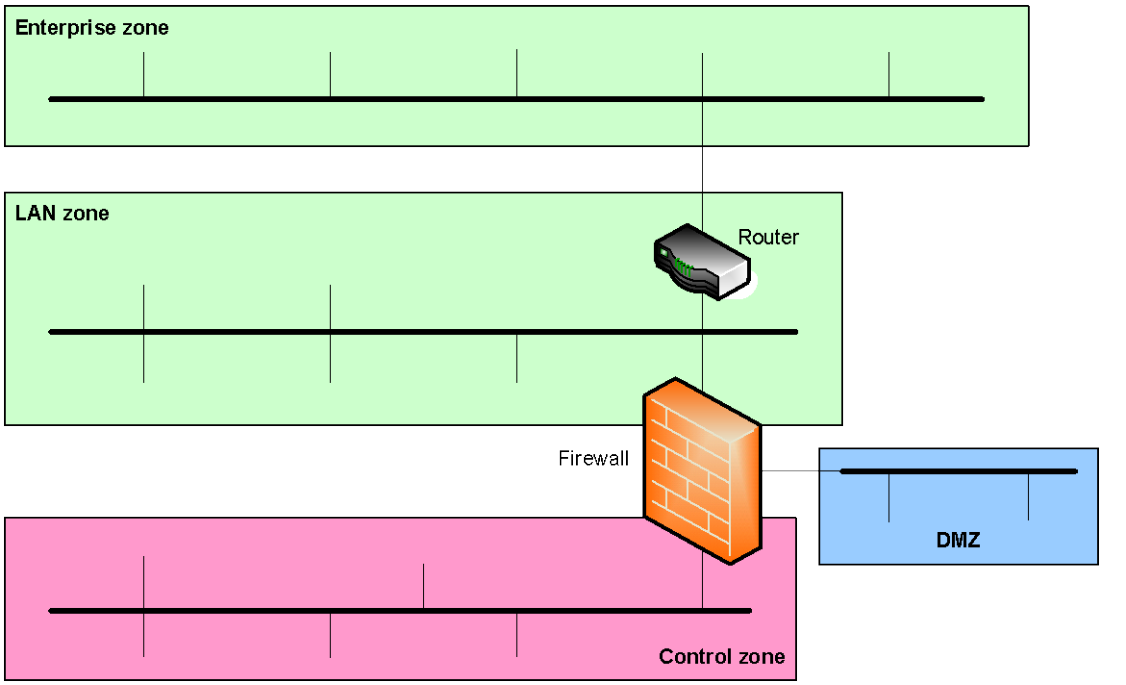



**Figure A.15 – Corporate security zone template architecture**

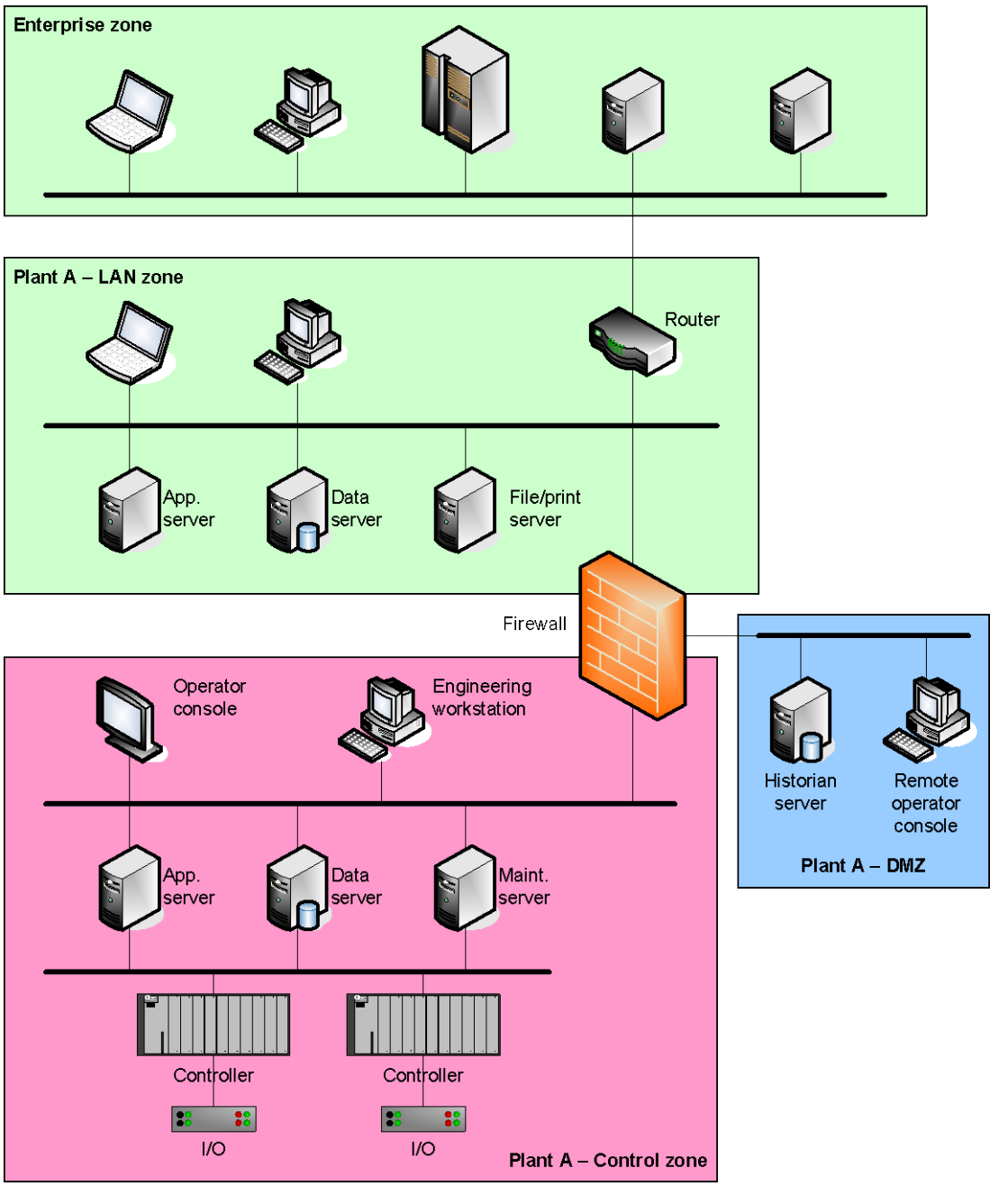



**Figure A.16 – Security zones for an example IACS**

#### A.3.4.2.3.4 Determining the target security level

The security level model introduces the concept of assigning a security level to the zone. In the example shown in Figure A.16 above, the inherent risk level of the IACS was determined to be High-risk based upon the detailed risk assessment of each IACS device. Extra security countermeasures need to be employed to protect the devices falling within the Plant A control zone. Using the security levels listed in IEC/TS 62443-1-1, Table 8, it is appropriate to assign a target security level to each of the zones, as seen in Table A.7.

**Table A.7 – Target security levels for an example IACS**

| Zone | Target security level = SL(target) |
|---|---|
| Plant A control zone | High |
| Plant A DMZ | Medium |
| Plant A LAN zone | Low |
| Enterprise zone | Low |

#### A.3.4.2.3.5 Selecting devices and a system design based upon SL(capability)

The security level capability of each device shall be examined to understand the security strengths and vulnerabilities it introduces to the zone. Although the SL(capability) cannot be quantitatively measured at this point in time, there are some more qualitative means to assess the relative SL(capability) of the devices comprising the IACS. These assessment items are typically covered as part of a detailed vulnerability assessment. For example:

- If the device is a web server, running an assessment tool to identify weaknesses of web server applications and determine if the weaknesses can be remediated.
- Running an assessment tool to identify the number of services and ports required for the application to function on the device.
- Examining the required ports and services to determine if these have been historically used by attackers to exploit system vulnerabilities.
- Examining the operating system of the device and determine if security patches and upgrades are still being supplied for the version in use.
- Running an assessment tool to subject the application to unusual inputs to determine if the device and application will continue to function under abnormal communication streams.
- Examining the exploit history of the underlying technologies used in the device to ascertain the likelihood for future exploits.

The organization should have some acceptance criteria for a device to be used in a particular target security level based upon the results of these assessment tools and identified weaknesses. If the SL(capability) of the device is simply too low to achieve the SL(target) for the zone, an alternate device may need to be selected. For an existing IACS comprised of older generation devices, it may be necessary to replace the device with a newer generation device with improved SL(capability). An example of this might be a PC-based operator control station running on Microsoft Windows® NT as its operating system. The detailed vulnerability assessment results for this device and application may show significant vulnerabilities. The security features built into this older operating system are less than in many of the newer generation operating systems. Additionally, security patches to address these vulnerabilities are no longer being supplied by the vendor. This leaves the device in a relatively weak position with respect to its SL(capability).

The SL(capability) of each new IACS device should be examined to ensure that it supports the goal SL(target) for the zone. Although quantitative measurements of SL(capability) may not be available and/or published, vendors may be able to provide some more qualitative measures based upon assessments they or third-parties have conducted using standard security tools and field trials. These detailed vulnerability assessment results should be considered and used in the decision process for selecting IACS devices.

The preliminary design identifying IACS devices and zone assignments shall be transformed into a detailed design identifying all equipment and network segments to be employed in the IACS. This is the time to relocate devices whose security risk needs do not align with the SL(target) for the zone. The output of this step should be a detailed network diagram locating all IACS and network devices that will be a part of the overall IACS.

#### A.3.4.2.4 Developing and implementing the selected countermeasures for each zone

##### A.3.4.2.4.1 General

The Security level lifecycle model's Develop and implement phase addresses the steps and tasks to reduce risk. The overall concept of this phase is to employ countermeasures to an IACS to achieve the target security level for the zone established during the assess phase. Figure A.17 addresses several different starting points. It applies to implementing a new IACS, making changes to an existing IACS in the form of new equipment, and improving the security of existing IACS. Figure A.17 is a frame of reference to guide thinking rather than a detailed flow diagram or checklist of steps that have to be followed.

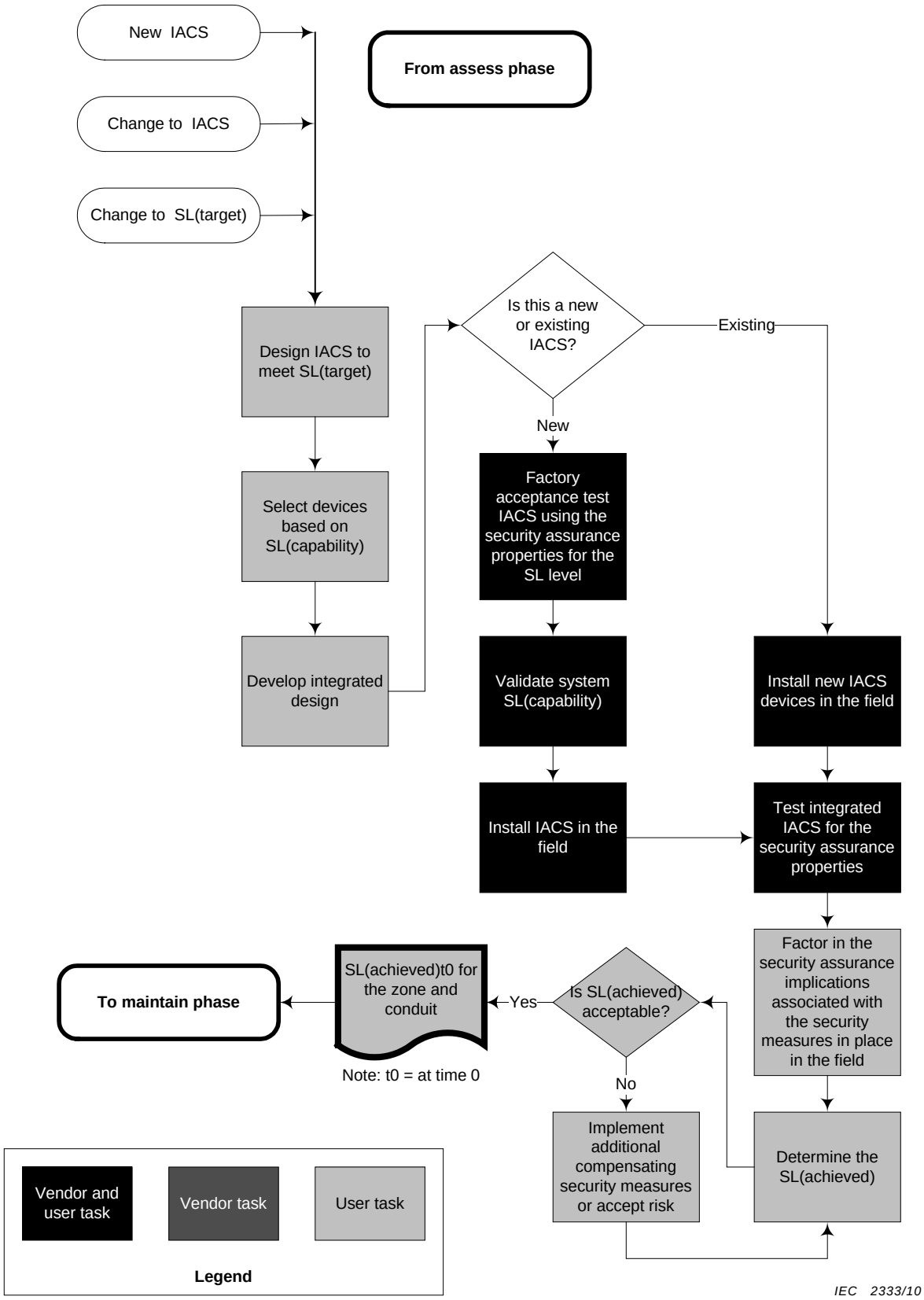



**Figure A.17 – Security level lifecycle model: Develop and implement phase**

The beginning point of this phase is the security goal to be achieved. This is expressed as the security level target for each zone of the IACS. Under the Assess phase these targets were established and preliminary zone assignments made for each of the IACS devices. The task at hand is to take this preliminary approach and create a detailed design for implementation.

#### A.3.4.2.4.2 Offline security testing

Just as functional testing of an IACS is critical to implementing an IACS so that it will meet the needs of the operating facility, security testing of the devices is also important to make sure the operational integrity and robustness will be achieved. A.3.4.3 provides more detailed information on performing security testing.

If the IACS is a new system, security testing should be conducted while the system is in an offline environment. This could be a factory acceptance test at the vendor's location or an offline staging step at the final field location. The location is not as important as making sure the security testing steps are undertaken. While it would be very valuable to security test all devices and countermeasures employed in the final installed state, this may not be affordable and practical. So the testing design should focus more on the SL(capability) of the IACS devices and the countermeasures that are not specific to the installed field location.

The preceding subclause noted several tools and items for consideration for testing SL(capability). These items are typically covered as part of a detailed vulnerability assessment. Security testing should include not only tests to assess the ability to resist typical security threats encountered under operating conditions, but should also include the measures that will be part of ongoing system security support. These include but are not limited to:

- testing the patching process for operating system patches and upgrades;
- testing the patching and upgrade process for IACS vendor updates;
- testing the offline system development environment;
- testing deployment of antivirus software and malware signature updates.

The overall goal of the security testing activities shown in the middle of Figure A.17 above is to validate that the SL(capability) of the devices aligns with the design basis.

#### A.3.4.2.4.3 Field security testing

The items shown on the right side of Figure A.17 above identify the testing activities associated with the final destination environment. This is the point where all the employed countermeasures are tested and/or examined to determine if the achieved security level equals or exceeds the target security level design basis for the zone.

If this is a new IACS being installed it is probably possible to conduct these tests before the IACS is placed online. If the activity is to retrofit and replace an existing IACS device or implement some new security countermeasures to the IACS, it may not be possible to obtain a window of opportunity to do full offline field security testing. Instead the challenge is often implementing the new device or countermeasure and field testing that the basic operating function of the IACS has not been unacceptably impacted by the security measures.

It is important to keep in mind that system performance testing should include system response to normal and abnormal industrial operating type events as well as normal and abnormal security incident type events. These combine to yield an overall measure of the robustness and integrity of the system.

Because each industrial operation is slightly different, it is not possible to identify a cookbook type procedure for this testing. It will require considerable design work to determine the best way to assurance test that the security functions are meeting the security objectives to achieve the Target Security Level.

#### A.3.4.2.4.4 Meeting the target security level

Achievement of the target security level in the field may require some degree of iteration. The field is not a perfect world. Typically it is appropriate to try to apply a common set of countermeasures to all the devices within the zone to achieve the desired security level. A

selected countermeasure identified for implementation on all devices may not be useable on a particular device because of an operational or physical constraint not initially recognized during system security design. Therefore it is important to recognize that real world situations may require the elimination of, as well as the addition of, countermeasures for individual devices within a zone to achieve the proper balance of security benefit versus risk so that all parties involved with the decision process are satisfied.

#### A.3.4.2.4.5 Illustrating the design process using the IACS example

The previous subclauses discussed the principles regarding implementing security countermeasures to meet the SL(target) for the zone. This subclause describes the design process of applying these principles to a real world example.

Table A.6 identified a historian server with a device risk level of Medium. Using the corporate template security architecture, this device was identified as needing to be located in a security zone with a SL(target) of medium or higher. The Plant A DMZ was identified as the appropriate zone for this device even though the device is currently located on the Plant A LAN zone.

In preparation for physical implementation of the Plant A DMZ, the SL(capability) of the historian server is examined to determine if it meets the SL(target). Examination of the vulnerabilities from performing a detailed vulnerability assessment reveals that:

- The operating system for the server is Microsoft Windows® NT, for which security updates are not available.
- No antivirus application is running on the server. The vendor of the historian application has not qualified any antivirus software products as compatible with the historian application.
- The majority of the users of the historian application are located in office areas with PC connections to the lower security Plant A LAN zone.
- Efforts to harden the server by shutting down non-needed tasks were not successful because the historian application vendor would not certify that the application would run properly if the services were shut down.

The conclusion is that the inherent SL(capability) of the historian server is inconsistent with the SL(target) for the Plant A DMZ.

Since the inherent SL(capability) is too low, the use of additional supplementary countermeasures are examined to determine if they can successfully reduce risk to meet the SL(target). Additional countermeasures such as eliminating Internet access, eliminating email, disabling media ports on the server, employing strong passwords are examined. Although these can contribute to risk reduction, it is felt that employment of these additional security practices would not compensate for the low inherent SL(capability) of the historian server.

Since the historian server directly interfaces to the IACS gateway of the regulatory control network, the security weaknesses of this device also lowers the SL(achieved) of the Plant A control zone. The conclusion is that the best way to address these unacceptable SL(achieved) states of both the Plant A DMZ and the Plant A control zone is to replace the present historian server with a newer historian software application running on a currently supported operating system. After examining the SL(capability) of the newer server and historian application to ensure it aligns with the SL(target), the server and application are tested and implemented in the Plant A DMZ during an industrial operation shutdown.

There are some important points worth highlighting in association with this example. The SL(achieved) of a zone is dependent on the SL(capability) of the devices in the zone but also the connectivity within and between zones. A vulnerability analysis for a device considers not only inherent properties of the device considered in isolation, but also the connectivity of this device in the network. This is important because an IACS that uses only devices that have High SL(capability) when considered in isolation may, when considered together, not

necessarily achieve the desired High SL(target) for a zone. For example, a new IACS device employing a new operating system, even if fully patched and running antivirus software, has a lower SL(achieved) when directly connected to the corporate IT network. Conversely, if one limits physical access and network connectivity to a zone, devices of lower SL(capability) might together achieve a higher SL(achieved) for the zone.

The security of the conduit between zones can also impact the SL(achieved) of the zone. For example, a conduit using a wireless communications link rather than a physical cable may have a different SL(achieved) for the conduit and have an impact on the SL(achieved) of the zones joined by the conduit.

Similarly the SL(achieved) of the zone in consideration may be impacted by the security level of the zone connecting to the zone in consideration. In the example, the users of the historian application are in a zone with a lower security level than the historian server. Even if the SL(achieved) of the conduit between these zones is High, the lower SL(achieved) of the Plant A LAN zone can potentially negatively impact the SL(achieved) of the Plant A DMZ.

#### A.3.4.2.5 Maintaining the security levels for each zone

##### A.3.4.2.5.1 General

The level of security of a device is constantly eroding. New security vulnerabilities are discovered nearly every week. During the period of time that vulnerability exploits are known and unmitigated, the IACS may be at risk and the SL(achieved) of the zone is potentially lower than the SL(target). This real-world situation shall be addressed with a plan to maintain the security level of the zone to an acceptable security level.

The Security lifecycle model's Maintain phase, shown in Figure A.18 below, depicts the cyclical set of activities that are critical to sustaining the security of the zone. The triggers to initiating the reassessment of risk include but are not limited to:

- a change to the physical industrial operation or changes to the IACS which could introduce new risks;
- a new vulnerability discovered in a software module used in the IACS;
- the release of a new operating system or application patch which triggers the deployment of exploit code to the Internet;
- scheduled periodic security audits and reviews.

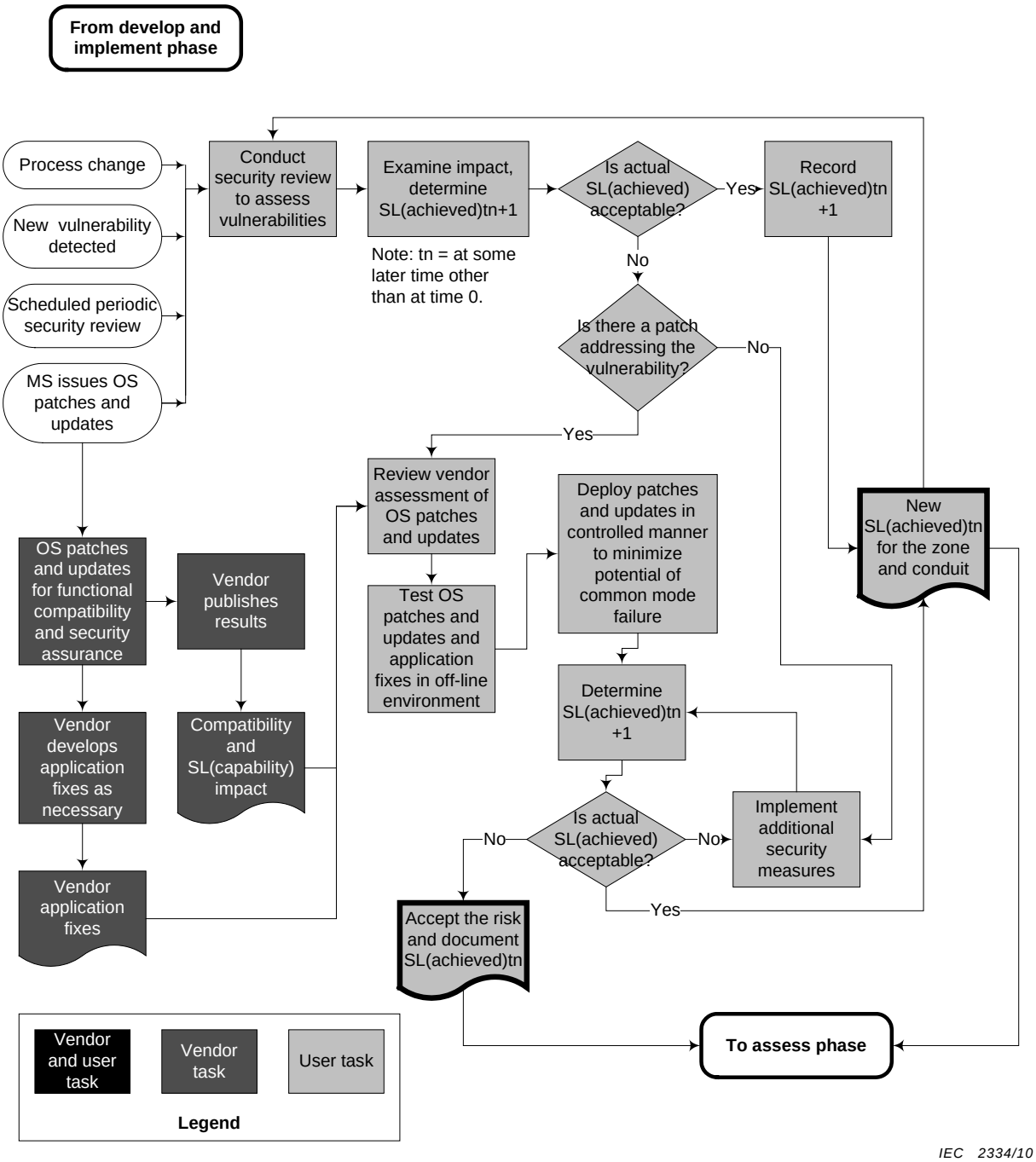



**Figure A.18 – Security level lifecycle model: Maintain phase**

### A.3.4.2.5.2 Patching IACS Devices

Figure A.18 above offers a high-level overview of how patching fits into the maintain phase of the security level lifecycle model. This subclause is not meant to be a comprehensive discussion of all the aspects associated with patching. The goal is to depict the iterative aspect of examining the SL(achieved) state of the zone and the need to make solid decisions about what patches to apply and when to apply them.

Vendors of IACS devices and applications share responsibility with users for addressing security risks. Users count on the vendors to understand the inner workings of their IACS applications, to determine the applicability of the patch and to perform thorough automated regression testing for compatibility of the IACS application with operating system patches and major revision updates. Since installing patches has the potential to interfere with the normal operation of the IACS software application, users need as much assurance as possible that the installation of the revised software will not result in a failure of the control device.

As Figure A.18 indicates, vendor compatibility testing is the first step in a multiphase testing plan before widespread patching is conducted on the running IACS. Additional testing should be conducted with the target environment of the device. Ideally this would be performed on an offline device identical to the live IACS. If this is not possible, alternate approaches should be considered which could include testing in a virtual environment or in a very controlled deployment to the live IACS.

Armed with vulnerability information from the operating system vendor, patch applicability information from the IACS vendor, compatibility information from the IACS vendor, knowledge of the use of the IACS device and finally user testing, the user shall make a decision on field deployment of the patch.

#### A.3.4.2.5.3 Employing additional countermeasures

It may be necessary to employ additional countermeasures to address unmitigated vulnerabilities from patches or vulnerabilities introduced by changes to the industrial operation. This is determined by assessing the SL(achieved) and comparing this to the SL(target) for the zone. As was noted earlier, this is rather subjective rather than being easily measured in good quantitative terms.

In some cases the business risk of taking action to raise SL(achieved) may be cost prohibitive in the short or long term. In this case, the technical decision makers should document:

- the risks;
- the countermeasures employed;
- the countermeasures considered, rejected and reasons why;
- the recommendation to business leaders to accept the risk for some period of time until a more acceptable countermeasure or security solution can be identified, tested and implemented.

Business leaders should formally sign off to document acceptance of this strategy.

#### A.3.4.2.5.4 Scheduled security reviews

A comprehensive CSMS includes a conformance element that should include a periodic assessment that the security practices and countermeasures as identified in the corporate security policy and standards are being employed and are effective in reducing risk to achieve the SL(target) level. This is another trigger to the Security level lifecycle model's Maintain phase.

A security audit may measure the degree of conformance to the defined policies and standards and result in metrics that are valuable to sustaining security. However, in addition to verifying alignment with the required practices, an organization should periodically (and based on triggers as shown in Figure A.18), assess whether the SL(achieved) meets or exceeds the SL(target) in its IACS zones.

### A.3.4.2.6 Supporting practices

#### A.3.4.2.6.1 Baseline practices

The following eight actions are baseline practices:

a) Defining and validating security policies. Detailed security policy statements define the operational level commitment to mitigate each of the security risks during the risk assessment.

b) Developing procedures that provide details, like actions to take for preventing, detecting and responding to threats.

c) Adapting standards from international organizations in the area of cyber security for use in the organization's IACS environment.

d) Developing services such as secure OS images and common applications for secure IACS use.

e) Identifying security tools and products to implement parts of the security policy. While security tools and products, like firewalls and VPNs, may be used in the IT and IACS environments, the rule sets and application of these types of tools and products may be significantly different due to the different risks associated with the environments.

f) Establishing a formal methodology for accepting risk, including the appropriate management level approval based on scope and documentation.

g) Implementing policies, procedures, tools, and the like in a manner that minimizes administrative overhead and burden on the end-user without compromising effectiveness. Well-designed controls often leave behind their own audit trail that can be used for verification later.

h) Documenting the reasons for selecting or not selecting certain security countermeasures and the risks they address in a Statement of Applicability (SoA). Good documentation on security mitigation controls aids in the decision making process, facilitates the communication of the decisions, provides a basis for training people to respond to incidents and threats and provides a basis for self-assessments or audits of the conformance to the countermeasures.

#### A.3.4.2.6.2 Additional practices

NOTE 1 IEC/TR 62443-3-1 [6] and IEC 62443-3-3 [8] will address related practices when they are completed.

NOTE 2 The authors of this standard realize that there are many different types of countermeasures available. They also realize that to include a list of different types of countermeasures here would either provide the reader with too much information to digest or not provide enough detail for the reader to accurately apply the controls to IACS. The authors therefore have chosen to defer the discussion of additional IACS security practices related to countermeasures to other documents, which can provide the reader with a much more in-depth look at the different types of countermeasures available and how to apply them correctly to the IACS environment.

#### A.3.4.2.7 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [24], [27], [28], [29], [30], [31], [33].

### A.3.4.3 Element: System development and maintenance

#### A.3.4.3.1 Description of element

This element addresses supporting methods necessary to develop and maintain the IACS information technology systems that impact and are impacted by the CSMS. It discusses the cyber security aspects of: requirements documentation, design, procurement, testing, change management, patch management and backup and recovery processes.

The key point of this element is to give insight about how to implement these methods in a cyber security aware manner. The approach's aim is not to reproduce documentation describing the fundamentals of these methods but to explain how security issues are inherent in system development and maintenance processes. Security issues shall be addressed throughout the normal course of all System Development and Maintenance processes.

#### A.3.4.3.2 Requirements documentation

A.3.4.2 introduces the concept of a target security level. The term 'requirements' refers to capabilities and/or characteristics of a given system or device. Requirements may refer to many characteristics in many contexts: systems or software, product or industrial operation, functional or non-functional requirements. However, for the purpose of this element, 'System requirements' are defined as the attributes of the target security level and 'Device requirements' are defined as the countermeasure characteristics necessary for the devices within the zone to achieve the desired target security level. Because the system requirements

define the target security level, they shall be determined in the Risk management and implementation phase. These system requirements are often referred to as high-level requirements. The device requirements may change depending on the results of the design phase.

For example, a system requirement for the control zone might be to limit all network traffic to authentic control and automation traffic. A device requirement for a control operator console might be to disable all unused networking and communications protocols. In this case, that device requirement might only partially achieve the system level requirement. It may be necessary to have multiple device requirements to meet the system requirements.

The detailed, verifiable, set of system and device requirements is the foundation for the testing methods and for the verification and validation design, procurement, change management and patch management processes. It is extremely difficult to tell if design, procurement, system changes, or patches violate the Target Security Level if the specific capabilities necessary to achieve at that level are not defined.

#### A.3.4.3.3 Design

Cyber security should be built into the IACS during the design process. This objective should be considered during system procurement and development as well as during maintenance of the system. Numerous documents exist that discuss sound system design processes. This standard does not attempt to cover this subject. But it is worth emphasizing that a critical aspect of the design process is that specific countermeasures should be mapped to each of the system requirements in order to verify that the devices and the system as a whole satisfies the target security level.

The design process not only covers the preparation of the project specification but also plan the verification approach and initial verification that the project meets the stated requirements. The initial verification may be performed through a paper analysis. The final verification is performed through testing of the system.

It is important to realize that new projects are continually being initiated and executed. To avoid the potential for rework when these projects are installed and go on-line, the operations and engineering groups responsible for executing projects need to be aware of any applicable industry-specific cyber security standards and corporate cyber security policies and procedures.

#### A.3.4.3.4 Procurement

The procurement process is particularly important in attaining the desired target security level. While specifying new or updated equipment to a vendor, it is important to include requirements for cyber security. If there are specific device requirements that are required to meet the system requirements, then these need to be explicitly declared in the procurement process for those devices. It may also be necessary to specify any device requirement for things that the vendor or integrator should not do. There are some practices that are common for device vendors or integrators to do on their devices that may lead to unnecessary security holes that would prevent the system from reaching the target security level. For example, vendors historically placed back-doors into their products in order to facilitate trouble-shooting and improve customer service response times. These back-doors are a vulnerability that an attacker could exploit. A sales representative may not even be aware of these back-doors and such trouble-shooting points should not be allowed unless they are explicitly included in the procurement requirements.

The topic of procurement language for cyber security is too large for this standard. Other groups have been developing this language and may be able to provide more information (for example, see [58]).

#### A.3.4.3.5 Testing

##### A.3.4.3.5.1 General

The purpose of a testing program is to ensure that the system meets the stated requirements for the project. For a well-designed system, it should be designed to meet both the operational and security requirements. One of the earlier decisions to be made when developing a testing program is what level of assurance the organization requires from its vendors and integrators about the cyber security of the devices or systems. The level of assurance required for a particular device or system will determine the type of testing required. A vendor may have a recommended testing strategy for a particular device or system, but the user will need to determine whether that testing strategy is sufficient to validate their security requirements.

Ideally, a system would be tested under all possible states to ensure that every security contingency is met or at least so that the residual risk is known. While complete system testing is theoretically possible, it is unobtainable for most specifications given financial and personnel constraints. Therefore, the challenge is to determine an acceptable level of risk and then perform a sufficient level of testing commensurate with the acceptable risk.

After the initial test planning, written test plans and procedures should be prepared for each testing stage. These should define the tests to be performed and the expected results. They should include system configuration, system inputs and outputs and tolerable error bands. During testing, it is important to at least do a cursory check of the results to verify that they are as expected or determine if corrective action needs to be taken. After each stage of the testing is completed, the results should be evaluated. Following the system validation test, a final report should be prepared reviewing the results of all of the testing and summarizing the conclusions.

##### A.3.4.3.5.2 Types of testing

Cyber security testing, like other testing in other domains, includes verification and validation testing. According to the Capability Maturity Model [39]: *"Verification confirms that work products properly reflect the requirements specified for them. In other words, verification ensures that 'you built it right'. Validation confirms that the product, as provided, will fulfill its intended use. In other words, validation ensures that 'you built the right thing'."* To summarize this, verification determines if the implementation satisfies the specification, while validation determines if the specification satisfies the requirement.

The specific testing performed will depend on the level of testing required, the component or system being tested and the type of testing required for the system or component. Cyber security testing is typically performed in three stages: component testing, integration testing, and system testing. Verification testing shall be implemented during the component and integration stages, although validation testing may also be useful. Both verification and validation testing shall be implemented at the system testing stage.

##### A.3.4.3.5.3 Component testing

Component testing should be performed by the vendor and verified by the system owner. The component may be software, hardware, firmware or any combination of these. The component needs to be tested to verify that it meets the specific operational and security requirements. Component testing is normally workbench testing and is necessary to ensure that, when the components are combined into a system, there is confidence that each individual component performs as intended.

##### A.3.4.3.5.4 Integration testing

Integration testing should be performed by the integrator and verified by the system owner. Such testing involves operational and security testing of the various components perhaps from different vendors, that are connected together on a workbench or in an auxiliary test bed

in an effort to see if all of the components will work together correctly before being placed in the IACS environment. Integration testing may involve using additional test tools, like network management and administration tools, which were not necessary during the component testing phase.

Rarely will a test bed have the exact configuration of the control system that exists in the operating facility. Often a simplified or replica system in a development or laboratory setup is best suited for the component and integration test phases. The integration tests should be designed around this test bed facility. Care should be taken to note differences between the integration test setup and the IACS environment as well as any additional tools needed so that items that could not be fully tested during integration testing are tested during system testing. For this reason, it may be helpful, especially during the integration test phase, to locate the simplified or replica system near the site of an operational system.

In some instances, it is possible to perform a non-production integration test to see how security countermeasures will work together and how they will interface with the operational features. For example, security countermeasures that consist of discrete hardware/software may be connected via a laboratory test bed network. In other cases, this integration may not be possible. The integration test plan should take advantage of any test bed scheme that can be configured to test combinations of operating conditions that may be present in the operational system.

#### A.3.4.3.5.5 System testing

System testing should be verified and validated by the owner. The objective of validation testing is to demonstrate through appropriate techniques, procedures, and procedure refinements (as needed) that the management, operational and technical countermeasures for the IACS are implemented correctly, are effective in their application, and ensure that the new security countermeasures, as procured and installed, meet the requirements.

System testing may include penetration testing of the system to ensure that the security components are capable of protecting the system from various threats as necessary to satisfy the security level for each zone. Penetration testing is where a known person tries to penetrate the security defenses in a system, looking for weaknesses and vulnerabilities that can be exploited to gain either access or control over that system. Many companies specialize in penetration testing for traditional IT systems. It may be more difficult to find a group that understands the special requirements of IACS.

A variety of testing tools such as test scripts, databases of variables, baseline configurations with an assumed start state, metrics and calibration tools are available to assist with the actual testing. Commercial and freeware tools that are preconfigured to perform diagnostic routines and simulate gateways and connected devices are also available.

If any penetration tests are conducted, the performance of the system during the tests needs to be noted in addition to the penetration testing results. There will most likely be some performance degradation in the system or components due to the penetration testing. These performance degradations should be noted for future use.

It is important to emphasize that security countermeasures may also involve people operating through policies and procedures, as well as manual checks of security. A countermeasure, for instance, may consist of a control engineer installing a security patch issued for hardware or software. The test plan might go through the sequence of a dry-run of the patch installation, noting other factors it influences.

#### A.3.4.3.5.6 Separation of development and test environments

Development and test activities can cause serious problems, such as unwanted modification of files or system environment or even system failure. It is important to conduct cyber security testing on systems that are *not* operational because of this, thus reducing the risk of

accidental change or unauthorized access to operational software and business data through inappropriate developer access. If the development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software and information if they share the same computing environment.

The preferred method of eliminating these problems is to use a system that is separate from the operational system to perform the initial development and testing. If this is not possible, care shall be taken to ensure that the system uses a properly defined change management system to document any changes that are made to the system and provide the capability to undo those changes.

#### A.3.4.3.6 Change management

Change management systems for SIS are used in some industries based on regulatory requirements. For a complete CSMS, change management systems should be used for all IACS. The change management process should follow separation of duty principles to avoid conflicts of interest. This means that the same individual cannot both approve a change and implement the change. A technically knowledgeable individual should review proposed changes to IACS for their potential impact to HSE risks and cyber security risks based on clearly defined policies. If one of the policies is violated by the change, then the proposed change may need to be reviewed by other knowledgeable personnel to verify that it is valid or disapprove the change.

For change management to be effective, there should be a detailed record of what is installed and this should form the basis for change proposals. The change management system shall be supported by a documented and proven backup and restoration procedure. It is critical that all system upgrades, patches and policy changes are implemented in accordance with the change management system procedures.

#### A.3.4.3.7 Patch management

Installing patches, upgrades, and policy changes, which seem innocuous in isolation, may have serious cyber security ramifications. Failure to install these can also present serious hazards. A method shall be developed to determine the relevance and criticality of the vulnerabilities new patches are intended to mitigate. Such a method shall determine the impact on the ability to maintain the Target Security Level if the patch is applied *and* if it is not applied.

NOTE IEC/TR 62443-2-3 [5] is a planned technical report on patch management.

#### A.3.4.3.8 Backup and recovery

Special care should be taken to verify that the backup and recovery processes are compatible with the Target Security Level for the system. Generally, the backup and recovery process should ensure that backup copies are protected to the same extent as the originals. This may require special procedures to verify that backups have not been corrupted and that mechanisms that flag a successful backup or restoration have not been compromised. The stability of backups should be verified on a regular basis to make sure that the media containing the files has not degraded and also that the data contained on the media is still capable of being read and used. It may be necessary to keep legacy equipment in instances where older backups cannot be read by newer equipment.

#### A.3.4.3.9 Supporting practices

##### A.3.4.3.9.1 Baseline practices

The following six actions are baseline practices:

a) Documenting security requirements (threats/countermeasures/testing plans).

b) Mapping security countermeasures to security requirements.

c) Defining expected failure response behavior.

d) Defining, developing, and testing component functionality so that the entire system meets the target security level.

e) Verifying and validating cyber security during component, integration and system testing.

f) Including an authorization trail, a backup and restoration system, a patch management system and an antivirus/malware procedure into the change management system.

#### A.3.4.3.9.2 Additional practices

The following five actions are additional practices:

a) Implementing separate development, test and operational environments.

b) Employing independent component verification and validation procedures.

c) Employing independent integration verification and validation procedures.

d) Employing independent system verification and validation procedures.

e) Integrating IACS change management procedures with existing PSM procedures.

#### A.3.4.3.10 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [38], [39].

### A.3.4.4 Element: Information and document management

#### A.3.4.4.1 Description of the element

Information and document management is the process for classifying all data, safeguarding the information, managing the documents and making appropriately available the information associated with the IACS and CSMS. IACS document management may be included in the organization's general records retention and document management system. Information and document management ensures that data is available for the required length of time based on internal (for example, organization policies and device maintenance) or external (for example, legal, regulatory and political) requirements.

#### A.3.4.4.2 Considerations for information and document management

Information associated with an organization's CSMS is important, often sensitive and needs to be appropriately controlled and managed. Organizations therefore should employ comprehensive information and document management policies for their CSMS. Information associated with the development and execution of a CSMS, risk analyses, business impact studies, risk tolerance profiles, and the like may be organization sensitive and may need to be protected, as are countermeasures, philosophy and implementation strategies. Additionally, business conditions change and require updated analyses and studies. Care should be given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

One of the first steps to creating an IACS information and document management system is to define information classification levels. Information (for example, confidential, restricted and public) should be defined for managing access and control of information assets. The levels and associated practices should address sharing, copying, transmitting and distributing information assets appropriate for the level of protection required.

After the basic levels have been defined, the information associated with the IACS (for example, control system design information, vulnerability assessments, network diagrams and industrial operation control programs) needs to be classified to indicate the level of protection

required. This level of protection should be determined based on the sensitivity of the information and the potential consequences if the information was released. The classification level should indicate the need and priority of the information, as well as the sensitivity of the information. Policies and procedures for access to the information or documents need to be linked to the access control procedures as defined in A.3.3.5, A.3.3.6, and A.3.3.7.

A lifecycle document management process should be developed and maintained for this purpose. This process should confirm the security, availability and usability of the control system configuration. This includes the logic used in developing the configuration or programming for the life of the IACS. This process should also include a mechanism for updates when changes occur.

Policies and procedures should be developed detailing retention, protection, destruction and disposal of company information including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements. The policies and procedures developed for the IACS information and document management system should be consistent with and feed into any corporate information and document management system. Legal reviews of the retention policies should be performed to ensure compliance with any laws or regulations. Documents requiring retention should be identified and a retention period should be documented.

It is also necessary to ensure that appropriate measures are employed to ensure that long-term records can be retrieved (that is, converting the data to a newer format, retaining older equipment that can read the data). Methods and procedures should be developed to prevent corruption of backup data. Backup copies should be made on a regular basis. These backups should be tested to verify that they are still viable. Restoration procedures should also be regularly checked and tested.

Periodic reviews of the classification levels of information and documents should be conducted. The need to treat some information or documents with special control or handling needs to be evaluated during these reviews. A method to increase or decrease the classification level of a particular piece of information or document will also need to be developed.

Periodic review of the information and document management system, as a whole, should also be conducted. This ensures that the owners of the information or documents conform to the appropriate policies, standards or other requirements set down by the organization.

#### A.3.4.4.3 Supporting practices

##### A.3.4.4.3.1 Baseline practices

The following six actions are baseline practices:

a) Defining information classification levels (that is, confidential, restricted and public) for access and control to include sharing, copying, transmitting and distributing appropriate for the level of protection required.

b) Classifying all information (for example, control system design information, vulnerability assessment results, network diagrams and industrial operation control programs) to indicate the need, priority and level of protection required commensurate with its sensitivity and consequence.

c) Reviewing information that requires special control or handling on a periodic basis to validate whether special handling is still required.

d) Developing and including policies and procedures detailing the record update, retention, destruction and disposal of information including written and electronic records, equipment and other media containing information. Any legal or regulatory requirements should be considered when developing these policies and procedures.

e) Developing and employing methods to prevent data-corruption around backup processes and logging.

f) Confirming the security, availability and usability of the control system configuration. This includes the logic used in developing the configuration or programming for the life of the IACS.

#### A.3.4.4.3.2 Additional practices

The following four actions are additional practices:

a) Employing the appropriate measures to ensure long-term records information can be retrieved (that is, converting the data to a newer format or retaining older equipment that can read the data).

EXAMPLE Emissions data recorded over a decade ago on a system that does not currently exist or is in a proprietary format.

b) Performing periodic reviews of conformance to the information and document management policy.

c) Performing legal reviews of the retention policies to ensure conformance to any laws or regulations.

d) Encrypting all communications over the Internet involving private information with secure socket layer (SSL) or equivalent strength encryption.

### A.3.4.4.4 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [6], [23], [24], [26].

## A.3.4.5 Element: Incident planning and response

### A.3.4.5.1 Description of the element

Incident planning and response addresses the need to be vigilant in efforts to detect cyber security incidents and to promptly identify and respond to these incidents. No matter how much care is taken in protecting a system, it is always possible that unwanted intrusions might compromise the system. Technology vulnerabilities continue to exist and external threats are increasing in number and sophistication, thereby requiring a robust strategy for determining the appropriate planning and response. Incident planning and response allows an organization to predefine how it will detect and react to cyber security incidents. This allows the organization to be proactive with its cyber security program instead of reactive.

Incident planning and response provides the organization the opportunity to plan for security incidents and then to respond per the established practices. The goals of incident planning and response are very similar to those from business continuity planning, but usually relate to smaller-scale and possibly more real-time, incidents. Part of the incident plan should include procedures for how the organization will respond to incidents, including notification processes, documentation processes, investigation and subsequent follow-up practices. Responding to emergencies, ensuring personnel safety and getting systems back online are part of incident response. Identifying an incident early and responding appropriately can limit the damage/consequence of the event.

Incident planning and response is a key element of the management system for any type of risk to an organization, including cyber security risks. Sound information management practices recognize the need to have a formal incident planning and response system in place.

There are three main phases that are part of incident planning and response: planning, response and recovery. The planning phase includes the initial system program development and the specific contingency planning efforts. The response phase involves the ability to

respond to actual incidents. The recovery phase restores IACS to their previous operational states.

#### A.3.4.5.2 Planning phase

A program should be established to recognize and respond to incidents within the IACS environment. This program needs to include a written plan, documenting the types of incidents that will be dealt with and the expected response to each of those incidents.

The incident plan should include the types of incidents that may occur and the expected response to those incidents. The various types of incidents that a system intrusion might cause should be identified and classified as to the effects and likelihood, so that a proper response can be formulated for each potential incident. This plan should include step-by-step actions that the various organizations should take. If there are reporting requirements, these should be noted, as well as where the report should be made and phone numbers in order to reduce reporting confusion. During the preparation of the incident response plan, input should be obtained from the various stakeholders including operations, management, legal and safety. These stakeholders should also sign off and approve the plan.

The incident plan should include contingency plans covering the full range of consequences that may occur due to failures in the IACS cyber security program. These contingency plans should include procedures for separating the IACS from all nonessential conduits that may provide attack vectors, protecting essential conduits from further attacks and restoring the IACS to a previously known state in the event of an incident. They should also be tested periodically to ensure that they continue to meet their objectives.

Another important piece of information that needs to be included in the incident plan is the contact information for all the personnel responsible for responding to incidents within the organization. It may be difficult to locate this information in the event of an incident occurring.

After the incident plan is complete, the organization needs to distribute copies to all appropriate personnel groups within the organization, as well as any appropriate outside organizations. All associated personnel and organizations need to be made aware of their responsibilities before, during and after an incident.

In addition to just distributing the plan to all appropriate organizations, the plan should be tested periodically to ensure that it is still relevant. The organization should conduct drills of the incident response plan and analyze the results of those drills. Any problems found during the drills should be addressed and the plan should be updated.

#### A.3.4.5.3 Response phase

There are several responses that can be taken in the event of a security incident. These range from doing nothing to having a full system shutdown. The particular response taken will depend on the type of incident and its effect on the system. A written plan should have been prepared during the Planning Phase that clearly documents the types of incidents that may occur and the expected response to those incidents. This will provide guidance during times when there might be confusion or stress due to the incident.

The organization needs to have procedures in place to identify and report incidents. These procedures should establish guidelines to determine what might constitute an incident and how potential incidents should be reported and classified. These guidelines should include information about recognizing and reporting unusual experiences that may actually be cyber security incidents. The procedures should also include any special responsibilities (for example, identification methods, reporting requirements and specific actions) that personnel need to be aware of when dealing with a cyber security incident.

If an incident is detected, the details of that incident should be documented to record the incident itself, the response(s) taken, the lessons learned and any actions to be taken to

modify the CSMS in light of this incident. The details of the incident need to be communicated to all appropriate groups within the organization (for example, management, IT, process safety, automation and control engineering and manufacturing) and any outside organizations affected by the incident. It is important that these details be communicated in a timely manner to help the organization prevent further incidents.

Since every incident may not be initially recognized or detected, the organization should have procedures in place to identify failed and successful cyber security breaches. Depending upon the magnitude of the damage inflicted by a particular incident, cyber security forensic specialists may need to be consulted to determine the root cause of the incident, to evaluate the effectiveness of the response(s) taken and, in case of an intentional loss, to preserve the chain of evidence to support efforts to prosecute the perpetrator. If the incident occurs on a critical IACS system resulting in a business continuity interruption, the goal will likely be to get the facility back to running as quickly as possible. This may involve reformatting hard disks and a complete reload of the operating system and applications which probably removes all forensics data. Establishing incident response priorities and practices prior to an incident is important so that everyone understands the goals and methods.

#### A.3.4.5.4 Recovery phase

The results of the incident might be minor or could cause many problems in the system. Step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible.

An important component of the recovery phase is the restoration of systems and information (that is, data, programs and recipes) to operational states. This requires a sufficient backup and recovery system capable of handling the entire IACS. It may be made up of one or multiple physical backup and recovery devices, but they should all work together to aid in the recovery of the IACS.

The organization should have an incident analysis process in place to address issues that are discovered and ensure they are corrected. The findings from the analysis process need to be incorporated into the appropriate cyber security policies and procedures, technical countermeasures and incident response plans. Cyber security-related incidents can be divided into three categories:

- malicious code such as viruses, worms, bots, rootkits and Trojan horses;
- accidental loss of availability, integrity or confidentiality (including production availability);
- unauthorized intrusion that extends to physical assets.

Incidents in the first two categories are typically managed within the IT security incident response process. The third category would typically be managed in collaboration with HSE specialists and site leadership.

#### A.3.4.5.5 Supporting practices

##### A.3.4.5.5.1 Baseline practices

The following nine actions are baseline practices:

a) Establishing procedures for the overall organization to recognize and report unusual experiences that may actually be cyber security incidents.

b) Establishing incident planning and response procedures which include:

   - naming the responsible person for executing the plan when the need arises;
   - structuring an incident response team that can be called in, including contributors from IT security and IACS and additional personnel;
   - establishing the responsibility for coordinating defense and response to an incident;

- handling the incident from initiation through final review;
- creating procedures for identifying, categorizing and prioritizing incidents;
- creating procedures for different types of incidents like DoS attacks, system hacking, malicious code, unauthorized access and inappropriate usage.

c) Identifying proactive measurements to automatically identify incidents during their early stage.

d) Preplanning responses to threat scenarios identified from vulnerability and risk assessments.

e) Communicating IACS incidents to all appropriate organizations including the IT, industrial operations safety, automation and control engineering and operations organizations for awareness building.

f) Communicating metrics and incidents to executive management.

g) Carrying out regular reviews of past incidents, to improve the CSMS.

h) Documenting the details of the incident, the lessons learned and any actions to be taken to modify the CSMS in light of this incident.

i) Conducting drills to test the plan. Holding meetings following the drills to identify areas for improvement.

#### A.3.4.5.5.2 Additional practices

The following thirteen actions are additional practices:

a) Developing forensic investigation capabilities for IACS systems either internally or externally.

b) Developing a process for immediately reporting cyber security incidents. Ensuring that the process has links to the organization's crisis management team. Educating personnel with examples of reportable incidents so they can better comply with reporting requirements.

c) Understanding any potential links between IT, safety and IACS and incorporating this understanding into integrated security incident response procedures.

d) Developing, testing, deploying and documenting the incident investigation process.

e) Developing corporate policies for reporting cyber security incidents and sharing incident information with industry-wide groups and government agencies where corporate policies allow.

f) Specifying roles and responsibilities with respect to local law enforcement and/or other critical stakeholders in an internal and shared incident investigation program.

g) Expanding the investigation of incidents based on the potential outcome that could have occurred rather than the actual outcome, recognizing that the cyber incident may include malicious intent. The level of incident investigation may need to be upgraded depending on the potential seriousness of the incident.

h) Developing methodologies and mechanisms to ensure that corrective actions identified as the result of a cyber security incident or a drill are fully implemented.

i) Providing security incident response training to organizational cross-functional training teams.

j) Reviewing final incident investigation results with all personnel whose job tasks are relevant to the findings. Reviewing the incident in light of trends and recording it so it can be used for subsequent trend analyses.

k) Promoting peer-to-peer and cross-industry mutual assistance activities in order to learn from others' experiences regarding cyber security incident evaluation, response, investigation, communication and correction.

l) Identifying previously unforeseen consequences, especially those that may affect future application of the plan. Incidents may include risk events, near misses and malfunctions. Also included are any observed or suspected weaknesses in the system or risks that may not have been previously recognized.

m) Incorporating emergency response planning into incident response planning.

#### A.3.4.5.6 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [26], [36].

## A.4 Category: Monitoring and improving the CSMS

### A.4.1 Description of category

A CSMS includes all the measures necessary to create and maintain a cyber security program. The scope and level of this effort are dependent on the organization's objectives, tolerance for risk and cyber security program maturity. This management system should address the requirements, methods, devices, interfaces and personnel necessary to implement the cyber security program.

Monitoring and improving the CSMS involves both ensuring that the CSMS is being used and also reviewing the CSMS itself for effectiveness. Figure A.19 shows the two elements that are part of the category:

- Conformance and
- Review, improve and maintain the CSMS.

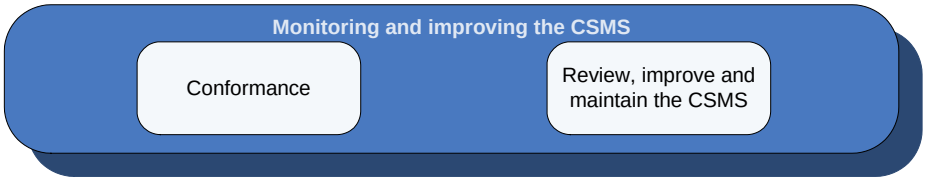



**Figure A.19 – Graphical view of category: Monitoring and improving the CSMS**

### A.4.2 Element: Conformance

#### A.4.2.1 Description of element

Conformance is the process of validating that the organization is following the cyber security program that was developed. The CSMS is only as good as an organization's ability to follow it. The organization needs to be held accountable to the policies and procedures set down as part of the CSMS or the management system will be ineffective. By validating its conformance with the CSMS, the organization can use the built-in processes of the CSMS to improve the overall system in the future.

As part of validating conformance with the CSMS, there are scheduled and unscheduled activities. Periodic reviews of the CSMS would be considered scheduled, but responding to a cyber security incident would most likely be considered unscheduled.

Establishing key performance indicators (KPI) will give the organization a way to measure the performance of the CSMS. Using KPI that are consistent with best-in-class solutions from industry groups or other organization will allow for benchmarking of the CSMS.

#### A.4.2.2 Scheduled versus unscheduled activities

Many subclauses of the CSMS include the idea of periodic reviews of some item in order to monitor or improve the CSMS over time. These reviews are all part of the Maturity Model of a security program as discussed in IEC/TS 62443-1-1. The reviews conducted as a standard part of a CSMS keep the system from degrading over time due to new threats, vulnerabilities or situations that did not exist when the system was first developed.

There may also be critical threats, vulnerabilities or situations that arise that need to be dealt with before the next scheduled review period. These would constitute unscheduled activities and may require a re-evaluation of the CSMS in order to ensure effectiveness.

Periodic reviews and audits of the CSMS determine if the desired policies, procedures and countermeasures have been implemented properly and that they are performing as intended. In the IACS environment, auditors shall fully understand the corporate cyber security policies and procedures and the specific HSE risks associated with a particular facility and/or industrial operation. Care shall be taken to ensure that the audits do not interfere with the control functions provided by the IACS equipment. It may be necessary to take a system off-line before the audit can be conducted. The audit should verify that:

- the policies, procedures and countermeasures present during system validation testing are still installed and operating correctly in the operational system;
- the operational system is free from security compromises;

  NOTE Should an incident occur, logs and records are expected to be generated, capturing information on the nature and extent of the incident.

- the management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.

A particular unscheduled activity that may trigger a review of the CSMS may be the addition or removal of assets from the IACS. A common practice during system maintenance or retooling may be to add, upgrade or remove equipment or software from the IACS. A well defined and followed change management process will catch this, which may trigger a review or audit of the CSMS. This review or audit would ensure that the change did not adversely affect the cyber security of the IACS. Another example of an unscheduled activity would be a response to a virus outbreak at a facility. After the CSMS system has been used to respond and recover from the incident, a review or audit of the CSMS should be conducted to determine where the failure occurred that allowed the virus to spread.

Any cyber security reviews or audits (internal or external) will provide the organization with valuable data in order to improve the CSMS. The results of these reviews or audits should include as much detailed information as necessary to both ensure that any legal or regulatory requirements are satisfied and that any modifications indicated by the review or audit can be made. The results should be sent to all of the appropriate personnel (that is, stakeholders, managers and security personnel).

#### A.4.2.3 Key performance indicators

KPI allow the organization to determine how well the CSMS in performing and helps it direct any resources towards areas that may need improvement. KPI should, as much as possible, be quantitative values (that is, numbers or percentages) indicating how a particular part of the CSMS performs with respect to expected conditions.

Since any reviews or audits or the CSMS should be expressed using these KPI, it is important to pick indicators that are relevant, meaningful and consistent with the CSMS and other requirements on the organization. The results of periodic scheduled activities may be expressed as the performance against a set of predefined metrics to indicate security performance and security trends. The results of unscheduled activities may be expressed as the effectiveness of the CSMS to deal with the unscheduled event or incident.

Organizational capability data should be a part of the performance indicators. Companies should track the percentage of personnel assigned to IACS roles and the percentage of those personnel who have passed the training and qualification requirements for their roles. While these data may seem esoteric, systemic problems can be indicated here before being noticed in poor audit results.

Benchmarking the KPI and the results of reviews or audits against other organizations or requirements is a good method for validating the CSMS. If benchmarking data are collected

over a period of time, it may be possible for the organization to determine trends in either threats or countermeasures. These may indicate places where the CSMS requirements may have to be reviewed as part of the review, improve and maintain subclause of the CSMS (see A.4.3).

#### A.4.2.4 Supporting practices

##### A.4.2.4.1 Baseline practices

The following two actions are baseline practices:

a) Providing assurance that the appropriateness of the control environment and compliance with the overall cyber security objectives are being met. Detecting if additions, upgrades, or removals (that is, software patches, application upgrades, and equipment changes) have introduced security exposures.

b) Confirming that, over a specified regular audit period all aspects of the CSMS are functioning as intended. A sufficient number of audits should be planned so that the audit task is spread uniformly over the chosen period. Management should ensure periodic audits are conducted. Management should ensure that there is evidence to:

- verify that documented procedures are being followed and are meeting their desired objectives;
- validate that technical controls (that is, firewalls and access controls) are in place and are working as intended both consistently and continuously.

##### A.4.2.4.2 Additional practices

The following three actions are additional practices:

a) Requiring that the cyber security metrics program is built upon the seven key steps listed as follows:

1) defining the metrics program goal(s) and objectives;
2) deciding what metrics to generate in order to measure the degree of adoption and conformance to the policies and procedures defined in the CSMS:
   - proactively assessing any potential security vulnerabilities (for example, % of security audit weaknesses fixed by the agreed date);
   - tracking implementation and usage of security and preventive measures (for example, % of conformance with security standards).
3) developing strategies for generating the metrics;
4) establishing benchmarks and targets;
5) determining how the metrics will be reported and to whom;
6) creating an action plan and acting on it;
7) establishing a formal program review/refinement cycle.

b) Reviewing the results of audits, self-assessments, cyber security incident reports and feedback provided by key stakeholders regularly to understand the effectiveness of the CSMS.

c) Conducting operational security reviews on the IACS by security trained IACS engineers. In addition, security issues are frequently reviewed at a broader level by a governance body.

#### A.4.2.5 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [24], [26], [35], [49], [50].

### A.4.3 Element: Review, improve and maintain the CSMS

#### A.4.3.1 Description of element

The process of continuously monitoring and reviewing the CSMS allows an organization to establish, with evidence, that it is meeting the goals, policies and procedures laid out in the CSMS. The KPI defined while developing the CSMS are used to evaluate the performance of the CSMS during the conformance review process. The Conformance element verifies that the CSMS is operating *as* defined, while this element verifies that the requirements used to develop the CSMS meet the organization's cyber security goals.

Internal checking methods, such as conformance audits and incident investigations, allow the organization to determine the effectiveness of the management system and whether it is operating according to expectations. It is also important to establish that the management system still meets the goals, targets and objectives set out during the planning process. If there are deviations from the original goals, targets or objectives, systematic changes to the management system may be required.

Because both threats and technologies for addressing security are evolving, it is anticipated that the organization's cyber security program will evolve, reflecting new threats and capabilities that are available. Organizations should be tracking, measuring and improving security efforts to keep people, property, products, industrial operations, data, and information systems secure.

The overall objective is to ensure that the CSMS remains effective by incorporating improvements made based on new threats, new capabilities and regular reviews. Continual attention to security provides an indicator to personnel that cyber security is a core company value.

#### A.4.3.2 Review of conformance to the CSMS

Conformance to the CSMS has been discussed in an earlier element. It verifies that the organization is following the policies and procedures expressed in the CSMS. As part of the conformance process, key performance indicators have been defined to measure the performance of the organization's CSMS. Poor marks in these KPI in one review cycle may indicate a singular problem that can be remedied by simple solutions. Poor marks in many of the KPI or in the same KPI over repeated reviews may indicate systemic problems with the CSMS. It may indicate that training or enforcement needs to be improved, resources are inadequate or that the implemented procedures are impractical. Managing the CSMS involves making these judgments. Whether the KPI are evaluated through independent or self-audits, it is useful to consult with the organization whose actions are being measured, to help make this determination.

It is important that the CSMS include requirements for improving conformance results. The responsible individual(s) should also be chartered to develop a long-term strategy for the improvement to assure a consistent cost-effective improvement path over time.

#### A.4.3.3 Measure and review the effectiveness of the CSMS

Measuring the effectiveness of the CSMS at a minimum involves reviewing incident data. The greater an organization's capability to detect failed and successful cyber security breaches and record these as incidents, the greater its capability to measure effectiveness of the CSMS in lowering risk. Incident data include the number of incidents, the type or class of incidents and the economic impact of the incidents. These data are extremely important both to understand the current economic impact of cyber security threats and to assess the effectiveness of specific countermeasures employed.

While analysis of incident data can measure effectiveness of the CSMS in the past, CSMS management is also charged with maintaining the effectiveness of the CSMS into the future.

To accomplish this, it is necessary to monitor changes to factors that might increase or decrease its effectiveness going forward. Key factors to monitor are the following:

- the level of risk, which may change due to a change in threat, vulnerability, consequence or likelihood;
- the organization's risk tolerance;
- the implementation of new or changed systems or industrial operations;
- industry practices;
- available technical and non-technical countermeasures;
- legal and regulatory requirements.

An organization's CSMS should be reviewed at regular intervals, to assess both its past effectiveness and the view going forward. This review should include a periodic assessment of cyber security policies and procedures to affirm that those policies and procedures are in place and working and meet the legal, regulatory and internal security requirements. In appropriate circumstances, assessments also apply to the policies and procedures of the organization's business partners, such as suppliers, support providers, joint ventures or customers.

In addition to regular reviews, major changes to the factors listed above should also trigger review of related aspects of the CSMS. An organization should determine a set of change triggers and thresholds, which would trigger such a review. These triggers should include the following factors:

- Internal factors: Based on the performance of the CSMS and the results of KPI and other suitable internal indicators (for example, risk tolerance, management changes, and the like).
- External factors: Changes in the threat environment, industry best practices, available solutions and legal requirements may indicate a need or opportunity for improvement of the CSMS.

The organization assigned to manage changes to the CSMS should also be responsible for reviewing the triggers and thresholds for changes and for using them to kick off the review process.

#### A.4.3.4 Legal and regulatory implications for the CSMS

The legal and regulatory environment that the organization is subject to may change over time. The organization may still be compliant with the CSMS as it was originally defined, but that CSMS may no longer satisfy the legal and regulatory requirements that apply.

The organization should periodically review its applicable legal and regulatory requirements and identify any areas where they may affect the CSMS. Also, any major changes to the legal and regulatory requirements, such as major new or updated requirements, should trigger a review of the CSMS to ensure it meets the new requirements.

#### A.4.3.5 Manage CSMS change

To have a coordinated system, an organization/team should be assigned to manage and coordinate the refinement and implementation of the CSMS changes. This organization/team is likely to be a matrix type organization drawing on key people from different business organizations. This team should use a defined method for making and implementing changes.

A number of internal and external factors will necessitate changes to the CSMS. The management of these changes requires coordination with the various stakeholders. When implementing changes to the management system, it is important to examine possible side effects relating to system operation or safety. IACS security also needs to take into account the different organizations, practices and response requirements when incorporating

improvements. Written procedures should be developed to manage changes to the CSMS. This process might include the following steps:

a) Defining the current management system

Before the CSMS can be refined, it is necessary to know and understand the current management system. All the policies relating to cyber security should be reviewed so all the stakeholders clearly understand the current policy and how it is being implemented. In addition, all assets and procedures related to the CSMS should be identified.

b) Defining the procedures for proposing and assessing changes to the CSMS

Once the current management system is understood, it should be reviewed for compliance and effectiveness, as described previously. Weaknesses or gaps in the management system should be identified and corrections proposed. The evaluation of the management system should identify areas where changes might be required. In addition, industry best practices and requirements outlined in this standard might be considered in defining changes that would strengthen the CSMS. Selection of new countermeasures will follow the principles outlined in the Risk Management and Implementation element of this standard (see A.3.4.2). Once defined, the proposed changes to the CSMS should be documented in a concise manner so that they can be consistently presented to other stakeholders.

c) Proposing and evaluating changes to the CSMS

With the changes identified and documented, they should be presented to the stakeholders. The proposed changes should be reviewed to determine if they will produce any negative or unforeseen side effects. They should also be evaluated to determine if any changes need to be made to the CSMS against the original requirements and testing suites. As new capabilities are developed, the reaction of many organizations is to incorporate the newest technology into the system. In the IACS environment, it is important to validate any new cyber security technology or solution before incorporating it.

d) Implementing CSMS changes

After the stakeholders agree on the change, the changes to the CSMS should be implemented. Changes to the policy should follow company procedures for policy changes and at a minimum these changes should be documented and written approval should be obtained from key stakeholders. Special attention to systems testing, validation and control vendor involvement is required.

e) Monitoring CSMS changes

With the new or revised CSMS in place, it is important to monitor and evaluate its performance. A review of the management system should be performed on a regular basis and whenever there are changes to the CSMS.

#### A.4.3.6 Supporting practices

##### A.4.3.6.1 Baseline practices

The following twelve actions are baseline practices:

a) Using a method to trigger a review of the level of residual risk and risk tolerance when there are changes to the organization, technology, business objectives, industrial operation or external events including identified threats and changes in social climate.

b) Analyzing, recording and reporting operational data to assess the effectiveness or performance of the CSMS.

c) Analyzing the results from the periodic reviews and audits of the CSMS to determine if a change is needed.

d) Investigating ineffective CSMS policies and procedures to determine any root causes where there are systemic problems. Actions are identified not only to resolve the issue, but also to minimize and prevent reoccurrences.

e) Reviewing potential threats and conducting an impact analysis on a regular basis to determine if countermeasures are required.

f) Identifying applicable and changing regulations and legislation and contractual cyber security obligations and requirements.

g) Involving the key stakeholders in the organization for confirmation on areas for further investigation and planning. The key stakeholders should include personnel from all of the different groups affected by the CSMS (that is, IT, IACS and safety).

h) Identifying appropriate corrective and preventive actions to further improve the performance process.

i) Prioritizing improvements in the CSMS and putting plans in place to implement them (that is, budgets and project planning).

j) Implementing all changes using the management of change processes within the organization. Special attention to systems testing, validation and control vendor involvement is required due to the HSE implications of the IACS environment.

k) Validating that agreed actions from previous audits and reviews have been implemented.

l) Communicating action plans and areas of improvement to all the stakeholders and the affected personnel.

#### A.4.3.6.2 Additional practices

The following two actions are additional practices:

a) Requiring that the cyber security metrics program is built upon the seven key steps listed as follows:

   1) defining the metrics program goal(s) and objectives;

   2) deciding what metrics to generate to measure the effectiveness of the CSMS to meet the organization's security goals;

      NOTE It may be good to provide a retrospective view of security preparedness by tracking the number and severity of past security incidents, including patterned small events.

   3) developing strategies for generating the metrics;

   4) establishing benchmarks and targets;

   5) determining how the metrics will be reported and to whom;

   6) creating an action plan and acting on it;

   7) establishing a formal program review/refinement cycle.

b) Undertaking many different strategies to drive continuous improvement in cyber security activities. The strategies are commensurate with risk and dependent upon corporate culture, existing systems, and size or complexity of digital systems. Some potential strategies are the following:

   - conducting benchmarking security activities both within and outside of the industry including the use of external validation to help validate improvements;
   - seeking employee feedback on security suggestions actively and reporting back to senior management as appropriate on performance shortcomings and opportunities;
   - using standard corporate business methodologies, such as Six Sigma™, for measuring, analyzing, improving and sustaining cyber security improvements.

#### A.4.3.7 Resources used

This element was based in part on material found in the following references, all of which are listed in the Bibliography: [24], [26], [35], [49].

# Annex B
(informative)

# Process to develop a CSMS

## B.1 Overview

Clause 4 and Annex A detail the individual elements associated with a comprehensive, integrated CSMS. Developing a functioning CSMS is a journey that may take months or years to achieve. This annex focuses on the ordering and iterative nature of the activities associated with developing the elements of the CSMS. The objectives of this annex are the following:

- to provide key insights about how successful organizations have sequenced these activities, and point out common pitfalls related to the order in which elements of a CSMS are addressed;
- to provide a step-by-step guide that an organization may reference as they begin the process of establishing a CSMS;
- to provide a step-by-step guide on how to use this standard.

## B.2 Description of the process

Figure B.1 shows the six top level CSMS activities and their relationships. Later figures of this annex break each of these down in further detail. While Figure B.1 shows interrelationships between all of the activities, not all of these interrelationships are shown in detail later in this annex. This has been done to balance the concise representation with the completeness of the topics being discussed.

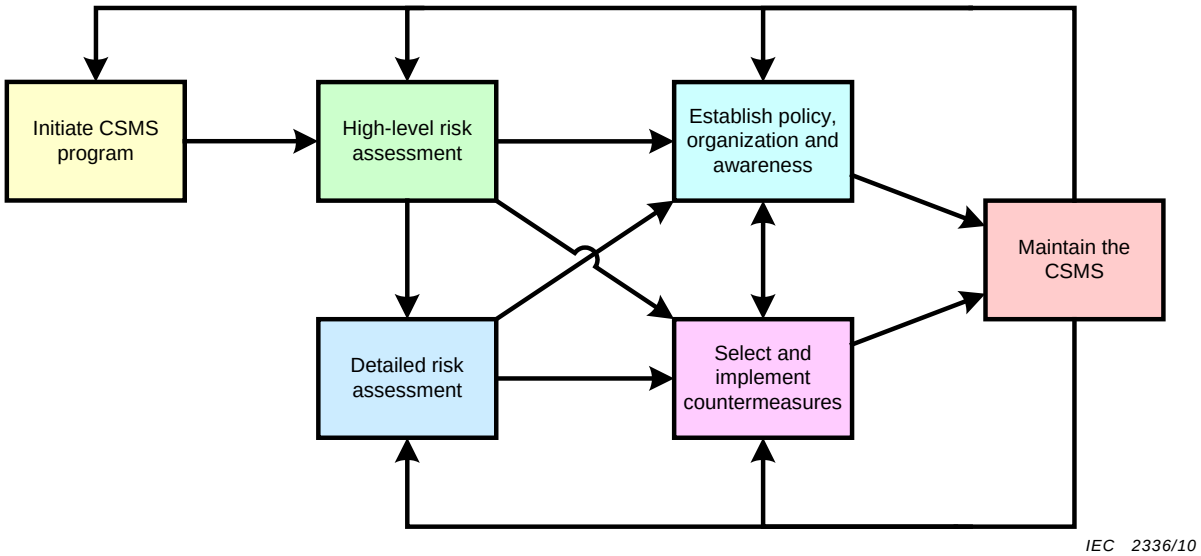



**Figure B.1 – Top level activities for establishing a CSMS**

The “Initiate CSMS program” activity puts the program on solid footing by establishing the purpose, organizational support, resources, and scope for the CSMS. Starting with this activity will maximize the effectiveness of the effort, as is the case for any program with broad impact. The initial scope may be smaller than desired, but can grow as the program succeeds.

Risk assessment drives the content of the CSMS. The “High-level risk assessment” activity lays out threats, likelihood of their realization, general types of vulnerabilities and consequences. The detailed risk assessment activity adds a detailed technical assessment of vulnerabilities to this risk picture. It is important to address risk assessment first at a high

level. A common pitfall is to expend resources early on to perform detailed vulnerability assessment and then experience an apathetic response to these technical results, because the overall higher level risk context has not been established.

The two activities “Establish policy, organization and awareness” and “Select and implement countermeasures” directly lower risk to the organization. These activities will implement both high-level and low-level decisions, driven by both the high-level and detailed risk assessments. The “Establish policy, organization and awareness” activity covers creation of policies and procedures, assignment of organizational responsibilities and planning and execution of training. The “Select and implement countermeasures” activity defines and implements the organization’s technical and non-technical cyber security defenses. These two main activities shall take place in a coordinated fashion. This is because in most cases related policies and procedures, training and assignment of responsibility are essential in order to make a countermeasure effective.

The “Maintain the CSMS” activity includes tasks to determine whether the organization conforms to its CSMS policies and procedures, whether the CSMS is effective in meeting the organization’s cyber security goals and whether these goals need to change in light of internal or external events. This activity defines when revision of its high-level or detailed risk assessments is required or may precipitate a change to the initial program parameters. It may also provide input for improvement of policies, procedures, organizational decisions or training in order to maximize effectiveness of countermeasures or point out weaknesses to be corrected in implementation of selected countermeasures. Organizations report that the Maintain the CSMS activity is very difficult, since initial enthusiasm for the program may have died down and other priorities emerge. However, without adequate attention to this activity, positive results from the program will ultimately be lost, because the environment in which the program will operate is not static.

The remainder of this annex gives the reader a better understanding of the six top level CSMS activities. The element or sub-element number has been referenced to aid the reader of this standard in finding more information about that particular topic.

## B.3 Activity: Initiate CSMS program

Figure B.2 illustrates the steps involved in the “Initiate CSMS program” activity.

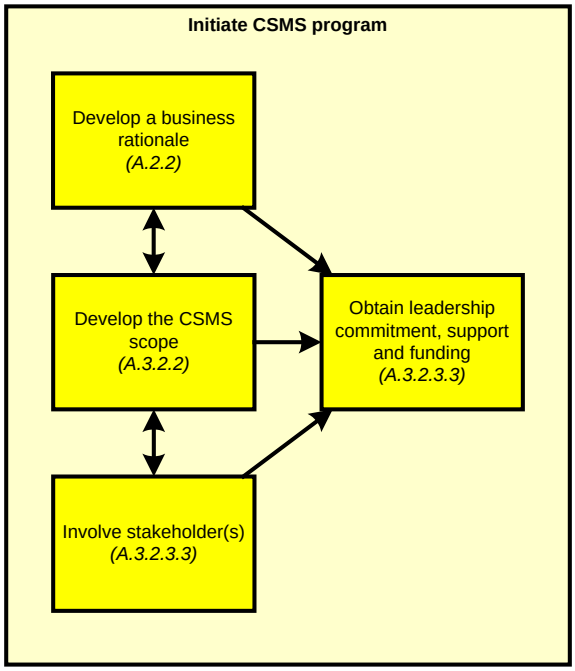



**Figure B.2 – Activities and dependencies for activity: Initiate CSMS program**

The desired outcome of the “Initiate CSMS program” activity is to obtain leadership commitment, support and funding for the CSMS. In order to achieve this, the first steps as shown in Figure B.2 are to develop a business rationale that will justify the program to management and a proposed scope for the program. In conjunction with these steps, individuals who are stakeholders based upon this rationale and scope are identified and involved. It is most effective to identify these stakeholders up front, wherever possible and make them a part of the effort to engage management for a commitment to the program. An effective organizational framework for security can then be built, starting at the top. A common pitfall is to attempt to initiate a CSMS program without at least a high-level rationale that relates cyber security to the specific organization and its mission. Cyber security activities require resources from the organization and although a program may start under the general consensus that cyber security is good, momentum will quickly be lost to competing demands if a business rationale has not been established.

## B.4 Activity: High-level risk assessment

Figure B.3 illustrates the steps involved in the “High-level risk assessment” activity.

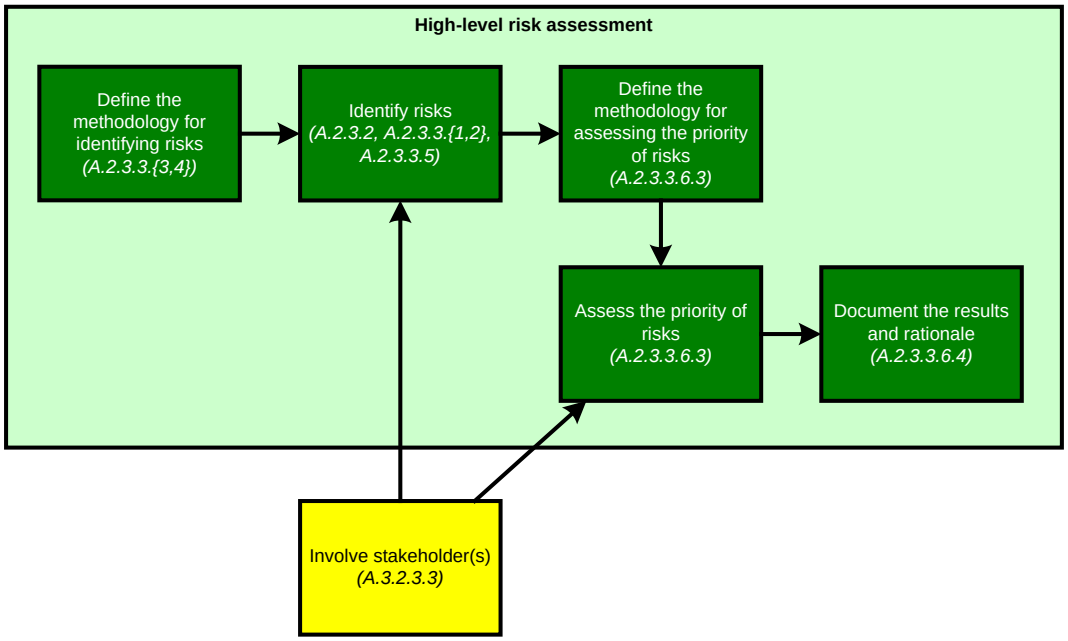



**Figure B.3 – Activities and dependencies for activity: High-level risk assessment**

The “High-level risk assessment” activity involves selecting methodologies for identifying and prioritizing risks and then executing those methodologies. It is important to define these methodologies up front so that they will provide structure for the rest of the risk assessment. Figure B.3 shows that it is important to involve the stakeholders, identified during the Initiate CSMS Program activity, in the process of identifying and assessing the priority of risks. The final step to document the results and rationale is important because this record will be found invaluable when the risk assessment needs to be confirmed or updated in the future.

## B.5 Activity: Detailed risk assessment

As shown in Figure B.4, the “Detailed risk assessment” activity provides greater detail to the risk assessment, by first taking an inventory of specific IACS systems, networks and devices. Resource or time constraints may not allow detailed examination of all of these assets. In this case, the threats, consequences and types of vulnerabilities identified in the high-level risk assessment are used to assist in setting priorities for those particular systems, networks and devices on which to focus. Other factors such as local support or history of problems will also contribute to determining the focus for detailed risk assessment. The identification of detailed vulnerabilities is guided by the vulnerability types from the high-level risk assessment, but is not limited to those types. Thus a detailed vulnerability assessment may uncover not only new types of vulnerabilities but also potentially new threats and associated consequences that had not been identified during the high-level risk assessment – in other words, new risks. In this case, the high-level assessment should be updated to include these. All vulnerabilities found are associated with a specific risk (threat, likelihood and consequence) and prioritized in a manner consistent with the method used during the high-level risk assessment.

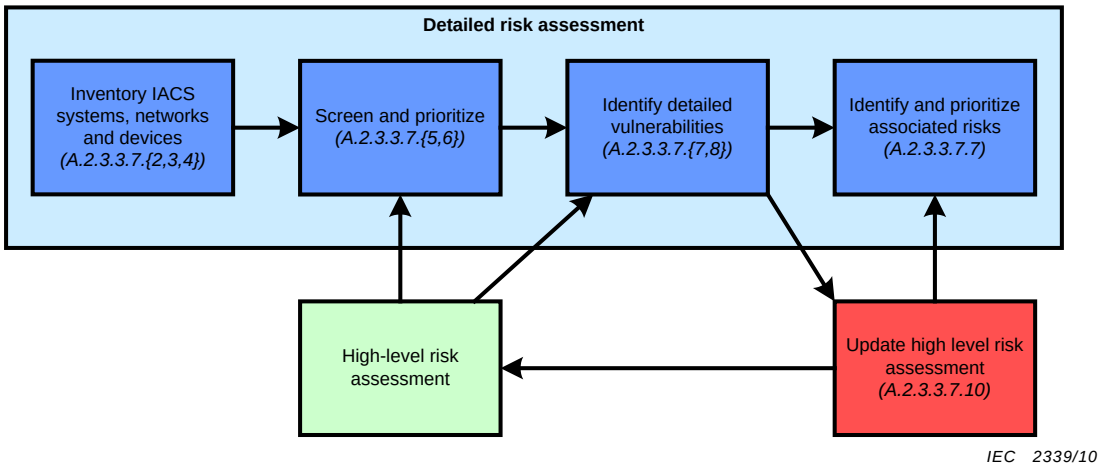



**Figure B.4 – Activities and dependencies for activity: Detailed risk assessment**

## B.6 Activity: Establishing security policy, organization and awareness

The appropriate policies for the organization are an operational interpretation of the organization's risk tolerance. An organization that creates policy before understanding its risk or risk tolerance may expend unnecessary effort following and enforcing inappropriate policy or likewise find its policies do not support the level of risk reduction required. Figure B.5 illustrates the steps involved in the "Establish security policy, organization and awareness" activity.

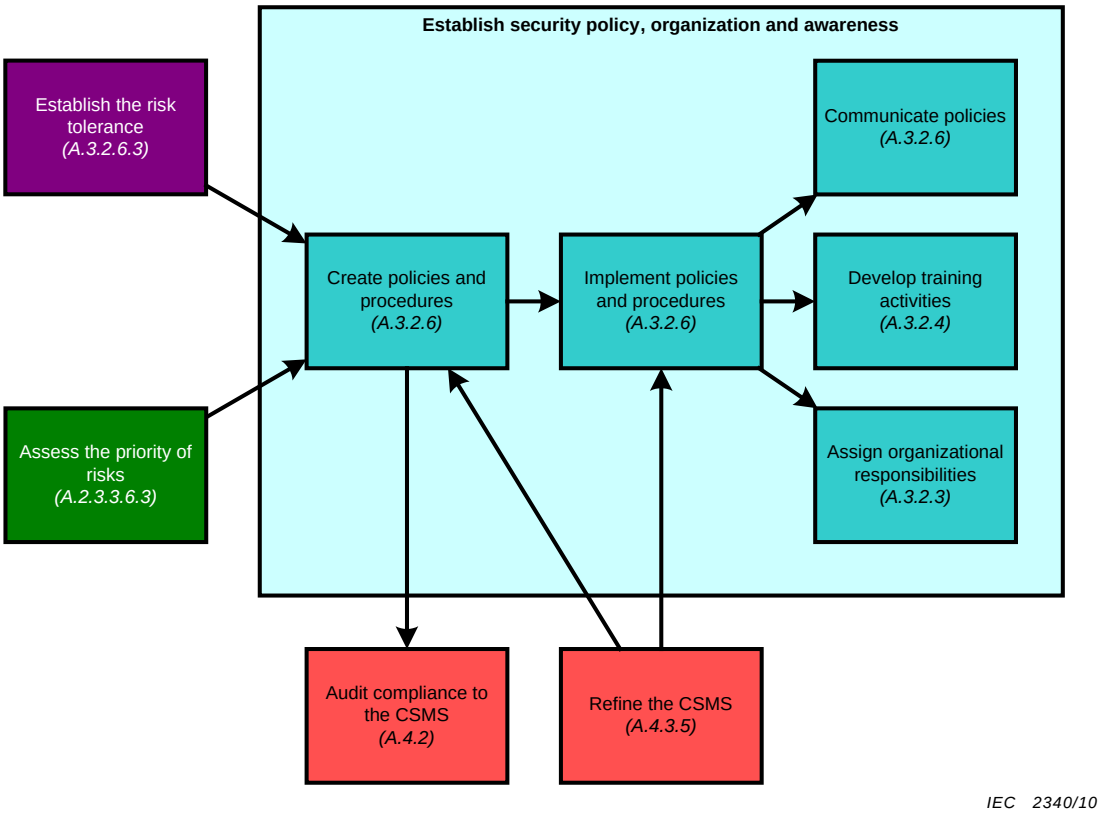



**Figure B.5 – Activities and dependencies for activity: Establish security policy, organization and awareness**

Implementation of policy involves communicating the policy to the organization, training personnel in the organization and assigning responsibility for adherence to the policy. Policies and procedures can impact any activity in the CSMS. For example, there may be policies

regarding common countermeasures to be used, requiring specific system development and maintenance processes or determining when risk is to be re-assessed. Thus, Figure B.5 does not attempt to depict all potential impacts of policies and procedures on the CSMS.

Figure B.6 further breaks down the two activities “Develop training activities” and “Assign organization responsibilities”. It shows many of the different training activities that make up a training program, the organizational responsibilities associated with those training activities, and the associated activities related parts of the CSMS program. This figure does not show all organizational responsibilities or training topics that might be related to the CSMS, but tries to show the main points that should be considered.

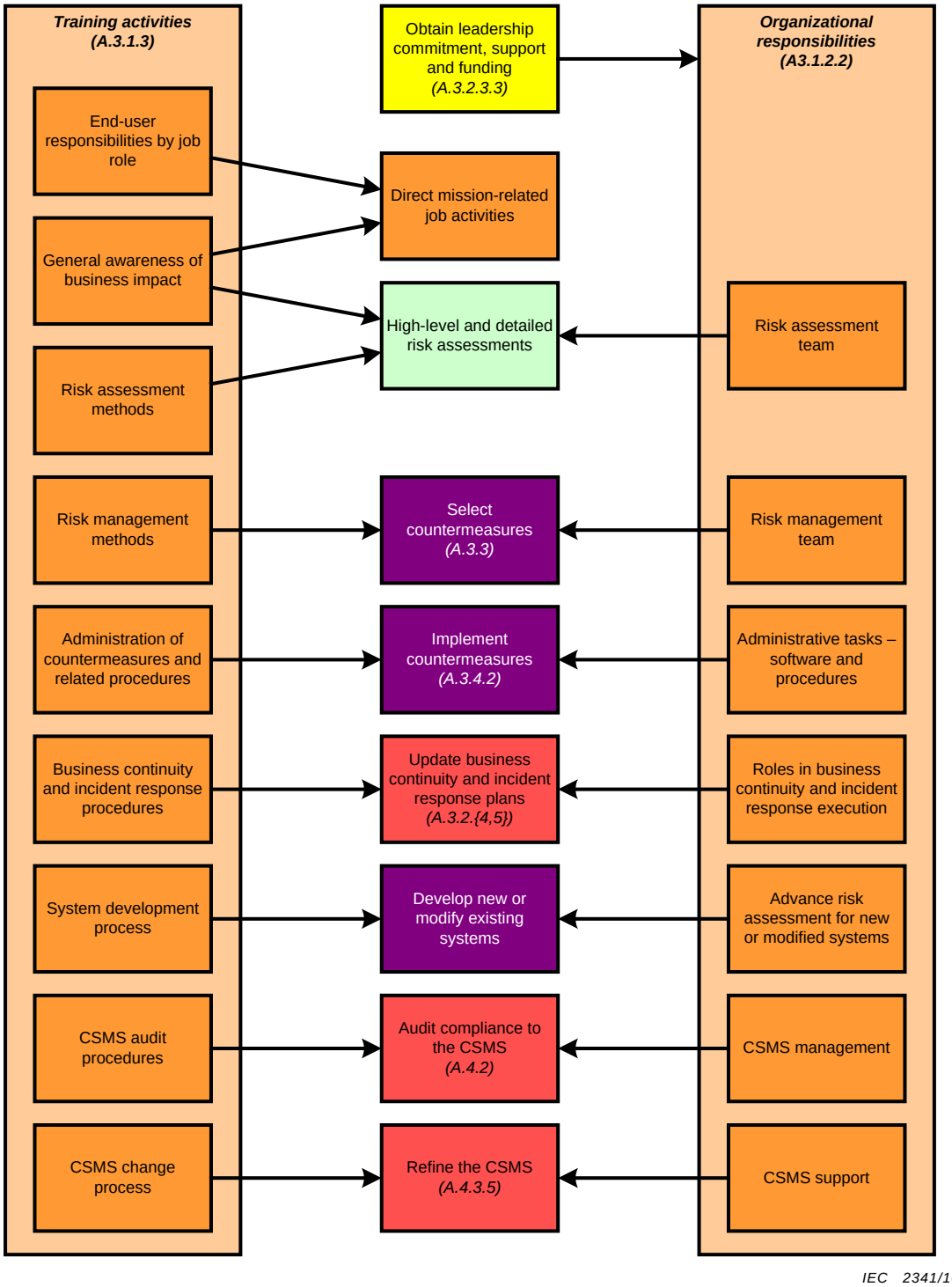



**Figure B.6 – Training and assignment of organization responsibilities**

## B.7 Activity: Select and implement countermeasures

Figure B.7 illustrates the steps involved in the “Select and implement countermeasures” activity.

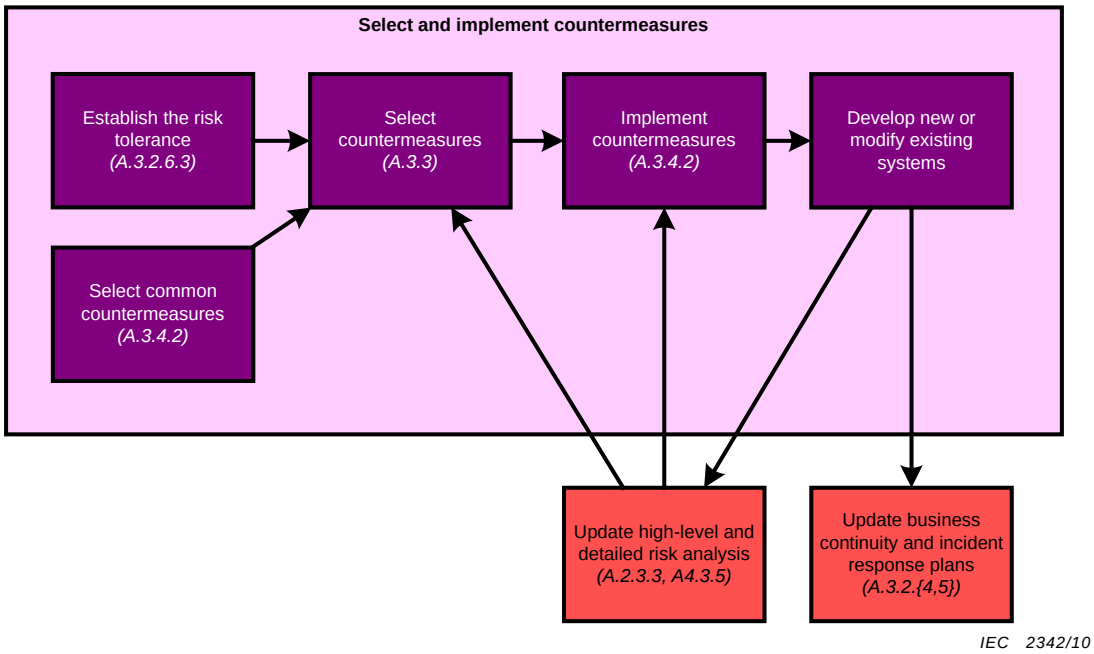



**Figure B.7 – Activities and dependencies for activity: Select and implement countermeasures**

The selection of countermeasures is the technical process of risk management. The organization’s risk tolerance, pre-selected common countermeasures and the results of high-level and detailed level risk assessment, drive the risk management approach for selecting countermeasures. If the organization is implementing a new system or modifying an existing system, this drives an update to high-level and detailed risk assessments for the scenario in which this new system is implemented. Countermeasures selection related to the new or modified system then proceeds based upon this updated risk information. Development or modification of systems requires an update to business continuity and incident response plans.

## B.8 Activity: Maintain the CSMS

As shown in Figure B.8, the “Maintain the CSMS” activity requires periodic review and refinement of the CSMS based on review results. Major inputs to this review are results from effectiveness measures and audits of conformance from internal monitoring of the CSMS itself. Other inputs to this review are external information about available countermeasures, evolving industry practices and new or changed laws or regulations.

A review of the CSMS identifies deficiencies and proposes improvements, which in turn creates refinements to the CSMS. Some of these refinements may take the form of new countermeasures or improvements in countermeasure implementation. Other refinements may modify policies and procedures or improve their implementation. Review of poor conformance results may point out the need for improvements in training or assignment of organizational responsibilities.

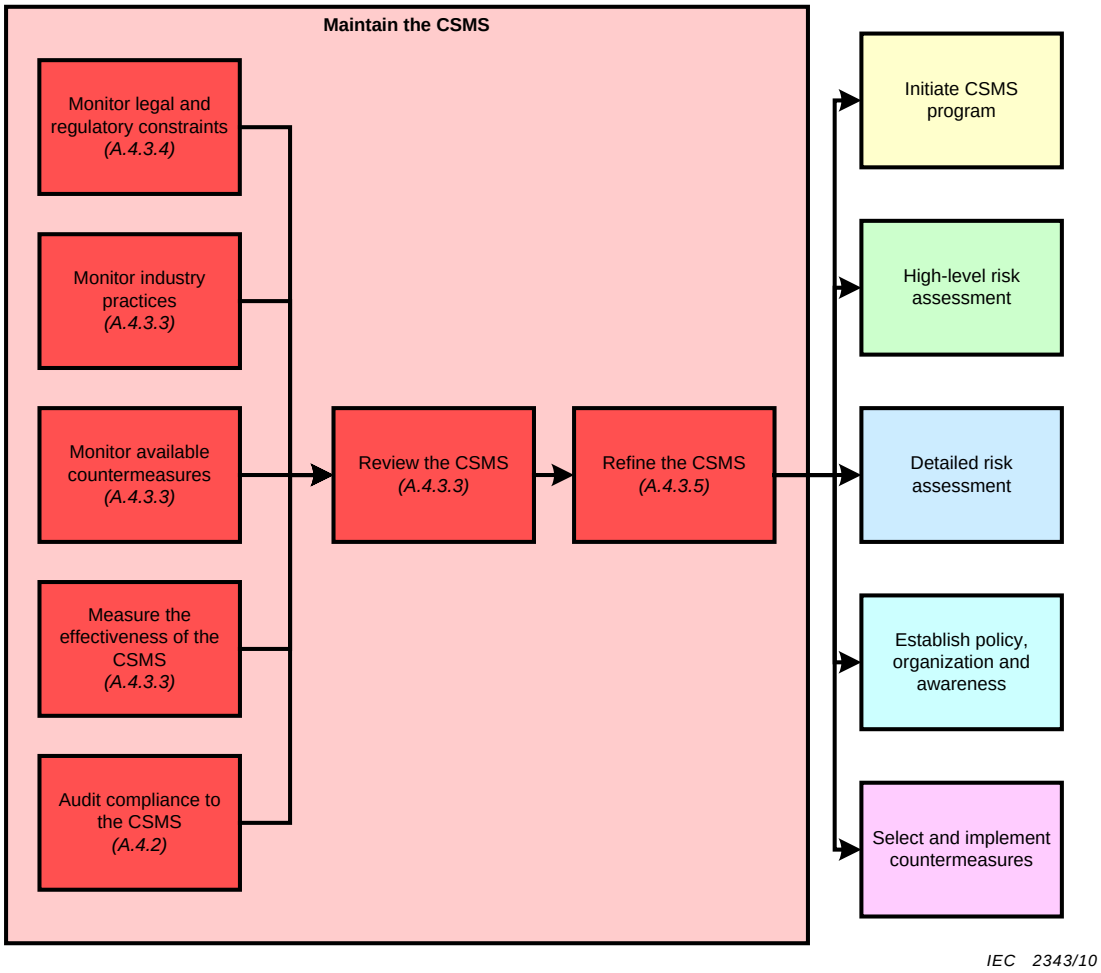



**Figure B.8 – Activities and dependencies for activity: Maintain the CSMS**

# Annex C
(informative)

# Mapping of requirements to ISO/IEC 27001

## C.1 Overview

The requirements contained within this document are very similar to the requirements contained within ISO/IEC 27001 [24]. This standard, IEC 62443-2-1, was developed by reference to ISO/IEC 27001 and many cross-references are made throughout. However, this standard does not use the same organization to describe its requirements. This alternate organization was deliberate, resulting from a change made during the development of the standard in response to initial IACS end-user reviewers, to aid user readability by combining similar requirements into larger subclauses and by providing considerable informative guidance in Annex A. Because many personnel with an information security background are already familiar with ISO/IEC 27001, this annex has been included to help those readers understand the similarities in the requirements of the two standards.

NOTE As a result of IEC national committee comments on the committee draft for vote (CDV) version of this standard, the normative body of the next edition of this standard will better reflect the organization of ISO/IEC 27001, with much of the previously requested IACS user guidance relegated to informative annexes. Work on the next edition of this standard will begin after adoption of this edition.

This annex contains two tables of requirements mappings. The first table contains the requirements in this standard and shows their related references from the ISO/IEC 27001 standard. The second table contains the requirements in ISO/IEC 27001 and shows their related references from this standard. The mapping of requirements is at a subclause level and does not represent an exhaustive analysis of all the detailed requirements. A more detailed analysis of the requirements may be done in a future revision to this standard.

## C.2 Mapping of this standard to ISO/IEC 27001:2005

Table C.1 shows a mapping of the requirements in this standard at a subclause level to portions of ISO/IEC 27001:2005.

NOTE A revision to ISO/IEC 27001 has been written, but was not published at the writing of this standard. No attempt has been made to provide an updated mapping of the requirements in this standard to the newer version of ISO/IEC 27001.

**Table C.1 – Mapping of requirements in this standard to ISO/IEC 27001 references**

| IEC 62443-2-1 requirement | Related ISO/IEC 27001 references |
|---|---|
| 4.2.2 Business rationale | 4.2.1e) Analyze and evaluate the risks<br>5.2.1 Provision of resources |
| 4.2.3 Risk identification, classification and assessment | 4.2.1c) Risk assessment approach<br>4.2.1d) Identify the risks<br>4.2.1e) Analyse and evaluate the risks<br>4.3.1 General document requirements<br>A.6.2 External parties<br>A.7.1 Responsibility for assets |
| 4.3.2.2 CSMS Scope | 4.2.1a) Scope and boundaries of ISMS<br>4.3.1 General document requirements |

**Table C.1** *(continued)*

| IEC 62443-2-1 requirement | Related ISO/IEC 27001 references |
|---|---|
| 4.3.2.3 Organizing for security | 4.2.1b) ISMS policy<br>4.2.1i) Obtain management authorization to implement and operate the ISMS<br>4.2.2a) Formulate a risk treatment plan<br>4.2.2b) Implement the risk treatment plan<br>4.2.2g) Manage resources for the ISMS<br>5.1 Management commitment<br>5.2.1 Provision of resources<br>A.6.1 Internal organization |
| 4.3.2.4 Staff training and security awareness | 4.2.2e) Implement training and awareness programs<br>5.2.2 Training, awareness and competence<br>A.8.2 Human resources security – During employment |
| 4.3.2.5 Business continuity plan | 4.3.2 Control of documents<br>4.3.3 Control of records<br>A.9.1 Secure areas<br>A.9.2 Equipment security<br>A.14.1 Information security aspects of business continuity management |
| 4.3.2.6 Security policies and procedures | 4.2.1b) ISMS policy<br>4.2.1h) Obtain management approval of the proposed residual risks<br>4.2.1i) Obtain management authorization to implement and operate the ISMS<br>4.2.2d) Define how to measure the effectiveness of the selected controls<br>4.3.1 General document requirements<br>4.3.2 Control of documents<br>7.1 Management review of the ISMS |
| 4.3.3.2 Personnel security | A.6.1 Internal organization<br>A.6.2 External parties<br>A.8.1 Human resources security – Prior to employment<br>A.8.2 Human resources security – During employment<br>A.8.3 Human resources security – Termination or change of employment<br>A.10.1 Operational procedures and responsibilities |
| 4.3.3.3 Physical and environmental security | A.9.1 Secure areas<br>A.9.2 Equipment security<br>A.10.7 Media handling |
| 4.3.3.4 Network segmentation | A.10.1 Operational procedures and responsibilities<br>A.10.3 System planning and acceptance<br>A.10.6 Network security management<br>A.11.4 Network access control |
| 4.3.3.5 Access control: Account administration | A.11.1 Business requirement for access control<br>A.11.2 User access management |
| 4.3.3.6 Access control: Authentication | A.11.3 User responsibilities<br>A.11.4 Network access control<br>A.11.5 Operating system access control |

**Table C.1** *(continued)*

| IEC 62443-2-1 requirement | Related ISO/IEC 27001 references |
|---|---|
| 4.3.3.7 Access control: Authorization | A.11.6 Application and information access control<br>A.11.7 Mobile computing and teleworking |
| 4.3.4.2 Risk management and implementation | 4.2.1d) Identify the risks<br>4.2.1e) Analyse and evaluate the risks<br>4.2.1f) Identify and evaluate options for the treatment of risks<br>4.2.1g) Select control objectives and controls for the treatment of risks<br>4.2.1h) Obtain management approval of the proposed residual risks<br>4.2.1j) Prepare a Statement of Applicability<br>4.2.2b) Implement the risk treatment plan<br>4.2.2c) Implement controls<br>4.2.2d) Define how to measure the effectiveness of the selected controls<br>4.2.2h) Implement procedures and controls to detect and respond to security events<br>5.2.1 Provision of resources |
| 4.3.4.3 System development and maintenance | A.10.1 Operational procedures and responsibilities<br>A.10.2 Third party service delivery management<br>A.10.3 System planning and acceptance<br>A.10.4 Protection against malicious and mobile code<br>A.10.5 Back-up<br>A.10.6 Network security management<br>A.10.8 Exchange of information<br>A.10.9 Electronic commerce services<br>A.10.10 Monitoring<br>A.12.1 Security requirements of information systems<br>A.12.2 Correct processing in applications<br>A.12.3 Cryptographic controls<br>A.12.4 Security of system files<br>A.12.5 Security in development and support processes<br>A.12.6 Technical Vulnerability Management |
| 4.3.4.4 Information and document management | 4.3.1 General document requirements<br>4.3.2 Control of documents<br>4.3.3 Control of records<br>A.10.7 Media handling |
| 4.3.4.5 Incident planning and response | 4.2.2h) Implement procedures and controls to detect and respond to security events<br>4.3.2 Control of documents<br>A.13.1 Reporting information security events and weaknesses<br>A.13.2 Management of information security incidents and improvements |

**Table C.1** *(continued)*

| IEC 62443-2-1 requirement | Related ISO/IEC 27001 references |
|---|---|
| 4.4.2 Conformance | 4.2.2d) Define how to measure the effectiveness of the selected controls<br>4.2.3a) Execute monitoring and reviewing procedures and other controls<br>4.2.3c) Measure the effectiveness of controls<br>4.2.3e) Conduct internal ISMS audits at planned intervals<br>6 Internal ISMS audits<br>A.10.10 Monitoring<br>A.15.1 Compliance with legal requirements<br>A.15.2 Compliance with security policies and standards, and technical compliance<br>A.15.3 Information systems audit considerations |
| 4.4.3 Review, improve and maintain the CSMS | 4.2.2f) Manage operation of the ISMS<br>4.2.3a) Execute monitoring and reviewing procedures and other controls<br>4.2.3b) Undertake regular reviews of the effectiveness of the ISMS<br>4.2.3c) Measure the effectiveness of controls<br>4.2.3d) Review risk assessments, residual risks, and acceptable levels of risk at planned intervals<br>4.2.3f) Review the ISMS on a regular basis to determine if the scope remains adequate and improvements to the ISMS are identified<br>4.2.3g) Update security plans from monitoring and reviewing activities<br>4.2.3h) Record actions and events that could have an impact of the effectiveness or performance of the ISMS<br>4.2.4a) Implement the identified improvements of the ISMS<br>4.2.4b) Take appropriate corrective and preventive actions<br>4.2.4c) Communicate the actions and improvements to all interested parties<br>4.2.4d) Ensure that the improvements achieve their intended objectives<br>5.1 Management commitment<br>6 Internal ISMS audits<br>7.1 Management review of the ISMS<br>7.2 Review input for management review<br>7.3 Review output from a management review<br>8.1 Continual improvement of the ISMS<br>8.2 Corrective action<br>8.3 Preventive action<br>A.13.2 Management of information security incidents and improvements |

## C.3 Mapping of ISO/IEC 27001:2005 to this standard

Table C.2 contains the reverse mapping to that in Table C.1.

**Table C.2 – Mapping of ISO/IEC 27001 requirements to this standard**

| ISO/IEC 27001 requirement | Related IEC 62443 2 1 references |
|---|---|
| 4.2.1a) Scope and boundaries of ISMS | 4.3.2.2 CSMS Scope |
| 4.2.1b) ISMS policy | 4.3.2.3 Organizing for security<br>4.3.2.6 Security policies and procedures |
| 4.2.1c) Risk assessment approach | 4.2.3 Risk identification, classification and assessment |
| 4.2.1d) Identify the risks | 4.2.3 Risk identification, classification and assessment<br>4.3.4.2 Risk management and implementation |
| 4.2.1e) Analyse and evaluate the risks | 4.2.2 Business rationale<br>4.2.3 Risk identification, classification and assessment<br>4.3.4.2 Risk management and implementation |
| 4.2.1f) Identify and evaluate options for the treatment of risks | 4.3.4.2 Risk management and implementation |
| 4.2.1g) Select control objectives and controls for the treatment of risks | 4.3.4.2 Risk management and implementation |
| 4.2.1h) Obtain management approval of the proposed residual risks | 4.3.2.6 Security policies and procedures<br>4.3.4.2 Risk management and implementation |
| 4.2.1i) Obtain management authorization to implement and operate the ISMS | 4.3.2.3 Organizing for security<br>4.3.2.6 Security policies and procedures |
| 4.2.1j) Prepare a Statement of Applicability | 4.3.4.2 Risk management and implementation |
| 4.2.2a) Formulate a risk treatment plan | 4.3.2.3 Organizing for security |
| 4.2.2b) Implement the risk treatment plan | 4.3.2.3 Organizing for security<br>4.3.4.2 Risk management and implementation |
| 4.2.2c) Implement controls | 4.3.4.2 Risk management and implementation |
| 4.2.2d) Define how to measure the effectiveness of the selected controls | 4.3.2.6 Security policies and procedures<br>4.3.4.2 Risk management and implementation<br>4.4.2 Conformance |
| 4.2.2e) Implement training and awareness programs | 4.3.2.4 Staff training and security awareness |
| 4.2.2f) Manage operation of the ISMS | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.2g) Manage resources for the ISMS | 4.3.2.3 Organizing for security |
| 4.2.2h) Implement procedures and controls to detect and respond to security events | 4.3.4.2 Risk management and implementation<br>4.3.4.5 Incident planning and response |
| 4.2.3a) Execute monitoring and reviewing procedures and other controls | 4.4.2 Conformance<br>4.4.3 Review, improve and maintain the CSMS |
| 4.2.3b) Undertake regular reviews of the effectiveness of the ISMS | 4.4.3 Review, improve and maintain the CSMS |

**Table C.2** *(continued)*

| ISO/IEC 27001 requirement | Related IEC 62443-2-1 references |
|---|---|
| 4.2.3c) Measure the effectiveness of controls | 4.4.2 Conformance<br>4.4.3 Review, improve and maintain the CSMS |
| 4.2.3d) Review risk assessments, residual risks, and acceptable levels of risk at planned intervals | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.3e) Conduct internal ISMS audits at planned intervals | 4.4.2 Conformance |
| 4.2.3f) Review the ISMS on a regular basis to determine if the scope remains adequate and improvements to the ISMS are identified | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.3g) Update security plans from monitoring and reviewing activities | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.3h) Record actions and events that could have an impact of the effectiveness or performance of the ISMS | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.4a) Implement the identified improvements of the ISMS | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.4b) Take appropriate corrective and preventive actions | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.4c) Communicate the actions and improvements to all interested parties | 4.4.3 Review, improve and maintain the CSMS |
| 4.2.4d) Ensure that the improvements achieve their intended objectives | 4.4.3 Review, improve and maintain the CSMS |
| 4.3.1 General document requirements | 4.2.3 Risk identification, classification and assessment<br>4.3.2.2 CSMS Scope<br>4.3.2.6 Security policies and procedures<br>4.3.4.4 Information and document management |
| 4.3.2 Control of documents | 4.3.2.5 Business continuity plan<br>4.3.2.6 Security policies and procedures<br>4.3.4.4 Information and document management<br>4.3.4.5 Incident planning and response |
| 4.3.3 Control of records | 4.3.2.5 Business continuity plan<br>4.3.4.4 Information and document management |
| 5.1 Management commitment | 4.3.2.3 Organizing for security<br>4.4.2 Conformance<br>4.4.3 Review, improve and maintain the CSMS |
| 5.2.1 Provision of resources | 4.2.2 Business rationale<br>4.3.2.3 Organizing for security<br>4.3.4.2 Risk management and implementation |
| 5.2.2 Training, awareness and competence | 4.3.2.4 Staff training and security awareness |
| 6 Internal ISMS audits | 4.4.2 Conformance<br>4.4.3 Review, improve and maintain the CSMS |

**Table C.2** *(continued)*

| ISO/IEC 27001 requirement | Related IEC 62443-2-1 references |
|---|---|
| 7.1 Management review of the ISMS | 4.3.2.6 Security policies and procedures<br>4.4.3 Review, improve and maintain the CSMS |
| 7.2 Review input for management review | 4.4.3 Review, improve and maintain the CSMS |
| 7.3 Review output from a management review | 4.4.3 Review, improve and maintain the CSMS |
| 8.1 Continual improvement of the ISMS | 4.4.3 Review, improve and maintain the CSMS |
| 8.2 Corrective action | 4.4.3 Review, improve and maintain the CSMS |
| 8.3 Preventive action | 4.4.3 Review, improve and maintain the CSMS |
| A.5.1 Information security policy | No specific clause; control system security policies interpret and apply general policies to this environment |
| A.6.1 Internal organization | 4.3.2.3 Organizing for security<br>4.3.3.2 Personnel security |
| A.6.2 External parties | 4.2.3 Risk identification, classification and assessment<br>4.3.3.2 Personnel security |
| A.7.1 Responsibility for assets | 4.2.3 Risk identification, classification and assessment |
| A.7.2 Information classification | No specific clause; control system security policies interpret and apply general policies to this environment |
| A.8.1 Human resources security – Prior to employment | 4.3.3.2 Personnel security |
| A.8.2 Human resources security – During employment | 4.3.2.4 Staff training and security awareness<br>4.3.3.2 Personnel security |
| A.8.3 Human resources security – Termination or change of employment | 4.3.3.2 Personnel security |
| A.9.1 Secure areas | 4.3.2.5 Business continuity plan<br>4.3.3.3 Physical and environmental security |
| A.9.2 Equipment security | 4.3.2.5 Business continuity plan<br>4.3.3.3 Physical and environmental security |
| A.10.1 Operational procedures and responsibilities | 4.3.3.2 Personnel security<br>4.3.3.4 Network segmentation<br>4.3.4.3 System development and maintenance<br>4.4.2 Conformance |
| A.10.2 Third party service delivery management | 4.3.4.3 System development and maintenance |
| A.10.3 System planning and acceptance | 4.3.3.4 Network segmentation<br>4.3.4.3 System development and maintenance |
| A.10.4 Protection against malicious and mobile code | 4.3.4.3 System development and maintenance |
| A.10.5 Back-up | 4.3.4.3 System development and maintenance |

**Table C.2** *(continued)*

| ISO/IEC 27001 requirement | Related IEC 62443-2-1 references |
|---|---|
| A.10.6 Network security management | 4.3.3.4 Network segmentation<br>4.3.4.3 System development and maintenance |
| A.10.7 Media handling | 4.3.3.3 Physical and environmental security<br>4.3.4.4 Information and document management |
| A.10.8 Exchange of information | 4.3.4.3 System development and maintenance |
| A.10.9 Electronic commerce services | 4.3.4.3 System development and maintenance |
| A.10.10 Monitoring | 4.3.4.3 System development and maintenance<br>4.4.2 Conformance |
| A.11.1 Business requirement for access control | 4.3.3.5 Access control: Account administration |
| A.11.2 User access management | 4.3.3.5 Access control: Account administration |
| A.11.3 User responsibilities | 4.3.3.6 Access control: Authentication |
| A.11.4 Network access control | 4.3.3.4 Network segmentation<br>4.3.3.6 Access control: Authentication |
| A.11.5 Operating system access control | 4.3.3.6 Access control: Authentication |
| A.11.6 Application and information access control | 4.3.3.7 Access control: Authorization |
| A.11.7 Mobile computing and teleworking | 4.3.3.7 Access control: Authorization |
| A.12.1 Security requirements of information systems | 4.3.4.3 System development and maintenance |
| A.12.2 Correct processing in applications | 4.3.4.3 System development and maintenance |
| A.12.3 Cryptographic controls | 4.3.4.3 System development and maintenance |
| A.12.4 Security of system files | 4.3.4.3 System development and maintenance |
| A.12.5 Security in development and support processes | 4.3.4.3 System development and maintenance |
| A.12.6 Technical Vulnerability Management | 4.3.4.3 System development and maintenance |
| A.13.1 Reporting information security events and weaknesses | 4.3.4.5 Incident planning and response |
| A.13.2 Management of information security incidents and improvements | 4.3.4.5 Incident planning and response<br>4.4.3 Review, improve and maintain the CSMS |
| A.14.1 Information security aspects of business continuity management | 4.3.2.5 Business continuity plan |
| A.15.1 Compliance with legal requirements | 4.4.2 Conformance |
| A.15.2 Compliance with security policies and standards, and technical compliance | 4.4.2 Conformance |
| A.15.3 Information systems audit considerations | 4.4.2 Conformance |

# Bibliography

NOTE This bibliography includes references to sources used in the creation of this standard as well as references to sources that may aid the reader in developing a greater understanding of cyber security as a whole and developing a management system. Not all references in this bibliography are referred to throughout the text of this standard. The references have been broken down into different categories depending on the type of source they are.

## References to other parts, both existing and anticipated, of the IEC 62443 series:

NOTE Some of these references are normative references (see Clause 2), published documents, in development, or anticipated. They are all listed here for completeness of the anticipated parts of the IEC 62443 series.

[1] IEC/TS 62443-1-1[2], *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[2] IEC/TR 62443-1-2[4], *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations*

[3] IEC/TR 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*

NOTE This standard is IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2 1: Establishing an industrial automation and control system security program*

[4] IEC 62443-2-2[5], *Industrial communication networks – Network and system security – Part 2-2: Operating an industrial automation and control system security program*

[5] IEC/TR 62443-2-3[4], *Industrial communication networks – Network and system security – Part 2-3: Patch management in the IACS environment*

[6] IEC/TR 62443-3-1, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

[7] IEC 62443-3-2[4], *Industrial communication networks – Network and system security – Part 3-2: Target security assurance levels for zones and conduits*

[8] IEC 62443-3-3[4], *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security assurance levels*

[9] IEC 62443-3-4[4], *Industrial communication networks – Network and system security – Part 3-4: Product development requirements*

[10] IEC 62443-4-1[4], *Industrial communication networks – Network and system security – Part 4-1: Embedded devices*

[11] IEC 62443-4-2[4], *Industrial communication networks – Network and system security – Part 4-2: Host devices*

[12] IEC 62443-4-3[4], *Industrial communication networks – Network and system security – Part 4-3: Network devices*

---

4 Under development.

5 Planned companion to this international standard.

[13] IEC 62443-4-4[4], *Industrial communication networks – Network and system security – Part 4-4: Application, data and functions*

**Other standards references:**

[14] IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

[15] IEC 61512-1, *Batch Control, Part 1: Models and terminology*

[16] IEC 62264-1, *Enterprise-Control System Integration, Part 1: Models and terminology*

[17] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*

[18] ISO/IEC 10746-1, *Information technology – Open distributed processing – Reference model: Overview*

[19] ISO/IEC 10746-2, *Information technology – Open distributed processing – Reference model: Foundations*

[20] ISO/IEC 15408-1:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

[21] ISO/IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

[22] ISO/IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

[23] ISO/IEC 17799, *Information technology – Security techniques – Code of practice for information security management*

[24] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

[25] 29 CFR 1910.119 – *U.S. Occupational Safety and Health Standards – Hazardous Materials – Process safety management of highly hazardous chemicals*

**Industry-specific and sector-specific references:**

[26] Guidance for Addressing Cyber Security in the Chemical Sector, Version 3.0, May 2006, American Chemistry Council's Chemical Information Technology Center (ChemITC), available at <http://www.chemicalcybersecurity.com/>

[27] Report on Cyber Security Vulnerability Assessments Methodologies, Version 2.0, November 2004, ChemITC, available at <http://www.chemicalcybersecurity.com/>

[28] Cyber Security Architecture Reference Model, Version 1.0, August 2004, ChemITC, available at <http://www.chemicalcybersecurity.com/>

[29] Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods, November 2004, ChemITC, available at <http://www.chemicalcybersecurity.com/>

[30] U.S. Chemicals Sector Cyber Security Strategy, September 2006, available at <http://www.chemicalcybersecurity.com/>

**Other documents and published resources:**

[31] Carlson, Tom, *Information Security Management: Understanding ISO 17799*, 2001, available at <http://www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf>

[32] Purdue Research Foundation, A Reference Model for Computer Integrated Manufacturing, 1989, ISBN 1-55617-225-7

[33] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002

[34] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004

[35] NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003

[36] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004

[37] NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, March 2006, Draft

[38] NIST Process Control Security Requirements Forum (PCSRF), Industrial Control System – System Protection Profile (ICS-SPP)

[39] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration (CMMI) for Software Engineering*, v1.1, August 2002

**Websites:**

[40] NASA/Science Office of Standards and Technology (NOST), available at <http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html>

[41] Zachmann Enterprise Reference Model, available at <http://www.zifa.com/>

[42] Sarbanes – Oxley Web site, available at <http://www.sarbanes-oxley.com/>

[43] Sans Web site, available at <http://www.sans.org/>

[44] MIS Training Institute, available at <http://www.misti.com/>

[45] U.S. National Institute of Standards & Technology, available at <http://www.nist.gov/>

[46] Information Systems Technology Audit Programs, available at <http://www.auditnet.org/asapind.htm>

[47] NIST eScan Security Assessment, available at <https://www.mepcenters.nist.gov/escan/>

[48] American National Standards Institute, available at <http://www.ansi.org/>

[49] IDEAL Model, available at <http://www.sei.cmu.edu/ideal/ideal.html>

[50] Control Objectives for Information and Related Technology (COBIT), available at <http://www.isaca.org/>

[51] Corporate Governance Task Force “Information Security Governance- A call to action”, available at <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>

[52] Michigan State Cybersecurity Definitions, available at <http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html>

[53] The Free Internet Encyclopedia – Wikipedia, available at <http://www.wikipedia.org/>

[54] Bridgefield Group Glossary, available at <http://www.bridgefieldgroup.com/>

[55] Six Sigma Information, available at <http://www.onesixsigma.com/>

[56] Carnegie Mellon Software Engineering Institute, available at <http://www.sei.cmu.edu/>

[57] Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team (CERT), available at <http://www.cert.org/>

[58] SCADA and Control Systems Procurement Project, available at <http://www.msisac.org/scada/>

[59] Interoperability Clearinghouse, available at <http://www.ichnet.org/>

[60] New York State Financial Terminology, available at <http://www.budget.state.ny.us/citizen/financial/glossary_all.html>

[61] Search Windows Security, available at <http://www.searchwindowssecurity.com/>

[62] Chemical Sector Cyber Security Program, available at <http://www.chemicalcybersecurity.com/>

[63] TechEncyclopedia, available at <http://www.techweb.com/encyclopedia/>

———————

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

## Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62443-2-1 a été établie par le comité d'études 65 de la CEI: Mesure, commande et automatisation dans les processus industriels.

La présente version bilingue (2012-04) correspond à la version anglaise monolingue publiée en 2010-11.

Le texte anglais de cette norme est issu des documents 65/457/FDIS et 65/461/RVD.

Le rapport de vote 65/461/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties existantes de la série de normes CEI 62443, publiée sous le titre générique *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*, est disponible sur le site internet de la CEI. La liste complète des parties existantes et prévues est également disponible dans la Bibliographie de cette norme.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

NOTE La révision de la présente norme internationale commencera peu après sa publication. La prochaine révision sera alignée plus étroitement sur l'ISO/CEI 27001, qui aborde de nombreux problèmes identiques, mais sans prendre en compte les exigences spécialisées concernant la poursuite du fonctionnement et la sécurité, courantes dans l'environnement des automatismes industriels et des systèmes de commande.

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

# 0 INTRODUCTION

## 0.1 Vue d'ensemble

La cyber-sécurité est un sujet dont l'importance ne cesse de prendre de l'ampleur dans les organisations modernes. De nombreuses organisations concernées par le traitement de l'information (IT) se soucient de la cyber-sécurité depuis de nombreuses années et ont mis en place des systèmes de gestion de cyber-sécurité (CSMS) reconnus, tels que ceux définis par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) (voir ISO/CEI 17799 [23][1] et ISO/CEI 27001 [24]). Ces systèmes de gestion fournissent aux organisations une méthode bien établie pour protéger leurs actifs des cyber-attaques.

Les organisations utilisant des systèmes d'automatisation et de commande industrielle (IACS) ont commencé à utiliser la technologie disponible dans le commerce (COTS) développée pour les systèmes professionnels dans leurs procédés journaliers, ce qui a occasionné une multiplication des cyber-attaques contre les systèmes IACS. Ces systèmes ne sont généralement pas aussi robustes, dans l'environnement IACS, que le sont les systèmes spécifiquement conçus pour traiter les cyber-attaques, et ce pour de nombreuses raisons. Cette faiblesse peut avoir des conséquences sur la santé, la sécurité et l'environnement (HSE).

Les organisations peuvent essayer d'utiliser les solutions existantes de cyber-sécurité informatiques et professionnelles pour résoudre la sécurité des IACS, sans comprendre les conséquences. Nombre de ces solutions peuvent être appliquées aux équipements IACS, mais elles doivent l'être de façon correcte pour éviter toute conséquence désastreuse.

## 0.2 Un système de gestion de la cyber-sécurité pour les équipements IACS

Les systèmes de gestion fournissent habituellement des indications sur ce qu'un système de gestion doit inclure, mais n'indique pas la façon dont le système de gestion doit être développé. La présente norme traite des aspects concernant les éléments inclus dans un CSMS d'IACS et fournit des indications sur la façon de développer le CSMS pour l'IACS.

En général, lorsque l'on se trouve confronté à un problème difficile, 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 aborder les risques liés à la cyber-sécurité des IACS. Cependant, l'erreur fréquemment commise pour aborder les risques liés à la cyber-sécurité consiste à traiter la cyber-sécurité d'un système à la fois. La cyber-sécurité est un défi beaucoup plus vaste qui oblige à prendre en compte l'ensemble complet des 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 nécessite une évolution culturelle de l'organisation.

Traiter la cyber-sécurité au niveau d'une organisation complète peut sembler une tâche impossible. Malheureusement, il n'existe pas de livre de recettes simples pour la sécurité. Il y a une excellente raison à cela. Il n'y a pas 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, en réalité, est un équilibre entre les risques et les coûts. Aucune situation ne ressemble à une autre. Dans certains cas, le risque peut être lié aux facteurs HSE plutôt qu'à un impact purement économique. Le risque peut être une conséquence irréversible plutôt qu'un contretemps financier temporaire. Par conséquent, un recueil de recettes donnant les pratiques de sécurité obligatoires serait soit trop restrictif et sans doute très coûteux à suivre, soit insuffisant pour prendre en compte le risque.

---

[1] Les nombres entre crochets font référence à la Bibliographie.

### 0.3 Relations entre la présente norme et l'ISO/CEI 17799 et l'ISO/CEI 27001

Les normes ISO/CEI 17799 [23] et ISO/CEI 27001 [24] sont d'excellentes normes décrivant un système de gestion de cyber-sécurité pour des systèmes professionnels de traitement de l'information. Une grande partie du contenu de ces normes est également valable pour les IACS. La présente norme met l'accent sur la nécessité d'une uniformité entre les pratiques de gestion de la cyber-sécurité des IACS et les pratiques de gestion de la cyber-sécurité des systèmes professionnels de traitement de l'information. L'uniformisation de ces programmes permettra de réaliser des économies. Les utilisateurs de la présente norme sont invités à consulter les normes ISO/CEI 17799 et ISO/CEI 27001 pour toute information de support complémentaire. La présente norme se fonde sur les indications fournies par ces normes ISO/CEI. Elle aborde certaines différences importantes entre les IACS et les systèmes professionnels généraux de traitement de l'information. Elle sensibilise le lecteur au concept essentiel selon lequel les risques liés à la cyber-sécurité des IACS peuvent avoir des implications HSE et il convient pour traiter ces risques de l'intégrer aux pratiques existantes de gestion des risques.

# RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

## Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

## 1 Domaine d'application

La présente partie de la CEI 62443 définit les éléments nécessaires à l'établissement d'un système de gestion de la cyber-sécurité (CSMS) pour les systèmes d'automatisation et de commande (IACS) industriels et fournit des indications sur la façon de développer ces éléments. La présente norme utilise, au sens large, la définition et le domaine d'application de ce qui constitue un IACS décrit dans la CEI/TS 62443-1-1.

Les éléments d'un CSMS décrits dans la présente norme sont essentiellement liés aux politiques, aux procédures, aux pratiques et au personnel; ils correspondent à ce doit être inclus ou à ce qu'il convient d'inclure dans le CSMS final de l'organisation.

NOTE 1 D'autres documents de la série CEI 62443 et de la Bibliographie décrivent plus en détail des technologies et/ou des solutions spécifiques pour la cyber-sécurité.

Les indications fournies sur la façon de développer un CSMS le sont à titre d'exemple. Elles représentent l'opinion de l'auteur concernant la façon dont une organisation doit s'y prendre pour développer les éléments, et peuvent ne pas fonctionner dans toutes les situations. Les utilisateurs de la présente norme doivent lire attentivement les exigences et appliquer les indications de façon appropriée afin de développer un CSMS entièrement fonctionnel pour une organisation. Il convient que les politiques et les procédures décrites dans cette norme soient adaptées aux besoins de l'organisation.

NOTE 2 Il peut y avoir le cas où un CSMS est déjà en place et où l'on ajoute la partie IACS, comme le cas où l'organisation n'a jamais créé formellement de CSMS. Les auteurs de la présente norme ne peuvent pas prévoir tous les cas dans lesquels l'organisation établira un CSMS pour l'environnement des IACS, aussi la présente norme n'a-t-elle pas vocation de proposer une solution pour tous les cas.

## 2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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[2] – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

## 3 Termes, définitions, termes abrégés, acronymes et conventions

### 3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI/TS 62443-1-1 ainsi que les suivants s'appliquent.

---

[2] Cette norme est issue de la norme ANSI/ISA 99.02.01:2009, qu'elle remplace entièrement pour l'utilisation internationale. Il est attendu que la deuxième édition de la CEI/TS 62443-1-1 soit une Norme internationale, non une TS, après inclusion de certaines exigences normatives auxquelles il est possible de se conformer.

**3.1.1**
**compte d'accès**
fonction de contrôle d'accès permettant à l'utilisateur d'accéder à un ensemble particulier de données ou de fonctions pour un certain équipement

NOTE La plupart du temps, les comptes sont liés à des identifications d'utilisateur (ID) et des mots de passe. Ces ID d'utilisateur et ces mots de passe peuvent être liés à un individu ou un groupe d'individus, tel que l'équipe de travail d'une salle de commande effectuant le même ensemble de tâches opérationnelles.

**3.1.2**
**pratiques administratives**
pratiques/procédures définies et documentées, que les individus ont la responsabilité personnelle de suivre à tout moment

NOTE Ces pratiques figurent habituellement dans les conditions d'embauche de l'organisation. Dans l'environnement IACS, elles ont souvent des implications HSE.

**3.1.3**
**actif**
objet physique ou logique possédé par une organisation ou sous la garde de celle-ci, ayant une valeur perçue ou réelle pour cette organisation

[IEC/TS 62443-1-1, 3.2.6]

NOTE Dans le cas qui nous concerne, un actif est n'importe quel élément qu'il convient de protéger en tant que partie du CSMS.

**3.1.4**
**authentification**
mesure de sécurité destinée à établir la validité d'une émission, d'un message ou d'un émetteur, ou moyen de vérifier l'autorisation d'un individu à recevoir des catégories spécifiques d'informations

[IEC/TS 62443-1-1, 3.2.13]

**3.1.5**
**système de gestion de brûleur**
système assurant, en toute sécurité, le démarrage, la surveillance et la fermeture des systèmes de brûleurs associés à des chaudières, des fusées éclairantes, des incinérateurs, des turbines à gaz, des oxydants thermiques et de tout autre équipement mis à feu

**3.1.6**
**plan de continuité d'activité**
document contenant des procédures identifiées destinées à la récupération après une interruption de grande ampleur et à la reprise de l'activité

NOTE 1 Ce terme général désigne également d'autres aspects de la reprise après sinistre, tels que la gestion des urgences, les ressources humaines et les relations avec les médias ou la presse.

NOTE 2 Un plan de continuité d'activité identifie également les procédures destinées à maintenir le déroulement des opérations essentielles pendant que l'on assure la reprise des activités après une interruption de grande ampleur.

**3.1.7**
**planification de continuité d'activité**
processus consistant à développer un plan de continuité d'activité

**3.1.8**
**gestion des changements**
processus consistant à contrôler et documenter tout changement dans un système afin de maintenir le bon fonctionnement de l'équipement sous contrôle

**3.1.9**
**adhésion**
respect des exigences contenues dans une norme par une autre norme

Adapté de [ISO/CEI 10746-2, 15.1]

NOTE Il s'agit d'une relation entre deux spécifications, A et B, qui est vérifiée lorsque la spécification A émet des exigences qui sont remplies par la spécification B (lorsque B adhère à A).

**3.1.10**
**conformité**
relation entre une mise en œuvre et une norme, selon laquelle toute proposition qui est vraie dans la norme doit être vraie dans sa mise en œuvre

Adapté de [ISO/CEI 10746-2, 15.1]

NOTE La relation de conformité est vérifiée lorsque les exigences spécifiques de la spécification (les exigences de conformité) sont remplies par la mise en œuvre. L'évaluation de conformité est le processus au moyen duquel on détermine cette relation.

**3.1.11**
**conséquence**
le résultat d'un incident particulier

**3.1.12**
**critique**
dispositif, système informatique, processus ou autre, à caractère essentiel, qui, s'il était touché par un incident, pourrait avoir un impact financier ou un impact sur la santé, la sécurité ou l'environnement (HSE) élevé pour l'organisation

**3.1.13**
**système de gestion de la cyber-sécurité**
programme conçu par une organisation pour maintenir la cyber-sécurité de l'ensemble des actifs de l'organisation à un niveau établi de confidentialité, d'intégrité et de disponibilité, qu'ils se trouvent du côté de l'activité ou du côté IACS de l'organisation

**3.1.14**
**exigences des dispositifs**
caractéristiques de contre-mesure que doivent vérifier les dispositifs présents dans une zone pour atteindre le niveau de sécurité cible souhaité

**3.1.15**
**gardien**
individu de confiance que la direction supérieure consulte pour établir la priorité des problèmes qu'elle doit résoudre, par rapport aux autres problèmes que d'autres personnes seront plus à même de résoudre

**3.1.16**
**santé, sécurité et environnement**
responsabilité de protéger la santé et la sécurité des travailleurs et du personnel environnant et de maintenir un niveau de respect élevé de l'environnement

**3.1.17**
**interface homme machine**
ensemble des moyens avec lesquels les personnes (les utilisateurs) interagissent avec une machine, un dispositif, un programme informatique ou tout autre outil complexe (le système)

NOTE Dans de nombreux cas, il s'agit d'écrans vidéo ou de terminaux informatiques, de boutons poussoirs, de signaux sonores, de voyants clignotants ou autre. L'interface homme/machine offre des moyens:

- d'entrée, permettant à l'utilisateur de commander la machine;

- de sortie, permettant à la machine d'informer l'utilisateur.

**3.1.18**
**incident**
événement ne faisant pas partie du fonctionnement attendu d'un système ou d'un service, qui cause ou peut causer une interruption ou une réduction de la qualité du service fourni par le système

**3.1.19**
**audit indépendant**
examen d'une organisation (politiques, procédures, procédés, équipements, personnel ou autre) par un groupe externe indépendant de l'organisation

NOTE L'audit peut être obligatoire pour les entreprises publiques.

**3.1.20**
**traitement de l'information**
actifs informatiques d'une organisation, correspondant à des actifs non physiques, tels que des applications logicielles, des programmes de pilotage de procédés et des fichiers concernant le personnel

NOTE 1 Cette utilisation du terme de traitement de l'information n'est pas abrégée dans l'ensemble du présent document.

NOTE 2 Une autre utilisation du terme de traitement de l'information (IT) désigne l'organisation interne à l'entreprise (par exemple, le service informatique) ou les éléments habituellement pris en charge par ce service (c'est-à-dire les ordinateurs administratifs, les serveurs et l'infrastructure réseau). Cette utilisation du terme de traitement de l'information est abrégée par le sigle IT dans l'ensemble de la présente norme.

**3.1.21**
**système patrimonial**
système d'automatisation et de commande industriel existant dans une installation, qui peut ne pas se présenter sous forme d'élément disponible dans le commerce (COTS)

NOTE Un système patrimonial peut avoir été COTS à un moment donné, mais ne plus être disponible et/ou ne plus être pris en charge.

**3.1.22**
**vraisemblance**
estimation quantitative selon laquelle une action, un événement ou un incident peut se produire

**3.1.23**
**utilisateur local**
utilisateur se trouvant dans le périmètre de la zone de sécurité à laquelle on s'intéresse

NOTE Une personne se trouvant dans la zone de fabrication immédiate ou la salle de commande est un exemple d'utilisateur local.

**3.1.24**
**système d'exécution de fabrication**
système de programmation et de suivi de la production, servant à analyser et rapporter la disponibilité et l'état des ressources, à planifier et mettre à jour les commandes, à rassembler les données d'exécution détaillées telles que l'utilisation des matériaux, l'utilisation de la main-d'œuvre, les paramètres opérationnels, l'état des commandes et des équipements et toute autre information critique

NOTE 1 Ce système permet d'accéder aux bordereaux concernant les matériaux et le transport, et à d'autres données du système de base de planification des ressources de l'entreprise; il sert habituellement à l'émission de rapports concernant les ateliers et à la surveillance de ceux-ci, effectués en temps réel, dans le but de fournir au système de base des informations relatives à l'activité.

NOTE 2 Voir la CEI 62264-1 pour plus d'informations.

**3.1.25**
**adresse MAC**
adresse matérielle permettant de différencier un dispositif en réseau d'un autre

**3.1.26**
**opérateur**
type particulier d'utilisateur, habituellement responsable du bon fonctionnement de l'équipement sous son contrôle

**3.1.27**
**gestion des correctifs**
partie de la gestion des systèmes consistant à acquérir, soumettre à essai et installer différents correctifs (modifications de code) à un système informatique administré

NOTE Les tâches de gestion des correctifs consistent à: garder à jour la connaissance des correctifs disponibles, décider des correctifs appropriés pour les différents systèmes, s'assurer que les correctifs sont installés correctement, soumettre à essai les systèmes après installation et documenter toutes les procédures associées, telles que les configurations spécifiques requises à distance à travers les différents environnements hétérogènes en fonction des meilleures pratiques reconnues.

**3.1.28**
**ingénieur de procédé**
personne normalement responsable des aspects techniques de l'activité industrielle et qui utilise les IACS et d'autres outils pour superviser et gérer l'automatisation industrielle dans l'installation

**3.1.29**
**système de gestion de l'information des procédés**
ensemble de systèmes qui fournit des informations de support permettant d'assister le fonctionnement de l'installation

**3.1.30**
**automate programmable**
dispositif programmable à microprocesseur que l'on utilise dans l'industrie pour commander les chaînes de montage et les machines dans les ateliers, ainsi que de nombreux autres types d'équipements mécaniques, électriques et électroniques dans les usines

NOTE Habituellement programmé comme indiqué en [14], un automate programmable est conçu pour une utilisation en temps réel dans des environnements industriels rigoureux. Reliés à des capteurs et des actionneurs, les automates programmables sont caractérisés par le nombre et le type de ports d'E/S qu'ils fournissent et par leur vitesse de balayage d'E/S.

**3.1.31**
**gestion de la sécurité des procédés**
régulation destinée à prévenir les sinistres dans les systèmes chimiques et biotechnologiques par la réalisation d'une conception sûre aux niveaux de la technique et de la gestion

**3.1.32**
**accès distant**
communication avec des actifs ou des systèmes situés dans un périmètre défini, ou utilisation de ces actifs et ces systèmes, depuis tout emplacement situé en dehors de ce périmètre

**3.1.33**
**utilisateur distant**
utilisateur se trouvant en dehors du périmètre de la zone de sécurité à laquelle on s'intéresse

EXEMPLE Une personne située dans un bureau du même bâtiment, une personne se connectant sur le réseau longue portée (WAN) de l'entreprise et une personne se connectant sur les réseaux de l'infrastructure publique sont chacune un utilisateur distant.

**3.1.34**
**évaluation des risques**
processus consistant à identifier et évaluer les risques pour l'activité de l'organisation (y compris pour sa mission, ses fonctions, son image ou sa réputation), les actifs ou les individus de l'organisation en déterminant la vraisemblance d'apparition, l'impact résultant et les contre-mesures additionnelles qui seraient susceptibles d'atténuer cet impact

NOTE Synonyme d'analyse des risques; englobe les analyses des menaces et de la vulnérabilité.

**3.1.35**
**atténuation des risques**
actions destinées à réduire la vraisemblance et/ou la gravité d'un événement

**3.1.36**
**tolérance des risques**
risques que l'organisation est désireuse d'accepter

**3.1.37**
**auto-évaluation**
examen d'une organisation (c'est-à-dire, ses politiques, ses procédures, ses activités, ses équipements et son personnel) par un groupe interne à l'organisation

NOTE Ce groupe peut soit être directement associé au processus d'activité de l'organisation, soit appartenir à une autre partie de l'organisation, mais il convient qu'il ait une parfaite connaissance des risques associés à ce processus d'activité.

**3.1.38**
**Six Sigma®**
méthodologie orientée procédé, conçue pour améliorer les performances de l'activité en améliorant certains aspects spécifiques des procédés stratégiques de l'activité

**3.1.39**
**piratage psychologique**
pratique consistant à obtenir des informations confidentielles par manipulation d'utilisateurs légitimes

**3.1.40**
**partie prenante**
individu ou groupe ayant des intérêts dans le fait qu'une organisation réussisse à produire les résultats attendus et à maintenir la viabilité des produits et des services de l'organisation

NOTE Les parties prenantes ont une influence sur les programmes, les produits et les services. Dans le cas qui nous concerne, les parties prenantes sont les membres du personnel de l'organisation responsables de la mise en place et de la supervision du processus de cyber-sécurité. Ces personnes comprennent le directeur du programme de cyber-sécurité ainsi que l'équipe multifonctions d'individus issus de l'ensemble des départements concernés par le programme de cyber-sécurité.

**3.1.41**
**administrateur système**
personne(s) responsable(s) de la gestion de la sécurité du système informatique

NOTE Cette gestion peut comprendre la maintenance des systèmes d'exploitation, la gestion des réseaux, l'administration des comptes et la gestion des correctifs, conformément au processus de gestion des modifications.

**3.1.42**
**exigences système**
attributs du niveau de sécurité cible souhaité

**3.1.43**
**surveillance d'accès guidé**
procédure de surveillance des actions d'un utilisateur connecté à distance

**3.1.44**
**évaluation de la vulnérabilité**
description formelle et évaluation de la vulnérabilité d'un système

## 3.2 Abréviations et acronymes

Ce paragraphe définit les abréviations et les acronymes utilisés dans ce document.

| | |
|---|---|
| ANSI | Institut national américain de normalisation (*American National Standards Institute*) |
| CFR | Code américain des réglementations fédérales (*Code of Federal Regulations*) |
| ChemITC | Centre de traitement de l'information chimique du Conseil américain pour la chimie (*Chemical Information Technology Center of the American Chemistry Council)* |
| COTS | disponible dans le commerce (*Commercial off the shelf*) |
| CPU | Unité centrale (*Central processing unit*) |
| CSCSP | Programme de cyber-sécurité du secteur chimique (*Chemical Sector Cyber Security Program*) |
| CSMS | Système de gestion de la cyber-sécurité (*Cyber security management system*) |
| CSVA | Évaluation de la vulnérabilité de la cyber-sécurité (*Cyber security vulnerability assessment*) |
| DCS | Système à commande distribuée (*Distributed Control System*) |
| DMZ | Zone démilitarisée (*Demilitarized zone*) |
| DoS, DDoS | Refus de service (*Denial of service*), Refus de service distribué (*Distributed denial of service*) |
| FDN | Réseau de dispositifs de terrain (*Field device network*) |
| FTP | Protocole de transfert de fichier (*File transfer protocol*) |
| IHM | Interface homme/machine |
| HSE | Santé, sécurité et environnement (*Health, safety and environmental*) |
| HVAC | Chauffage, ventilation et climatisation (*Heating, ventilation, and air-conditioning*) |
| IACS | Système(s) d'automatisation et de commande industrielle (*Industrial automation and control system(s)*) |
| ID | Identification |
| CEI | Commission Électrotechnique Internationale |
| IEEE | Institut des ingénieurs électriciens et électroniciens (*Institute of Electrical and Electronics Engineers*) |
| IP | Protocole Internet (*Internet Protocol*) |
| ISA | Société internationale d'automatisation (*International Society of Automation*) |
| ISO | Organisation internationale de normalisation (*International Organization for Standardization*) |
| IT | Traitement de l'information (*Information technology*) |
| KPI | Indicateur(s) de performance clé(s) (*Key performance indicator(s)*) |
| LAN | Réseau local (*Local Area Network*) |
| MAC | Contrôle d'accès au support (*Media Access Control*) |
| MES | Système d'exécution de fabrication (Manufacturing execution system) |

| | |
|---|---|
| NERC | Conseil nord-américain pour la fiabilité électrique (*North American Electric Reliability Council*) (concerne les États-Unis et le Canada) |
| NIST | Institut national américain de technologie et des normes (*National Institute of Standards and Technology)* |
| OS | Système d'exploitation (*Operating system*) |
| PC | Ordinateur personnel (*Personal computer*) |
| PCN | Réseau de commande de processus (*Process control network*) |
| PCSRF | Forum des exigences de sécurité pour la commande de procédé du NIST (*Process Control Security Requirements Forum*) |
| PIM | Gestion des informations de traitement (*Process information management*) |
| PIN | Numéro d'identification personnel (*Personal identification number*) |
| PLC | Automate programmable (*Programmable logic controller*) |
| PSM | Gestion de la sécurité des procédés (*Process safety management*) |
| RAID | Ensemble redondant de disques indépendants (*Redundant array of independent disks*) |
| RCN | Réseau de commande réglementaire (*Regulatory control network*) |
| SANS | Institut pour l'administration des systèmes, les audits, la mise en réseau et la sécurité (*SysAdmin, Audit, Networking, and Security Institute*) |
| SCADA | Commande, surveillance et acquisition de données (*Supervisory control and data acquisition*) |
| SI | Système international d'unités |
| SIS | Système(s) équipé(s) pour la sécurité (*Safety instrumented system(s)*) |
| SoA | Déclaration d'applicabilité (*Statement of applicability*) |
| SOC | Conditions normalisées de fonctionnement (*Standard operating condition*) |
| SOP | Procédure normalisée d'utilisation (*Standard operating procedure*) |
| SP | Publication spéciale (*Special Publication*) (par le NIST) |
| SSL | Protocole SSL (*Secure Socket Layer*) |
| TCP | Protocole de contrôle d'émission (*Transmission control protocol*) |
| TR | Rapport technique (*Technical report*) |
| VLAN | Réseau local virtuel (*Virtual local area network*) |
| VPN | Réseau privé virtuel (*Virtual private network*) |
| WAN | Réseau étendu (*Wide area network*) |

### 3.3 Conventions

Les éléments d'un CSMS sont les suivants:

- l'objectif de l'élément,
- une description élémentaire de l'élément,
- une justification expliquant pourquoi l'élément est inclus et
- les exigences concernant cet élément.

Une présentation sous forme de tableau fournit une description et les exigences de chacun des éléments. Les exigences sont numérotées de la même façon que les paragraphes (mais ne constituent pas en elles-mêmes des paragraphes), de telle sorte que les exigences peuvent être consultées individuellement et sélectivement.

# 4 Éléments d'un système de gestion de la cyber-sécurité

## 4.1 Vue d'ensemble

Cet article présente les éléments dont est constitué un CSMS pour IACS. Ces éléments représentent ce qui doit être inclus et ce qu'il convient d'inclure dans le CSMS afin de protéger un IACS des cyber-attaques.

Les éléments sont présentés dans les trois catégories principales suivantes:

- Analyse des risques,
- Traitement du risque par le CSMS, et
- Surveillance et amélioration du CSMS.

Chacune de ces catégories est divisée à son tour en groupes d'éléments et/ou en éléments. La Figure 1 décrit la relation entre les catégories, les groupes d'éléments et les éléments.

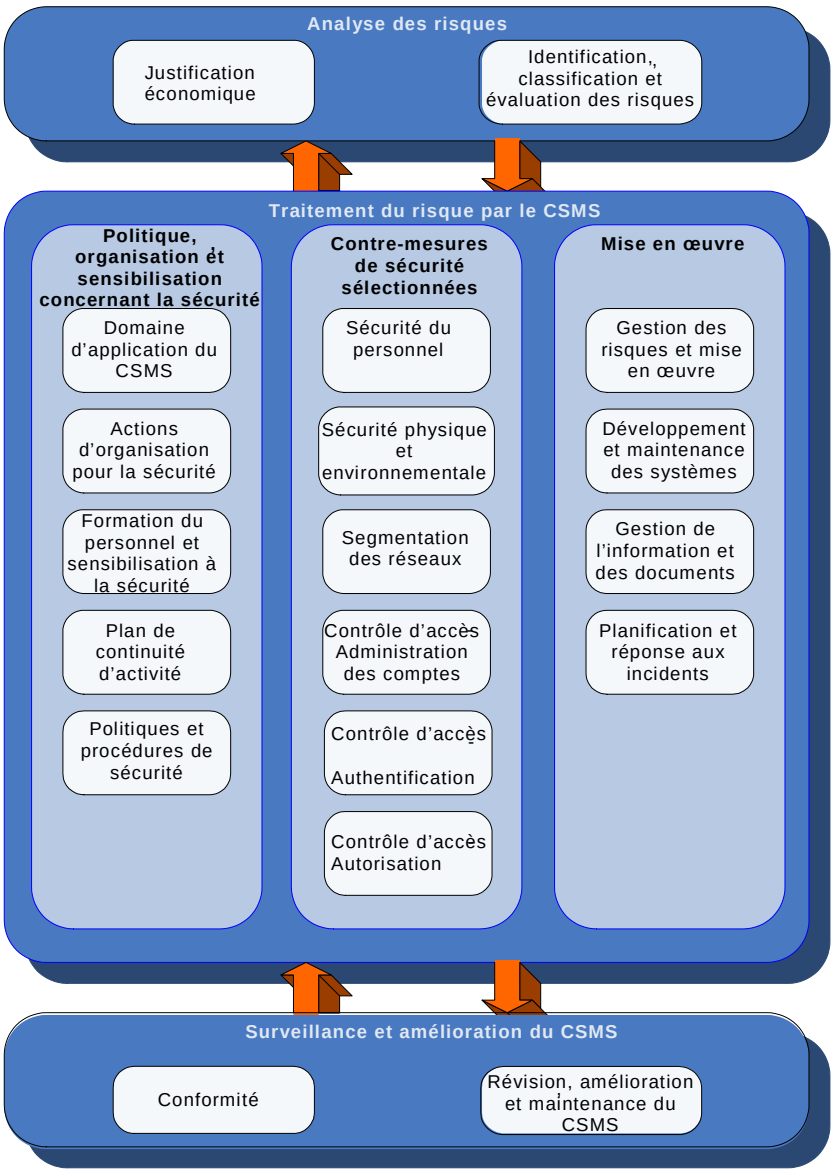



**Figure 1 – Représentation graphique des éléments d'un système de gestion de la cyber-sécurité**

Chaque élément de cet article contient l'objectif de l'élément, une description élémentaire de l'élément, une justification expliquant pourquoi l'élément a été inclus et les exigences concernant cet élément.

L'Annexe A est structurée à la base de la même façon que cet article, en catégories, groupes d'éléments et éléments. Cependant, l'annexe fournit des indications sur la façon de développer les éléments d'un CSMS. Il convient que le lecteur lise l'Annexe A pour comprendre les besoins et les problèmes particuliers liés au développement d'un CSMS pour IACS. Il convient d'adapter les indications de l'Annexe A aux exigences particulières de chacune des organisations.

La présente norme spécifie les éléments exigés dans un CSMS. Elle n'a pas pour vocation de spécifier un quelconque procédé séquentiel destiné à identifier et traiter les risques qui concernent ces éléments. L'organisation devra par conséquent créer ce procédé d'après sa culture, son mode d'organisation et l'état actuel de ses activités de cyber-sécurité. Pour aider les organisations dans cet aspect de l'application de la norme, A.3.4.2 donne un exemple de procédé d'identification et de traitement des risques. En outre, l'Annexe B donne un aperçu d'un ordonnancement efficace pour les activités liées à l'ensemble des éléments abordés dans la présente norme.

Si le CSMS est un excellent outil de gestion des risques pour les grandes entreprises, on peut également l'utiliser dans les petites entreprises. Le CSMS peut être davantage formalisé dans une grande entreprise, il peut donc être utilisé dans nombre de situations et géographies différentes. Dans une petite entreprise, il est nécessaire d'effectuer des activités CSMS similaires, mais celles-ci peuvent ne pas être aussi formelles. L'Article 4 et l'Annexe A donnent des indications qui aideront l'utilisateur à mieux comprendre les éléments et les activités d'un CSMS.

## 4.2 Catégorie: Analyse des risques

### 4.2.1 Description d'une catégorie

La première catégorie principale du CSMS est l'Analyse des risques. Cette catégorie donne la plupart des informations générales qui se répercutent dans de nombreux autres éléments du CSMS. La Figure 2 indique les deux éléments appartenant à cette catégorie:

- Justification économique et
- Identification, classification et évaluation des risques.

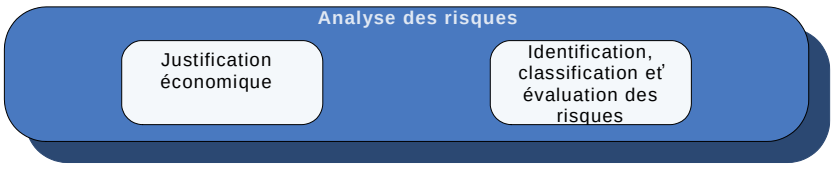



**Figure 2 – Représentation graphique de la catégorie: Analyse des risques**

### 4.2.2 Élément: Justification économique

**Objectif:**

Identifier et documenter les besoins particuliers d'une organisation en ce qui concerne le traitement des cyber-risques encourus par les IACS.

**Description:**

La justification économique repose sur la nature et l'ampleur des conséquences potentielles de type financier, HSE ou autre au cas où les IACS subiraient des cyber-incidents.

**Justification:**

Il est essentiel d'établir une justification économique pour permettre à une organisation de maintenir sa gestion des approvisionnements à un niveau approprié pour le programme de cyber-sécurité des IACS.

**Exigences:**

**Tableau 1 – Justification économique: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.2.2.1** | **Développer une justification économique** | Il convient que l'organisation développe une justification économique de haut niveau, servant de base à ses efforts pour assurer la cyber-sécurité des IACS et qui aborde les particularités de la dépendance de l'organisation vis à vis des IACS. |

### 4.2.3 Élément: Identification, classification et évaluation des risques

**Objectif:**

Identifier l'ensemble des cyber-risques liés aux IACS auxquels l'organisation est exposée et évaluer la vraisemblance et la gravité de ces risques.

**Description:**

Les organisations protègent leur capacité à remplir leur mission en identifiant, hiérarchisant et analysant, d'une manière systématique, les menaces, vulnérabilités et conséquences potentielles au moyen de méthodologies acceptées. Le premier ensemble d'exigences présente les actions entreprises par une organisation pour effectuer une évaluation des risques détaillée et de haut niveau qui englobe une évaluation de la vulnérabilité, dans un ordre chronologique type. Parmi ces exigences, celles liées à la préparation des évaluations des risques détaillées et de haut niveau sont indiquées en 4.2.3.1, 4.2.3.2 et 4.2.3.8 ci-dessous. Les autres exigences (4.2.3.10 à 4.2.3.14) sont des exigences générales qui s'appliquent au processus d'évaluation des risques global. Le paragraphe 4.3.4.2 décrit le processus consistant à prendre les mesures résultant de cette évaluation.

**Justification:**

L'objectif d'un investissement dans la cyber-sécurité est la réduction des risques; un tel objectif est motivé par la compréhension du niveau de risque et des potentielles atténuations.

**Exigences:**

**Tableau 2 – Identification, classification et évaluation des risques: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.2.3.1** | **Choisir une méthodologie d'évaluation des risques** | L'organisation doit choisir une approche et une méthodologie particulières pour l'évaluation et l'analyse des risques, qui permette d'identifier les risques et d'en établir la priorité d'après les menaces contre la sécurité, les vulnérabilités et les conséquences liées à leurs actifs IACS. |
| **4.2.3.2** | **Fournir les informations générales concernant l'évaluation des risques** | Il convient que l'organisation fournisse aux participants des informations appropriées, notamment une formation aux méthodologies, avant de commencer l'identification des risques. |

| Description | | Exigence |
|---|---|---|
| **4.2.3.3** | **Effectuer une évaluation des risques de haut niveau** | Une évaluation des risques système de haut niveau doit être effectuée pour permettre de comprendre les conséquences financières et HSE au cas où il aurait été porté atteinte à la disponibilité, l'intégrité ou la confidentialité de l'IACS. |
| **4.2.3.4** | **Identifier les IACS** | L'organisation doit identifier les différents IACS, rassembler des informations au sujet des dispositifs afin de caractériser la nature des risques pour la sécurité, et grouper les dispositifs en systèmes logiques. |
| **4.2.3.5** | **Développer des schémas de réseau simples** | L'organisation doit développer des schémas de réseau simples pour chacun des systèmes logiquement intégrés, qui montreront les principaux dispositifs, les types de réseau et l'emplacement des équipements. |
| **4.2.3.6** | **Établir la priorité des systèmes** | L'organisation doit développer les critères et attribuer un niveau de priorité pour atténuer les risques auxquels chacun des systèmes de commande logique est exposé. |
| **4.2.3.7** | **Effectuer une évaluation détaillée de vulnérabilité** | L'organisation doit effectuer une évaluation de vulnérabilité détaillée de ses IACS logiques individuels, dont le domaine d'application peut être déterminé par les résultats de l'évaluation des risques de haut niveau et la priorité établie pour les IACS soumis à ces risques. |
| **4.2.3.8** | **Identifier une méthodologie détaillée d'évaluation des risques** | La méthodologie d'évaluation des risques de l'organisation doit comprendre des méthodes permettant d'établir des priorités pour les vulnérabilités identifiées dans l'évaluation de la vulnérabilité détaillée. |
| **4.2.3.9** | **Effectuer une évaluation détaillée des risques** | L'organisation doit effectuer une évaluation des risques détaillée intégrant les vulnérabilités identifiées dans l'évaluation de la vulnérabilité détaillée. |
| **4.2.3.10** | **Identifier la fréquence des réévaluations et les critères de déclenchement** | L'organisation doit identifier la fréquence de réévaluation des risques et des vulnérabilités ainsi que les critères de déclenchement de la réévaluation d'après les évolutions liées à la technologie, l'organisation ou le mode de fonctionnement industriel. |
| **4.2.3.11** | **Intégrer les résultats des évaluations des risques physiques, HSE et de cyber-sécurité** | Les résultats des évaluations des risques physiques, HSE et de cyber-sécurité doivent être intégrés pour permettre de comprendre le risque global auquel les actifs sont exposés. |
| **4.2.3.12** | **Effectuer des évaluations de risques pendant tout le cycle de vie des IACS** | Des évaluations des risques doivent être effectuées à chacune des étapes du cycle de vie de la technologie, à savoir le développement, la mise en œuvre, les modifications et la mise hors service. |
| **4.2.3.13** | **Documenter l'évaluation des risques** | La méthodologie d'évaluation des risques et les résultats de l'évaluation des risques doivent être documentés. |
| **4.2.3.14** | **Maintenir des dossiers d'évaluation de la vulnérabilité** | Il convient de maintenir à jour des dossiers d'évaluation de la vulnérabilité pour tous les actifs dont est composé l'IACS. |

## 4.3 Catégorie: Traitement du risque par le CSMS

### 4.3.1 Description de la catégorie

La deuxième catégorie principale du CSMS est le Traitement du risque par le CSMS. Cette catégorie englobe l'ensemble des exigences et des informations contenues dans le CSMS. Elle comprend les trois groupes d'éléments suivants:

- Politique, organisation et sensibilisation concernant la sécurité;

- Contre-mesures sélectionnées pour la sécurité; et
- Mise en œuvre.

### 4.3.2 Groupe d'éléments: Politique, organisation et sensibilisation concernant la sécurité

#### 4.3.2.1 Description du groupe d'éléments

Le premier groupe d'éléments de cette catégorie traite du développement des politiques de cyber-sécurité fondamentales, s'intéresse aux organisations responsables de la cyber-sécurité et de la sensibilisation aux problèmes de cyber-sécurité, au sein de l'organisation. La Figure 3 est une représentation graphique des cinq éléments contenus dans ce groupe d'éléments:

- Domaine d'application du CSMS,
- Actions d'organisation pour la sécurité,
- Formation du personnel et sensibilisation concernant la sécurité,
- Plan de continuité d'activité, et
- Politiques et procédures de sécurité.

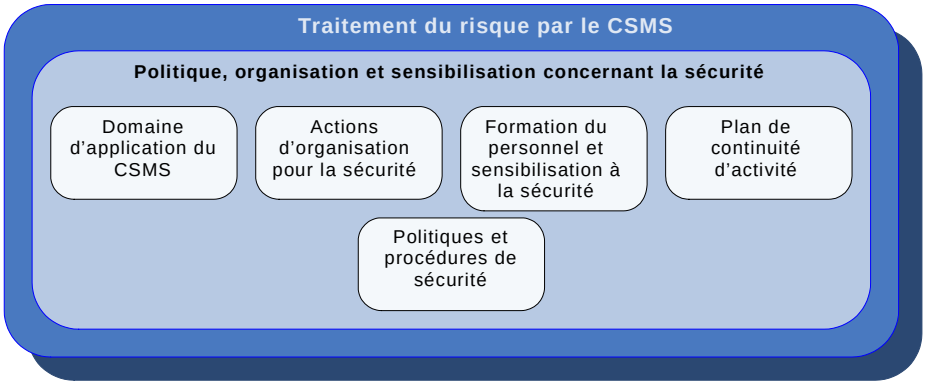



**Figure 3 – Représentation graphique du groupe d'éléments: Politique, organisation et sensibilisation concernant la sécurité**

#### 4.3.2.2 Élément: Domaine d'application du CSMS

**Objectif:**

Identifier, évaluer et documenter les systèmes, les processus et les organisations auxquels le CSMS s'applique.

**Description:**

Le domaine d'application englobe tous les aspects de l'IACS, les points d'intégration avec les partenaires d'activité, les clients et les fournisseurs.

**Justification:**

Il convient que la direction comprenne les limites dans lesquelles le CSMS s'applique à l'organisation et établir une orientation et des priorités pour le CSMS. En développant un domaine d'application clairement défini, la direction peut exprimer plus facilement ses buts et ses objectifs concernant le CSMS.

**Exigences:**

**Tableau 3 – Domaine d'application du CSMS: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.2.2.1** | **Définir le domaine d'application du CSMS** | L'organisation doit développer un domaine d'application formel écrit pour le programme de cyber-sécurité. |
| **4.3.2.2.2** | **Définir le contenu du domaine d'application** | Il convient que le domaine d'application explique les buts, processus et calendriers stratégiques du CSMS. |

### 4.3.2.3 Élément: Actions d'organisation pour la sécurité

**Objectif:**

Établir les entités responsables de gérer, mettre en place et évaluer la cyber-sécurité globale des actifs IACS de l'organisation.

**Description:**

La direction supérieure établit une organisation, une structure ou un réseau de personnes pour assurer une supervision et fournir des instructions concernant la gestion des risques de cyber-sécurité associés aux IACS. Elle fournit également le personnel nécessaire à l'exécution et l'évaluation des programmes de cyber-sécurité dans l'ensemble de l'organisation pour toute la durée de vie du CSMS. Une organisation, à n'importe quel niveau, peut mettre en œuvre cette norme, qu'il s'agisse d'une compagnie ou de l'ensemble d'une entreprise, d'une division, d'une usine ou d'un sous-ensemble d'une usine.

**Justification:**

L'implication dans un programme de sécurité commence au sommet de l'organisation. Étant donné que la cyber-sécurité des IACS nécessite différents ensembles de compétences que l'on ne trouve que rarement dans une section particulière ou un service particulier d'une organisation, il est impératif que la direction supérieure formule une approche pour gérer la sécurité, qui permette d'identifier clairement les responsabilités et fasse bon usage des compétences et de la main-d'œuvre. Cette approche peut prendre différentes formes, qu'il s'agisse d'une organisation en elle-même ou d'un réseau de personnes collaborant pour traiter différents aspects de la sécurité. L'approche choisie dépend étroitement de la culture opérationnelle de l'organisation.

**Exigences:**

**Tableau 4 – Actions d'organisation pour la sécurité: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.2.3.1** | **Obtenir l'appui de la direction supérieure** | L'organisation doit obtenir l'appui de la direction supérieure pour ce qui concerne le programme de cyber-sécurité. |
| **4.3.2.3.2** | **Établir la ou les organisations de sécurité** | Une organisation, une structure ou un réseau de parties prenantes, placé sous la direction supérieure, doit être établi (ou choisi) et se voir confier la responsabilité de fournir des instructions et une supervision claires pour les aspects de la cyber-sécurité des IACS. |
| **4.3.2.3.3** | **Définir les responsabilités organisationnelles** | Les responsabilités organisationnelles doivent être clairement définies pour la cyber-sécurité et les activités de sécurité physique qui y sont liées. |

| Description | | Exigence |
|---|---|---|
| **4.3.2.3.4** | **Définir la constitution de l'équipe des parties prenantes** | Il convient que l'équipe centrale concernée soit multifonctions par nature, et ainsi qu'elle détienne l'ensemble des compétences nécessaires à la prise en charge de la sécurité pour toutes les parties des IACS. |

### 4.3.2.4 Élément: Formation du personnel et sensibilisation à la sécurité

**Objectif:**

Fournir à l'ensemble du personnel (employés, intérimaires et sous-traitants) les informations permettant d'identifier, d'examiner, de prendre en charge et, s'il y a lieu, de corriger les vulnérabilités et les menaces subies par les IACS, et contribuer pour que leurs propres pratiques de travail utilisent des contre-mesures efficaces.

**Description:**

Il convient que l'ensemble du personnel reçoive une formation technique adéquate au sujet des menaces et des vulnérabilités connues liées au matériel, aux logiciels et au piratage psychologique.

**Justification:**

En ce qui concerne les IACS, il convient d'accorder autant d'importance à la cyber-sécurité qu'à la sûreté et l'intégrité de fonctionnement, car les conséquences peuvent en être tout aussi désastreuses. Sensibiliser l'ensemble du personnel à la sécurité est essentiel si l'on souhaite réduire les risques de cyber-sécurité. Un personnel informé et vigilant est l'une des meilleures lignes défensives pour la sécurisation d'un système. Il est donc essentiel que l'ensemble du personnel comprenne l'importance de la sécurité dans le maintien du bon fonctionnement du système.

**Exigences:**

**Tableau 5 – Formation du personnel et sensibilisation à la sécurité: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.2.4.1** | **Développer un programme de formation** | L'organisation doit concevoir et mettre en œuvre un programme de formation à la cyber-sécurité. |
| **4.3.2.4.2** | **Donner une formation aux procédures et aux installations** | L'ensemble du personnel (employés, intérimaires et sous-traitants) doit être formé initialement, puis périodiquement par la suite, aux procédures de sécurité correctes et à l'utilisation correcte des installations de traitement d'information. |
| **4.3.2.4.3** | **Assurer la formation du personnel de support** | Il convient que tous les membres du personnel travaillant à la gestion des risques, au développement des IACS, à l'administration/maintenance des systèmes et à d'autres tâches touchant le CSMS soient formés aux objectifs de sécurité et aux fonctions industrielles de ces tâches. |
| **4.3.2.4.4** | **Valider le programme de formation** | Il convient que le programme de formation soit validé continuellement pour permettre au personnel de comprendre le programme de sécurité et de recevoir la formation appropriée. |
| **4.3.2.4.5** | **Réviser le programme de formation au fil du temps** | Le programme de formation à la cyber-sécurité doit être révisé, si nécessaire, pour tenir compte des nouvelles menaces et vulnérabilités ou de l'évolution des menaces et vulnérabilités existantes. |

| Description | | Exigence |
|---|---|---|
| **4.3.2.4.6** | **Conserver les dossiers de formation des employés** | Il convient de tenir à jour les dossiers de formation des employés et des plans de mise à jour des formations, et de les consulter régulièrement. |

### 4.3.2.5 Élément: Plan de continuité d'activité

**Objectif:**

Identifier les procédures destinées à maintenir et/ou rétablir les opérations essentielles de l'activité pendant la résolution d'une interruption majeure.

**Description:**

Il convient qu'un plan de continuité d'activité contienne les objectifs de remise en état des différents systèmes et sous-systèmes impliqués en fonction des besoins typiques de l'activité, une liste des interruptions potentielles et les procédures de remise en état pour chacune d'elles, ainsi qu'un calendrier pour soumettre à essai une partie ou la totalité des procédures de remise en état. Il convient que l'un des principaux objectifs de la remise en état soit le maintien d'une disponibilité maximale du système de commande.

**Justification:**

Aucun ensemble de mesures de défense ne pourra prévenir toutes les interruptions dues aux incidents de cyber-sécurité. Un plan de continuité d'activité détaillé peut permettre de rétablir et d'utiliser les informations IACS dès que possible à la suite d'une interruption majeure.

**Exigences:**

**Tableau 6 – Plan de continuité d'activité: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.2.5.1** | **Spécifier les objectifs de remise en état** | Avant de créer un plan de continuité d'activité, l'organisation doit spécifier les objectifs de remise en état des systèmes concernés en fonction des besoins de l'activité. |
| **4.3.2.5.2** | **Déterminer l'impact et les conséquences pour chaque système** | Il convient que l'organisation détermine l'impact sur chaque système d'une interruption majeure et les conséquences liées à la perte d'un ou de plusieurs systèmes. |
| **4.3.2.5.3** | **Développer et mettre en œuvre des plans de continuité d'activité** | Des plans de continuité doivent être développés et mis en œuvre pour garantir que les processus d'activité puissent être rétablis en fonction des objectifs de remise en état. |
| **4.3.2.5.4** | **Constituer une équipe de poursuite d'activité** | Il convient de constituer une équipe de poursuite d'activité dont feront partie les propriétaires des IACS et des autres procédés. En cas d'interruption majeure, il convient que cette équipe détermine la priorité des systèmes d'activité et des systèmes IACS critiques pour rétablir les opérations. |
| **4.3.2.5.5** | **Définir et communiquer les rôles et responsabilités spécifiques** | Le plan de continuité d'activité doit définir et communiquer les rôles et responsabilités spécifiques pour chaque partie du plan. |
| **4.3.2.5.6** | **Créer des procédures de sauvegarde supportant le plan de continuité d'activité** | L'organisation doit créer des procédures de sauvegarde et de restauration (voir 4.3.4.3.9) supportant le plan de continuité d'activité. |

| Description | | Exigence |
|---|---|---|
| **4.3.2.5.7** | **Soumettre à essai et mettre à jour le plan de continuité d'activité** | Le plan de continuité d'activité doit être soumis à essai régulièrement et mis à jour si nécessaire. |

### 4.3.2.6 Élément: Politiques et procédures de sécurité

**Objectif:**

Aborder la façon dont une organisation définit la sécurité, exécute son programme de sécurité, définit et prend en charge la tolérance des risques, et révise son programme pour lui apporter des améliorations.

**Description:**

Il convient de développer les politiques de cyber-sécurité destinées à l'environnement IACS d'après les politiques de haut niveau existantes, les risques caractérisés et les niveaux de tolérance des risques identifiés par la direction. Les procédures de cyber-sécurité sont développées à partir des politiques de cyber-sécurité et identifient la façon dont les politiques doivent être mises en œuvre.

**Justification:**

Ces politiques et procédures écrites permettent aux employés, intérimaires, sous-traitants ou autres de bien comprendre le point de vue de l'entreprise sur la cyber-sécurité et leurs propres rôles et leurs responsabilités afin d'assurer la sécurité des actifs de l'entreprise.

**Exigences:**

**Tableau 7 – Politiques et procédures de sécurité: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.2.6.1** | **Développer les politiques de sécurité** | L'organisation doit développer des politiques de cyber-sécurité de haut niveau pour l'environnement IACS, qui soient approuvées par la direction. |
| **4.3.2.6.2** | **Développer des procédures de sécurité** | L'organisation doit développer et approuver des procédures de cyber-sécurité reposant sur les politiques de cyber-sécurité et fournir des indications sur les actions à effectuer pour satisfaire aux politiques. |
| **4.3.2.6.3** | **Maintenir une uniformité entre les systèmes de gestion des risques** | Il convient que les politiques et procédures de cyber-sécurité destinées aux risques IACS soient conformes aux politiques établies par d'autres systèmes de gestion des risques, ou constituent des extensions de ces politiques. |
| **4.3.2.6.4** | **Définir les exigences d'adhésion aux politiques et procédures de cyber-sécurité** | Les politiques et procédures de cyber-sécurité, pour l'environnement IACS, doivent comprendre des exigences d'adhésion. |
| **4.3.2.6.5** | **Déterminer la tolérance des risques de l'organisation** | L'organisation doit déterminer et documenter sa tolérance des risques pour permettre la création de politiques et d'activités de gestion des risques. |
| **4.3.2.6.6** | **Communiquer les politiques et les procédures à l'organisation** | Les politiques et les procédures de cyber-sécurité, pour l'environnement IACS, doivent être communiquées à l'ensemble du personnel concerné. |

| Description | | Exigence |
|---|---|---|
| **4.3.2.6.7** | **Réviser et mettre à jour les politiques et procédures de cyber-sécurité** | Les politiques et procédures de cyber-sécurité doivent être révisées régulièrement, validées pour permettre de confirmer qu'elles sont à jour, puis suivies et mises à jour pour permettre de vérifier qu'elles restent appropriées. |
| **4.3.2.6.8** | **Démontrer l'implication de la direction supérieure dans la cyber-sécurité** | La direction supérieure doit démontrer son implication pour la cyber-sécurité en soutenant les politiques de cyber-sécurité. |

### 4.3.3 Groupe d'éléments: Contre-mesures de sécurité sélectionnées

#### 4.3.3.1 Description du groupe d'éléments

Le deuxième groupe d'éléments de cette catégorie est Contre-mesures de sécurité sélectionnées. Les éléments de ce groupe traitent de certains des principaux types de contrôles de sécurité inclus dans un CSMS bien conçu. Le présent document ne cherche pas à décrire la mise en œuvre complète d'une des contre-mesures de sécurité sélectionnées. Il décrit de nombreux problèmes de politique, de procédure et de pratique liés à ces contre-mesures de sécurité particulières. La Figure 4 donne une représentation graphique des six éléments de ce groupe d'éléments:

- Sécurité du personnel,
- Sécurité physique et environnementale,
- Segmentation des réseaux,
- Contrôle d'accès – Administration des comptes,
- Contrôle d'accès – Authentification et
- Contrôle d'accès – Autorisation.

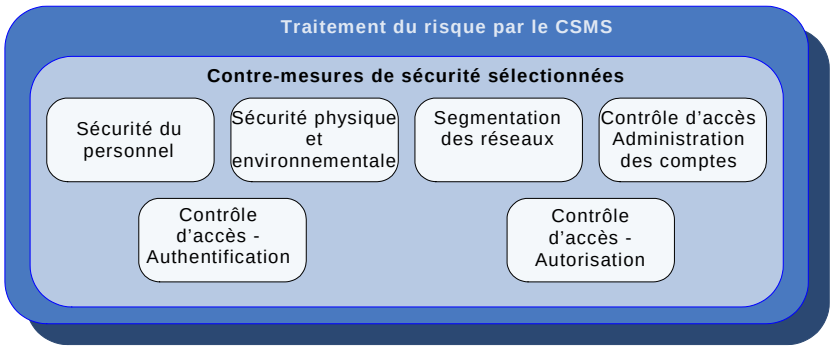



**Figure 4 – Représentation graphique du groupe d'éléments: Contre-mesures de sécurité sélectionnées**

L'inclusion de ces contre-mesures particulières a été décidée en raison de leur impact fort sur la politique et l'architecture, rendant leur examen essentiel lors de la construction de n'importe quel CSMS. Cette norme n'a pas pour objet de spécifier une liste complète et suffisante de contre-mesures, car seul le processus d'évaluation et de gestion des risques décrit dans la norme permet de déterminer si une telle liste est complète ou non.

#### 4.3.3.2 Élément: Sécurité du personnel

**Objectif:**

Établir les politiques et les procédures permettant de déterminer si les employés sont capables de maintenir la sécurité des IACS de l'organisation pendant toute la durée de leur présence dans l'entreprise.

**Description:**

La sécurité du personnel consiste à observer les nouveaux venus et le personnel déjà en place pour déterminer s'ils sont capables d'assurer pour l'organisation la sécurité des IACS. Un nouveau venu sera évalué avant son entrée dans l'organisation pour s'assurer que son comportement est compatible avec ses responsabilités futures dans le domaine de la sécurité. On s'assurera que le personnel existant continue de présenter un comportement compatible avec ses responsabilités actuelles dans le domaine de la sécurité.

**Justification:**

Dans de nombreuses organisations, les exigences de sécurité du personnel reposent sur des préoccupations relatives aux menaces internes ou aux risques d'accidents dus à la négligence de détails ou causés par du personnel qui ne devrait pas effectuer ces tâches parce qu'il n'a pas la formation appropriée ou utilise des substances susceptibles d'altérer son jugement. Mettre en œuvre des politiques de sécurité du personnel peut permettre de réduire ce genre de problème.

**Exigences:**

**Tableau 8 – Sécurité du personnel: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.2.1** | **Établir une politique de sécurité du personnel** | Une politique de sécurité du personnel doit être établie, qui indique clairement l'implication de l'organisation dans la sécurité et les responsabilités du personnel en matière de sécurité. (Par personnel, on entend les employés, les candidats à l'embauche, les intérimaires et les sous-traitants.) |
| **4.3.3.2.2** | **Présélectionner le personnel au départ** | À moins que la loi ne l'interdise, l'ensemble du personnel ayant accès aux IACS (accès physique et cyber-accès), y compris les nouveaux embauchés et les personnes transférées vers des fonctions sensibles, doit faire l'objet d'une présélection comprenant la validation de leur identité et un examen de leur expérience antérieure, au cours du processus d'embauche. |
| **4.3.3.2.3** | **Présélectionner le personnel continuellement** | Il convient de rester vigilant en permanence à tout signe de changement, au sein du personnel, pouvant indiquer un conflit d'intérêt ou toute préoccupation concernant le fait d'accomplir le travail de manière appropriée. |
| **4.3.3.2.4** | **Aborder les responsabilités concernant la sécurité** | Il convient que la politique de sécurité du personnel définisse les responsabilités concernant la sécurité, depuis l'embauche de la personne jusqu'à son départ, en particulier pour les fonctions sensibles. |
| **4.3.3.2.5** | **Documenter et communiquer les attentes et responsabilités en matière de sécurité** | Les attentes et responsabilités en matière de sécurité doivent être documentées clairement et communiquées régulièrement au personnel. |
| **4.3.3.2.6** | **Énoncer clairement les termes et conditions d'embauche concernant la cyber-sécurité** | Les termes et conditions d'embauche doivent indiquer clairement la responsabilité du personnel vis à vis de la cyber-sécurité. Ces responsabilités doivent se prolonger pendant une période de temps raisonnable après que la personne ait quitté l'entreprise. |
| **4.3.3.2.7** | **Séparer les tâches pour maintenir un équilibre approprié des pouvoirs** | Il convient de séparer les tâches au sein du personnel pour maintenir un équilibre des pouvoirs approprié, afin qu'aucun individu n'ait, à lui seul, le contrôle total sur les actions permettant de modifier l'utilisation opérationnelle des IACS. |

### 4.3.3.3 Élément: Sécurité physique et environnementale

**Objectif:**

Créer un environnement sûr pour la protection des actifs IACS. Un actif est un objet physique ou logique possédé par une organisation ou sous la garde de celle-ci, ayant une valeur perçue ou réelle pour cette organisation (voir CEI/TS 62443-1-1). Les actifs IACS sont les actifs faisant partie de l'IACS, qu'ils soient de type physique ou virtuel, ou ceux pouvant affecter le fonctionnement de l'IACS. Les mesures de sécurité physique garantissent que tous les actifs, en particulier ceux liés aux IACS d'une organisation, sont protégés physiquement contre tout accès non autorisé, perte, dommage, mauvaise utilisation ou autre. Les mesures de sécurité environnementale garantissent que les actifs d'une organisation sont protégés contre toute condition ambiante qui les rendrait inutilisables ou endommagerait les informations qu'ils contiennent.

**Description:**

Il convient de concevoir des mesures de sécurité physique et environnementale en complément des mesures de cyber-sécurité prises pour protéger les actifs faisant partie de l'IACS et coordonnées avec la sécurité physique du reste de l'usine. Quand on développe un programme visant à assurer la sécurité physique des actifs, il est important d'inclure la totalité

des systèmes dans le domaine d'application et de ne pas limiter l'effort aux installations de la traditionnelle salle informatique. Il convient de faire preuve de bon sens technique pour équilibrer les risques au moment de déterminer les procédures de sécurité physique. La segmentation physique est une contre-mesure de sécurité clé conçue pour répartir les dispositifs en différentes zones de sécurité, dans lesquelles on utilise des pratiques de sécurité identifiées pour obtenir le niveau de sécurité cible souhaité.

**Justification:**

Les actifs physiques constituent autant un moyen pour aboutir à une fin que la fin elle-même. Dans les systèmes de commande modernes, les actifs physiques fournissent le moyen avec lequel le cyber-système fonctionne. Par conséquent, l'actif a de la valeur en lui-même, mais il a également de la valeur en tant que partie intégrante du système de commande. Étant donné que l'actif a besoin du système de commande, et réciproquement, tous deux doivent être protégés si l'on souhaite que l'ensemble du système soit protégé. Il convient que le principe de sécurité qui l'emporte sur tous les autres soit que l'utilisation de contre-mesures de sécurité doit être proportionnelle au niveau de risque. La segmentation physique est une contre-mesure de sécurité importante, utilisée en même temps que d'autres niveaux de défense pour réduire les risques auxquels l'IACS peut être exposé, mais elle peut ne pas être nécessaire si les risques de sécurité se trouvent dans des limites acceptées.

**Exigences:**

**Tableau 9 – Sécurité physique et environnementale: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.3.1** | **Établir des politiques de sécurité physique et de cyber-sécurité complémentaires** | On doit établir des politiques et procédures de sécurité qui traitent à la fois de la sécurité physique et de la cyber-sécurité destinées à protéger les actifs. |
| **4.3.3.3.2** | **Établir le ou les périmètres de sécurité physique** | On doit établir un ou plusieurs périmètres de sécurité physique pour fournir des barrières contre tout accès non autorisé aux actifs protégés. |
| **4.3.3.3.3** | **Mettre en place des contrôles d'entrée** | On doit mettre en place des contrôles d'entrée appropriés au niveau de chaque barrière ou limite. |
| **4.3.3.3.4** | **Protéger les actifs contre les dommages environnementaux** | On doit protéger les actifs contre les dommages environnementaux causés par des menaces telles que le feu, l'eau, la fumée, la poussière, les radiations, la corrosion et les impacts. |
| **4.3.3.3.5** | **Exiger des employés qu'ils suivent les procédures de sécurité** | On doit exiger des employés qu'ils suivent et fassent respecter les procédures de sécurité physique qui ont été établies. |
| **4.3.3.3.6** | **Protéger les connexions** | On doit protéger de façon adéquate toutes les connexions qui sont sous le contrôle de l'organisation contre les intrusions et les dommages. |
| **4.3.3.3.7** | **Entretenir les équipements** | On doit entretenir correctement les équipements, y compris les équipements environnementaux auxiliaires, pour en garantir le bon fonctionnement. |
| **4.3.3.3.8** | **Établir des procédures pour la surveillance et l'émission d'alarmes** | On doit établir des procédures pour la surveillance et l'émission d'alarmes lorsque la sécurité physique ou environnementale est compromise. |
| **4.3.3.3.9** | **Établir des procédures pour l'ajout, l'enlèvement et l'élimination des actifs** | Il convient d'établir et d'auditer des procédures concernant l'ajout, l'enlèvement et l'élimination des actifs. |

| Description | | Exigence |
|---|---|---|
| **4.3.3.3.10** | **Établir des procédures pour la protection provisoire des actifs critiques** | On doit établir des procédures pour assurer la protection des composants critiques durant l'interruption des opérations, par exemple en cas d'incendie, de pénétration d'eau, de manquements aux règles de sécurité, d'interruptions et de sinistres naturels ou autres. |

### 4.3.3.4 Élément: Segmentation des réseaux

**Objectif:**

Grouper et séparer les dispositifs IACS clés en zones de niveaux de sécurité communs afin de gérer les risques de sécurité et d'obtenir le niveau de sécurité cible souhaité pour chaque zone.

**Description:**

La segmentation des réseaux est une contre-mesure de sécurité clé conçue pour répartir les dispositifs en différentes zones de sécurité, dans lesquelles on utilise des pratiques de sécurité identifiées pour obtenir le niveau de sécurité cible souhaité. La zone peut être un segment de réseau autonome isolé ou un segment de réseau séparé du réseau de l'organisation par une quelconque barrière de réseau. Il convient de concevoir l'IACS de manière à le rendre capable de filtrer les trames de communication non essentielles ou de les empêcher d'atteindre les dispositifs IACS.

Pour les réseaux basés sur le protocole TCP/IP (Transmission Control Protocol / Internet Protocol), les dispositifs barrières les plus courants utilisés sont les pare-feu, les routeurs et les commutateurs de niveau 3. Pour les réseaux qui ne sont pas de type TCP/IP, les dispositifs barrières peuvent être des passerelles autonomes ou des dispositifs intégrés dans le module d'interface réseau d'un dispositif IACS.

**Justification:**

Il convient que le principe de sécurité qui l'emporte sur tous les autres soit que l'utilisation des contre-mesures de sécurité doit être proportionnelle au niveau de risque. La segmentation des réseaux est une contre-mesure de sécurité importante, utilisée en même temps que d'autres niveaux de défense pour réduire les risques auxquels l'IACS peut être exposé, mais elle peut ne pas être nécessaire si les risques de sécurité sont faibles.

**Exigences:**

**Tableau 10 – Segmentation des réseaux: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.4.1** | **Développer l'architecture de segmentation des réseaux** | Une stratégie de contre-mesure de segmentation de réseaux employant des zones de sécurité doit être développée pour les dispositifs IACS en fonction du niveau de risque de l'IACS. |
| **4.3.3.4.2** | **Employer l'isolation ou la segmentation sur les IACS à risque élevé** | Les IACS à risque élevé doivent être isolés des zones ayant des risques ou des niveaux de sécurité différents, ou employer un dispositif barrière qui les isole de ces zones. |
| **4.3.3.4.3** | **Bloquer les communications non essentielles au moyen de dispositifs barrières** | Des dispositifs barrières doivent bloquer toutes les communications non essentielles entrant et sortant de la zone de sécurité contenant des équipements de commande critiques. |

#### 4.3.3.5 Élément: Contrôle d'accès – Administration des comptes

**Objectif:**

S'assurer en permanence que seules les entités appropriées disposent de comptes autorisant les accès et que ces comptes fournissent les droits d'accès appropriés.

**Description:**

Le contrôle d'accès est la méthode permettant de contrôler qui ou quelles entités peuvent accéder aux locaux et aux systèmes et quel type d'accès est autorisé. Le contrôle d'accès comporte trois aspects clés: l'administration des comptes, l'authentification et l'autorisation. Ces trois aspects doivent fonctionner de concert pour l'établissement d'une stratégie de contrôle d'accès solide et sûre.

L'administration des comptes est la méthode consistant à attribuer et retirer des comptes d'accès et à maintenir les permissions et les droits correspondant à ces comptes pour permettre l'accès à des ressources et des fonctions spécifiques des locaux physiques, du réseau ou du système. Il convient que les comptes d'accès soient basés sur la fonction ou sur le rôle, et puissent être définis pour les individus, les groupes d'individus travaillant en équipe ou les dispositifs assurant une fonction.

**Justification:**

Une mauvaise utilisation des données et des systèmes peut avoir des conséquences graves, telles que mettre en danger la vie humaine, polluer l'environnement, occasionner des pertes financières ou dégrader l'image de l'entreprise. Ces risques augmentent si les employés, les sous-traitants et le personnel intérimaire ont des droits d'accès indus aux données et aux systèmes.

**Exigences:**

**Tableau 11 – Contrôle d'accès – Administration des comptes: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.5.1** | **Les comptes d'accès mettent en œuvre la politique de sécurité basée sur les autorisations** | Les droits d'accès mis en œuvre pour les comptes d'accès doivent être établis conformément à la politique de sécurité sur les autorisations de l'organisation (voir 4.3.3.7.1). |
| **4.3.3.5.2** | **Identifier les individus** | En ce qui concerne les contrôles de cyber-sécurité, on doit déterminer s'il faut choisir des comptes d'accès pour les individus plutôt que pour les équipes en considérant les menaces, les risques et les vulnérabilités. Dans ce cas, les considérations engloberont les risques HSE des contrôles individuels, la réduction au moyen de contrôles de sécurité physiques complémentaires, l'exigence de définir des responsabilités et les besoins administratifs/opérationnels. |
| **4.3.3.5.3** | **Autoriser l'accès par compte** | L'accès doit être accordé, modifié ou résilié sous l'autorité d'un directeur compétent. |
| **4.3.3.5.4** | **Enregistrer les comptes d'accès** | Un dossier doit être géré, qui contient tous les comptes d'accès et le détail des individus et des dispositifs autorisés à utiliser le compte, leurs permissions et le responsable ayant accordé les autorisations. |
| **4.3.3.5.5** | **Suspendre ou supprimer les comptes non nécessaires** | Les comptes d'accès doivent être suspendus ou supprimés dès qu'ils ne sont plus nécessaires (par exemple, en cas de changement de fonction). |
| **4.3.3.5.6** | **Réviser les permissions des comptes** | Tous les comptes d'accès établis doivent être revus régulièrement pour faire en sorte que le ou les individus et les dispositifs n'aient que les permissions minimums nécessaires. |

| Description | | Exigence |
|---|---|---|
| **4.3.3.5.7** | **Changer les mots de passe par défaut** | Les mots de passe par défaut des comptes d'accès doivent être modifiés avant la mise en service de l'IACS. |
| **4.3.3.5.8** | **Auditer l'administration des comptes** | Il convient d'examiner périodiquement l'adhésion à la politique d'administration des comptes. |

### 4.3.3.6 Élément: Contrôle d'accès – Authentification

**Objectif:**

Identifier positivement les utilisateurs des réseaux, les hôtes, les applications, les services et les ressources en ce qui concerne les transactions informatisées, afin qu'ils puissent se voir accorder les droits et les responsabilités correspondant aux comptes que leur a accordés l'administration des comptes.

**Description:**

Le contrôle d'accès est la méthode permettant de contrôler qui ou quelles ressources peuvent accéder aux locaux et aux systèmes et quel type d'accès est accordé. Le contrôle d'accès comporte trois aspects clés: l'administration des comptes, l'authentification et l'autorisation. Ces trois aspects doivent fonctionner de concert pour l'établissement d'une stratégie de contrôle d'accès solide et sûre.

Il existe plusieurs types de stratégies d'authentification, chacune présentant différents degrés de force. Les méthodes d'authentification fortes sont des méthodes qui identifient l'utilisateur de façon précise et sûre. Les méthodes d'authentification faibles sont des méthodes pouvant être facilement contournées, laissant l'accès à l'information à qui ne devrait pas en disposer. L'emplacement physique de l'utilisateur peut avoir un impact significatif sur le risque d'accès à l'IACS.

**Justification:**

Les exigences d'authentification sont plus rigoureuses pour les utilisateurs chargés de l'administration ou de la configuration et les utilisateurs distants que pour les autres utilisateurs. En effet, les utilisateurs chargés de l'administration ou de la configuration ont des droits plus importants et leurs actions ont potentiellement plus d'impact que celles des autres utilisateurs, et les utilisateurs distants ne sont généralement pas soumis à des contrôles d'accès physique complémentaires. Le blocage automatique de compte en cas d'erreur de saisie à la connexion ou de période d'inactivité prolongée augmente la force de l'authentification, mais doit être considéré attentivement dans l'environnement IACS, car le fait qu'un utilisateur autorisé ne puisse s'authentifier pourrait avoir des implications HSE si celui-ci n'était pas en mesure d'effectuer certaines tâches dans une situation critique. Dans l'environnement IACS, on met fortement l'accent sur le fait de combiner les mesures d'authentification physiques à des pratiques d'authentification électroniques.

**Exigences:**

**Tableau 12 – Contrôle d'accès – Authentification: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.6.1** | **Développer une stratégie d'authentification** | Les entreprises doivent avoir une stratégie d'authentification ou une approche pour définir la ou les méthodes d'authentification à utiliser. |
| **4.3.3.6.2** | **Authentifier tous les utilisateurs avant l'utilisation du système** | Tous les utilisateurs doivent être authentifiés avant de pouvoir utiliser l'application demandée, sauf s'il existe des combinaisons compensatoires de technologies de contrôle d'entrée et de pratiques administratives. |
| **4.3.3.6.3** | **Exiger des méthodes d'authentification fortes pour l'administration du système et la configuration d'application** | On doit utiliser des pratiques d'authentification fortes (comme exiger des mots de passe élaborés) sur tous les comptes d'accès d'administrateur système et les comptes d'accès à la configuration d'application. |
| **4.3.3.6.4** | **Consigner et examiner toutes les tentatives d'accès aux systèmes critiques** | Il convient d'utiliser des fichiers de consignation pour enregistrer toutes les tentatives d'accès aux systèmes critiques, et d'examiner aussi bien les tentatives réussies que les échecs. |
| **4.3.3.6.5** | **Authentifier au niveau approprié tous les utilisateurs distants** | L'organisation doit employer un mode d'authentification ayant un niveau de force approprié pour identifier efficacement un utilisateur interactif distant. |
| **4.3.3.6.6** | **Développer une politique pour les ouvertures de session et les connexions distantes** | L'organisation doit développer une politique concernant les ouvertures de session distantes par un utilisateur et/ou les connexions distantes (par exemple, les connexions de tâche à tâche) au système de commande, qui définisse les réponses appropriées de la part du système en cas d'échec des tentatives de connexion ou de périodes d'inactivité. |
| **4.3.3.6.7** | **Désactiver le compte d'accès après un certain nombre de tentatives de connexion distantes infructueuses** | Après un certain nombre de tentatives de connexion infructueuses de la part d'un utilisateur distant, il convient que le système désactive le compte d'accès pendant un certain temps. |
| **4.3.3.6.8** | **Exiger une nouvelle authentification après une certaine inactivité de l'utilisateur distant sur le système** | Après une période d'inactivité définie, il convient d'exiger de l'utilisateur distant qu'il s'authentifie à nouveau avant qu'il ne puisse accéder à nouveau au système. |
| **4.3.3.6.9** | **Employer l'authentification pour la communication de tâche à tâche** | Il convient que les systèmes emploient des modes d'authentification appropriés pour la communication de tâche à tâche entre les applications et les dispositifs. |

### 4.3.3.7 Élément: Contrôle d'accès – Autorisation

**Objectif:**

Accorder les droits d'accès aux ressources en cas d'authentification réussie de l'utilisateur et d'identification de son compte d'accès associé. Les droits accordés sont déterminés par la configuration des comptes effectuée lors de l'étape d'administration des comptes du processus d'activité.

**Description:**

Le contrôle d'accès est la méthode permettant de contrôler qui ou quelles ressources peuvent accéder aux locaux et aux systèmes et quel type d'accès est autorisé. Le contrôle d'accès comporte trois aspects clés: l'administration des comptes, l'authentification et l'autorisation.

Ces trois aspects doivent fonctionner de concert pour l'établissement d'une stratégie de contrôle d'accès solide et sûre.

L'autorisation explore les contrôles destinés à protéger les informations et les actifs de toute destruction, modification ou divulgation délibérée ou accidentelle. Elle se concentre spécifiquement sur les mesures conçues pour faire en sorte que les agents authentifiés aient accès aux actifs de type information requis. Comme pour l'authentification, l'autorisation dépend de l'emplacement de l'utilisateur.

**Justification:**

Il est important de faire en sorte que, dans l'environnement IACS, les bonnes personnes puissent accéder aux bonnes informations et aux systèmes, et qu'elles ne soient pas dans l'impossibilité d'accomplir leurs tâches en ne disposant pas des autorisations nécessaires. L'autorisation d'effectuer les fonctions d'une tâche spécifique est fournie par l'application. Il est nécessaire de prendre en compte les implications en matière de sécurité quand on développe la stratégie d'autorisation.

**Exigences:**

**Tableau 13 – Contrôle d'accès – Autorisation: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.3.7.1** | **Définir une politique de sécurité pour les autorisations** | Les règles qui définissent les droits accordés au personnel par les comptes d'accès pour les différentes tâches doivent être définis dans une politique de sécurité sur les autorisations qui sera clairement documentée et appliquée à tout le personnel lors de l'authentification. |
| **4.3.3.7.2** | **Établir des méthodes d'autorisation physiques et logiques appropriées pour l'accès aux dispositifs IACS** | Les permissions pour 'accéder aux dispositifs IACS doivent être logiques (règles accordant ou refusant l'accès à des utilisateurs connus en fonction de leur rôle), physiques (verrous, caméras et autres dispositifs de contrôle qui limitent l'accès à une console informatique active), ou les deux. |
| **4.3.3.7.3** | **Contrôler l'accès à l'information ou aux systèmes au moyen de comptes d'accès basés sur les rôles** | Il convient que les comptes d'accès soient basés sur les rôles, ce qui permet de donner l'accès à des informations ou systèmes appropriés au rôle de cet utilisateur. Les implications concernant la sécurité doivent être prises en compte lors de la définition des rôles. |
| **4.3.3.7.4** | **Employer des méthodes d'autorisation multiple pour les IACS critiques** | Dans les environnements de commande critiques, il convient d'employer des méthodes d'autorisation multiple pour limiter l'accès aux IACS. |

### 4.3.4 Groupe d'éléments: Mise en œuvre

#### 4.3.4.1 Description du groupe d'éléments

Le troisième groupe d'éléments de cette catégorie est Mise en œuvre. Les éléments de ce groupe concernent les problèmes liés à la mise en œuvre du CSMS. La Figure 5 est une représentation graphique des quatre éléments de ce groupe d'éléments:

- Gestion des risques et mise en œuvre,
- Développement et maintenance des systèmes,
- Gestion de l'information et des documents, et
- Planification et réponse aux incidents.

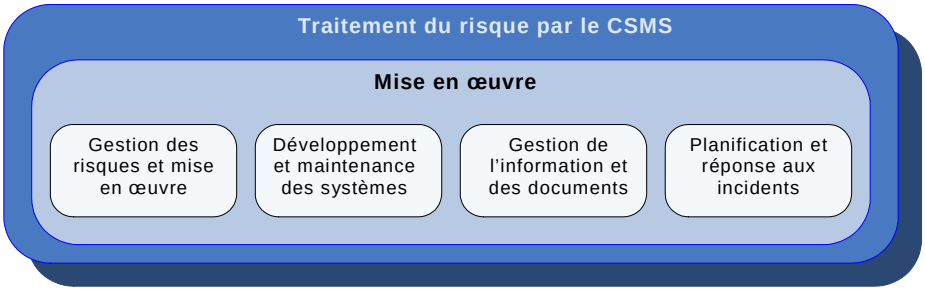



**Figure 5 – Représentation graphique du groupe d'éléments: Mise en œuvre**

#### 4.3.4.2 Élément: Gestion des risques et mise en œuvre

**Objectif:**

Réduire les risques et les maintenir à un niveau acceptable dans l'IACS conforme à la tolérance des risques de l'organisation.

**Description:**

La gestion des risques et la mise en œuvre concernent la sélection, le développement et la mise en œuvre de contre-mesures proportionnelles aux risques. Les contre-mesures peuvent prendre en compte l'utilisation de produits à fortes capacités de sécurité inhérentes, de contrôles de sécurité manuels et procéduraux, et de contrôles technologiques destinés à prévenir ou réduire les incidents liés à la sécurité.

**Justification:**

L'élément Gestion des risques et mise en œuvre sert à transformer les résultats issus de l'élément Identification, classification et évaluation des risques de la présente norme en actions efficaces et concrètes. Le risque, bien qu'il ne puisse être totalement éliminé, peut être géré de telle manière qu'il y ait un équilibre entre le coût de la prévention du risque et le coût potentiel de l'incident.

**Exigences:**

**Tableau 14 – Gestion des risques et mise en œuvre: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.4.2.1** | **Gérer les risques IACS d'une manière continuelle** | L'organisation doit adopter un cadre de gestion des risques qui englobe la sélection et la mise en œuvre des dispositifs IACS et des contre-mesures pour gérer les risques à un niveau acceptable pendant toute la durée de vie de l'installation. |
| **4.3.4.2.2** | **Employer un ensemble commun de contre-mesures** | Partout où un risque spécifique a été identifié, il convient de définir et de mettre en application dans l'organisation un ensemble commun de contre-mesures (techniques et administratives) défini pour traiter les risques de sécurité physique et de cyber-sécurité. |

#### 4.3.4.3 Élément: Développement et maintenance des systèmes

**Objectif:**

S'assurer que le niveau de tolérance des risques souhaité par l'organisation soit maintenu malgré l'évolution des actifs IACS de l'organisation du fait de la maintenance des systèmes existants et du développement et de l'acquisition de nouveaux systèmes.

**Description:**

Le présent élément concerne la conception de la cyber-sécurité dans les systèmes, dès leurs premières phases de développement. Il concerne également la maintenance des politiques et des procédures de sécurité lorsque le système évolue au cours de son cycle de vie.

**Justification:**

Les organisations ont constaté que la maintenance du CSMS pose davantage de problèmes que son élaboration. C'est pour cette raison qu'il est essentiel de disposer de procédures permettant de traiter la cyber-sécurité de manière proactive faisant partie de l'évolution naturelle des systèmes IACS.

**Exigences:**

**Tableau 15 – Développement et maintenance des systèmes: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.4.3.1** | **Définir et soumettre à essai les fonctions et capacités de sécurité** | Les fonctions et capacités de sécurité de chaque nouveau composant de l'IACS doivent être définies clairement, qu'il soit développé ou acheté, et il doit être testé en même temps que les autres composants, afin que l'ensemble du système ait le profil de sécurité souhaité. |
| **4.3.4.3.2** | **Développer et mettre en œuvre un système de gestion des modifications** | Un système de gestion des modifications doit être développé et mis en œuvre pour l'environnement IACS. Le processus de gestion des modifications doit suivre le principe de séparation des tâches pour éviter les conflits d'intérêt. |
| **4.3.4.3.3** | **Évaluer tous les risques liés à la modification de l'IACS** | Au moyen de critères clairement définis, les modifications que l'on se propose d'apporter aux IACS doivent faire l'objet d'un examen permettant de déterminer leur impact potentiel sur les risques HSE et les risques de cyber-sécurité. Cet examen sera effectué par des personnes ayant les connaissances techniques requises des opérations industrielles et du système IACS. |
| **4.3.4.3.4** | **Exiger des politiques de sécurité pour le développement de systèmes ou les modifications de maintenance** | Les exigences de sécurité d'un nouveau système installé dans l'environnement IACS d'une zone existante doivent satisfaire aux politiques et procédures de sécurité exigées pour cette zone ou cet environnement. De manière similaire, les mises à niveau ou modifications de maintenance doivent satisfaire aux exigences de sécurité de la zone. |
| **4.3.4.3.5** | **Intégrer les procédures de gestion des modifications concernant la cyber-sécurité et celles concernant la gestion de la sécurité des procédés (PSM)** | Il convient que les procédures de gestion des modifications concernant la cyber-sécurité soient intégrées aux procédures PSM existantes. |
| **4.3.4.3.6** | **Réviser et maintenir les politiques et procédures** | Les opérations, les politiques et les procédures de gestion des modifications doivent être révisées et à jour afin que les modifications apportées à la sécurité ne dégradent pas la sécurité et n'augmentent pas les risques d'interruption d'activité. |

| Description | | Exigence |
|---|---|---|
| **4.3.4.3.7** | **Établir et documenter une procédure de gestion des correctifs** | Une procédure de gestion des correctifs doit être établie, documentée et suivie. |
| **4.3.4.3.8** | **Établir et documenter une procédure de gestion des antivirus/malware** | Une procédure de gestion des antivirus/malware doit être établie, documentée et suivie. |
| **4.3.4.3.9** | **Établir une procédure de sauvegarde et de restauration** | Une procédure destinée à la sauvegarde et la restauration des systèmes informatiques, ainsi qu'à la protection des copies de sauvegarde, doit être établie, utilisée et vérifiée au moyen d'essais appropriés. |

### 4.3.4.4 Élément: Gestion de l'information et des documents

**Objectif:**

Classifier, gérer, sauvegarder et présenter les informations associées à l'IACS et au CSMS au personnel autorisé au moment approprié.

**Description:**

Il convient que les organisations emploient des informations et des documents compréhensibles pour les politiques de gestion qu'elles appliquent à leurs actifs de type information, dans le domaine d'application de leur IACS et leur CSMS. Il convient de protéger soigneusement ces informations et de s'assurer que les versions appropriées sont bien conservées. Les systèmes de classification d'information qui permettent aux actifs de type information de recevoir le niveau de protection approprié sont essentiels pour atteindre cet objectif.

**Justification:**

Nombre d'informations au sujet de l'IACS peuvent être stockées électroniquement ou sous forme de copie papier à l'extérieur de l'IACS et ne sont pas protégées par les contrôles d'autorisation IACS. Tout accès non autorisé à ces informations ou toute utilisation non autorisée de celles-ci constitue une menace pour la sécurité des IACS. Ces informations doivent être contrôlées et gérées de manière appropriée.

**Exigences:**

**Tableau 16 – Gestion de l'information et des documents: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.4.4.1** | **Développer les procédés de gestion du cycle de vie des informations IACS** | Un procédé de gestion de document, applicable au cycle de vie, doit être développé et maintenu pour les informations IACS. |
| **4.3.4.4.2** | **Définir les niveaux de classification des informations** | Des niveaux de classification des informations (par exemple: confidentiel, restreint et public) doivent être définis pour l'accès à ces informations et le contrôle de celles-ci, notamment le partage, la copie, l'émission et la distribution, qui doivent correspondre au niveau de protection requis. |
| **4.3.4.4.3** | **Classifier tous les actifs de type information du CSMS** | Tous les actifs logiques appartenant au domaine d'application du CSMS (c'est-à-dire les informations sur la conception du système de commande, les évaluations de vulnérabilité, les schémas de réseau et les programmes relatifs aux opérations industrielles) doivent être classifiés pour indiquer la protection requise, proportionnelle aux conséquences de leur divulgation ou modification non autorisée. |

| Description | | Exigence |
|---|---|---|
| **4.3.4.4.4** | **Assurer un contrôle approprié des dossiers** | Il convient de développer des politiques et procédures détaillant la conservation, la protection physique et l'intégrité, la destruction et l'élimination de tous les actifs en fonction de leur classification, ce qui inclut les dossiers imprimés et électroniques, les équipements et autres supports contenant des informations, en tenant compte des exigences légales ou réglementaires. |
| **4.3.4.4.5** | **Assurer la récupération des dossiers à long terme** | Il convient d'employer des mesures appropriées afin que les dossiers à long-terme puissent être récupérés (c'est-à-dire convertir les données en un format plus récent ou conserver les anciens équipements pouvant lire les données). |
| **4.3.4.4.6** | **Maintenir les classifications des informations** | Il convient de réviser périodiquement les informations nécessitant un contrôle particulier ou des manipulations particulières pour vérifier que ces manipulations particulières sont toujours exigées. |
| **4.3.4.4.7** | **Auditer le processus de gestion de l'information et des documents** | Il convient de vérifier périodiquement l'adhésion à la politique de gestion de l'information et des documents. |

### 4.3.4.5 Élément: Planification et réponse aux incidents

**Objectif:**

Prédéfinir la façon dont l'organisation détecte les incidents de cyber-sécurité et y réagit.

**Description:**

Quand on développe un programme de planification et de réponse aux incidents, il est important d'inclure la totalité des systèmes dans le domaine d'application et de ne pas limiter l'effort aux installations de la traditionnelle salle informatique. Il convient qu'une partie du plan de réponse aux incidents comporte des procédures définissant la façon dont l'organisation doit répondre aux incidents, ce qui comprend des méthodes de notification et de documentation, des investigations, des remises en état et les pratiques de suivi qui les accompagnent.

**Justification:**

Identifier un incident suffisamment tôt et y réagir de façon appropriée peut permettre de limiter les conséquences de l'événement. La planification et la réponse aux incidents donnent à l'organisation la possibilité de planifier en prévision les incidents de sécurité et d'y réagir selon les pratiques établies dans l'entreprise. Quelle que soit la vigilance dont on fait preuve pour protéger un système, il est toujours possible que des intrusions indésirables le compromettent. La technologie est toujours vulnérable, et les menaces externes sont de plus en plus nombreuses et sophistiquées; il est donc nécessaire de faire appel à une stratégie robuste pour déterminer le mode de planification et de réponse approprié. On capture les connaissances que l'on retire des incidents réels, car elles sont extrêmement importantes pour permettre d'évaluer et d'améliorer le CSMS.

**Exigences:**

**Tableau 17 – Planification et réponse aux incidents: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.3.4.5.1** | **Mettre en œuvre un plan de réponse aux incidents** | L'organisation doit mettre en œuvre un plan de réponse aux incidents permettant d'identifier le personnel responsable et de définir les actions que doivent entreprendre les personnes désignées. |

| Description | | Exigence |
|---|---|---|
| **4.3.4.5.2** | **Communiquer le plan de réponse aux incidents** | Le plan de réponse aux incidents doit être communiqué à toutes les organisations appropriées. |
| **4.3.4.5.3** | **Établir une procédure de signalement des activités et événements inhabituels** | Il convient que l'organisation établisse une procédure de signalement permettant de signaler les activités et événements inhabituels pouvant constituer des incidents de cyber-sécurité. |
| **4.3.4.5.4** | **Apprendre aux employés à signaler les incidents de cyber-sécurité** | Il convient de sensibiliser les employés au fait qu'ils ont la responsabilité de signaler les incidents de cyber-sécurité, et aux méthodes à utiliser pour signaler ces incidents. |
| **4.3.4.5.5** | **Signaler les incidents de cyber-sécurité sans délai** | Il convient que l'organisation signale les incidents de cyber-sécurité sans délai. |
| **4.3.4.5.6** | **Identifier les incidents et y répondre** | Lorsqu'un incident est identifié, l'organisation doit y répondre rapidement selon les procédures établies. |
| **4.3.4.5.7** | **Identifier les intrusions informatiques réussies ou ayant échoué** | Il convient que l'organisation dispose de procédures permettant d'identifier les intrusions informatiques, qu'elles aient échoué ou réussi. |
| **4.3.4.5.8** | **Documenter le détail des incidents** | Les détails d'un incident identifié doivent être documentés pour enregistrer l'incident ainsi que la réponse, les leçons qui en ont été retirées et les actions entreprises pour modifier le CSMS suite à cet incident. |
| **4.3.4.5.9** | **Communiquer le détail des incidents** | Les détails documentés d'un incident doivent être communiqués à toutes les organisations appropriées (à savoir la direction, le service informatique, la sécurité des procédés, la sécurité technique des automatismes et des commandes et la fabrication) sans délai. |
| **4.3.4.5.10** | **Prendre en compte et corriger les problèmes repérés** | L'organisation doit utiliser une méthodologie économique permettant de prendre en compte les problèmes repérés et de faire en sorte qu'ils soient corrigés. |
| **4.3.4.5.11** | **Effectuer des exercices** | Il convient d'effectuer régulièrement des exercices pour soumettre à essai le programme de réponse aux incidents. |

## 4.4 Catégorie: Surveillance et amélioration du CSMS

### 4.4.1 Description de la catégorie

La troisième catégorie principale du CSMS est intitulée Surveillance et amélioration du CSMS. Elle consiste aussi bien à s'assurer que le CSMS est utilisé qu'à vérifier l'efficacité du CSMS lui-même. La Figure 6 est une représentation graphique des deux éléments de la catégorie:

- Conformité et
- Révision, amélioration et maintenance du CSMS.


**Figure 6 – Représentation graphique de la catégorie: Surveillance et amélioration du CSMS**

### 4.4.2 Élément: Conformité

**Objectif:**

Faire en sorte que le CSMS développé pour une organisation soit suivi.

**Description:**

La conformité à un CSMS signifie que l'organisation adhère aux politiques énoncées, exécute les procédures au moment approprié et produit les rapports appropriés qui permettront d'effectuer des révisions ultérieurement.

**Justification:**

Le CSMS, s'il n'est pas utilisé, n'ajoute aucune valeur à l'organisation, quelle que soit sa qualité, et ne contribue en aucune façon à réduire les risques.

**Exigences:**

**Tableau 18 – Conformité: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.4.2.1** | **Spécifier la méthodologie du procédé d'audit** | Le programme d'audit doit spécifier la méthodologie du procédé d'audit. |
| **4.4.2.2** | **Auditer périodiquement les IACS** | S'assurer que l'IACS se conforme au CSMS. Le CSMS doit comporter des audits périodiques de l'IACS, dont le but est de vérifier que les politiques et procédures de sécurité fonctionnent comme prévu et atteignent les objectifs de sécurité de la zone. |
| **4.4.2.3** | **Établir des critères de conformité** | Il convient que l'organisation définisse des indicateurs de performances et des critères de réussite, qui serviront à surveiller la conformité au CSMS. Il convient que les résultats de chacun des audits périodiques soient exprimés de façon à traduire les performances par rapport à ces critères et présentent les performances de sécurité et les tendances de sécurité. |
| **4.4.2.4** | **Établir une piste d'audit des documents** | Une liste des documents et des rapports nécessaires à l'établissement d'une piste d'audit doit être développée. |
| **4.4.2.5** | **Définir des mesures disciplinaires en cas de non-conformité** | L'organisation doit indiquer ce que la non-conformité au CSMS signifie; les mesures disciplinaires les concernant doivent également être définies. |
| **4.4.2.6** | **Vérifier la compétence des auditeurs** | Il convient de spécifier la compétence exigée pour effectuer les audits des systèmes spécifiques du domaine d'application. Il convient de déterminer le niveau d'indépendance nécessaire, en tant que partie de l'autorité. |

### 4.4.3 Élément: Révision, amélioration et maintenance du CSMS

**Objectif:**

Faire en sorte que le CSMS continue d'atteindre ses objectifs au fil du temps.

**Description:**

Réviser, améliorer et maintenir le CSMS constitue une façon de superviser en permanence le CSMS pour vérifier l'efficacité de son fonctionnement et gérer les modifications qu'il est nécessaire d'apporter au CSMS au fil du temps.

**Justification:**

Il est nécessaire de réviser et surveiller le CSMS pour que celui-ci reste efficace, car il doit être capable de répondre à l'évolution des menaces, des vulnérabilités et des conséquences, qu'elles soient internes ou externes, ainsi qu'à l'évolution de la tolérance des risques, des exigences légales et des approches techniques et non techniques dans le domaine de la diminution des risques.

**Exigences:**

**Tableau 19 – Révision, amélioration et maintenance du CSMS: Exigences**

| Description | | Exigence |
|---|---|---|
| **4.4.3.1** | **Attribuer à une organisation la gestion et la mise en œuvre des modifications du CSMS** | On doit confier à une organisation la tâche consistant à gérer et coordonner la mise au point et la mise en œuvre des modifications du CSMS, et à utiliser une méthode précise pour réaliser et mettre en œuvre les modifications. |
| **4.4.3.2** | **Évaluer périodiquement le CSMS** | L'organisation dirigeante doit évaluer périodiquement l'ensemble du CSMS pour vérifier que les objectifs de sécurité sont respectés. |
| **4.4.3.3** | **Établir des déclencheurs pour évaluer le CSMS** | Il convient que l'organisation établisse une liste de déclencheurs dont les seuils auront été définis, qui pourront déclencher une révision des éléments concernés du CSMS et éventuellement une modification. Ces déclencheurs comprendront au minimum: l'apparition d'incidents graves liés à la sécurité, l'évolution de la législation et de la réglementation, l'évolution des risques et les modifications majeures apportées à l'IACS. Il convient que les seuils soient basés sur la tolérance des risques de l'organisation. |
| **4.4.3.4** | **Identifier et mettre en œuvre des actions correctives et préventives** | L'organisation doit identifier et mettre en œuvre des actions correctives et préventives appropriées qui modifieront le CSMS pour satisfaire aux objectifs de sécurité. |
| **4.4.3.5** | **Réviser la tolérance des risques** | Il convient de réexaminer la façon dont l'organisation tolère les risques chaque fois qu'il y a des changements importants dans l'organisation, la technologie, les objectifs d'activité, l'activité interne et les événements externes, comme en cas de menaces identifiées ou de changements dans le climat social. |
| **4.4.3.6** | **Surveiller et évaluer les stratégies CSMS dans l'industrie** | Il convient que les propriétaires de systèmes de gestion surveillent les meilleures pratiques CSMS de l'industrie pour l'évaluation des risques et l'atténuation des risques, et en apprécient l'applicabilité. |
| **4.4.3.7** | **Surveiller et évaluer la législation en vigueur relative à la cyber-sécurité** | L'organisation doit identifier la législation en vigueur relative à la cyber-sécurité, ainsi que les évolutions dans cette législation. |
| **4.4.3.8** | **Demander aux employés leur avis sur les suggestions liées à la sécurité, et le rapporter** | Il convient de rechercher activement l'avis des employés sur les suggestions liées à la sécurité, et de le rapporter à la direction si nécessaire en cas de défaut ou d'opportunités dans les performances. |

# Annexe A
(informative)

# Instructions pour le développement des éléments d'un CSMS

## A.1 Vue d'ensemble

La présente annexe donne au lecteur les instructions nécessaires au développement d'un CSMS satisfaisant aux exigences spécifiées à l'Article 4. Les instructions présentées ici fournissent le cadre d'un système de gestion global qui permet aux organisations adoptant le CSMS de personnaliser celui-ci en fonction de leurs besoins particuliers. Il convient de les prendre en compte comme point de départ ou base de référence pour le CSMS. Toutes les instructions peuvent ne pas être nécessairement applicables, car elles dépendent de l'application concernée; l'organisation peut avoir besoin d'une sécurité plus importante que ce qui est présenté ici. Ce n'est également pas un processus étape par étape, comme cela a été spécifié en 4.1.

La présente annexe est organisée avec les mêmes catégories, groupes d'éléments et éléments que ceux énumérés à l'Article 4 (voir Figure A.1). Chaque élément de cette annexe est organisé de la façon suivante:

- Description d'élément – description élémentaire de l'élément;
- Information spécifique à l'élément – un ou plusieurs paragraphes donnant des instructions détaillées concernant cet élément. Leur structure et leur contenu sont spécifiques à l'élément;
- Pratiques en support:
  - Pratiques de base – recommandations aux organisations pour les aider à atteindre un niveau élémentaire de cyber-sécurité. Ces pratiques deviennent les blocs de construction pour les exigences relatives à chaque élément.
  - Pratiques additionnelles – pratiques de sécurité innovantes utilisées par certaines organisations pour une cyber-sécurité encore plus performante;
- Ressources utilisées – sources donnant des informations complémentaires, ainsi que les documents référencés (en plus du présent document).

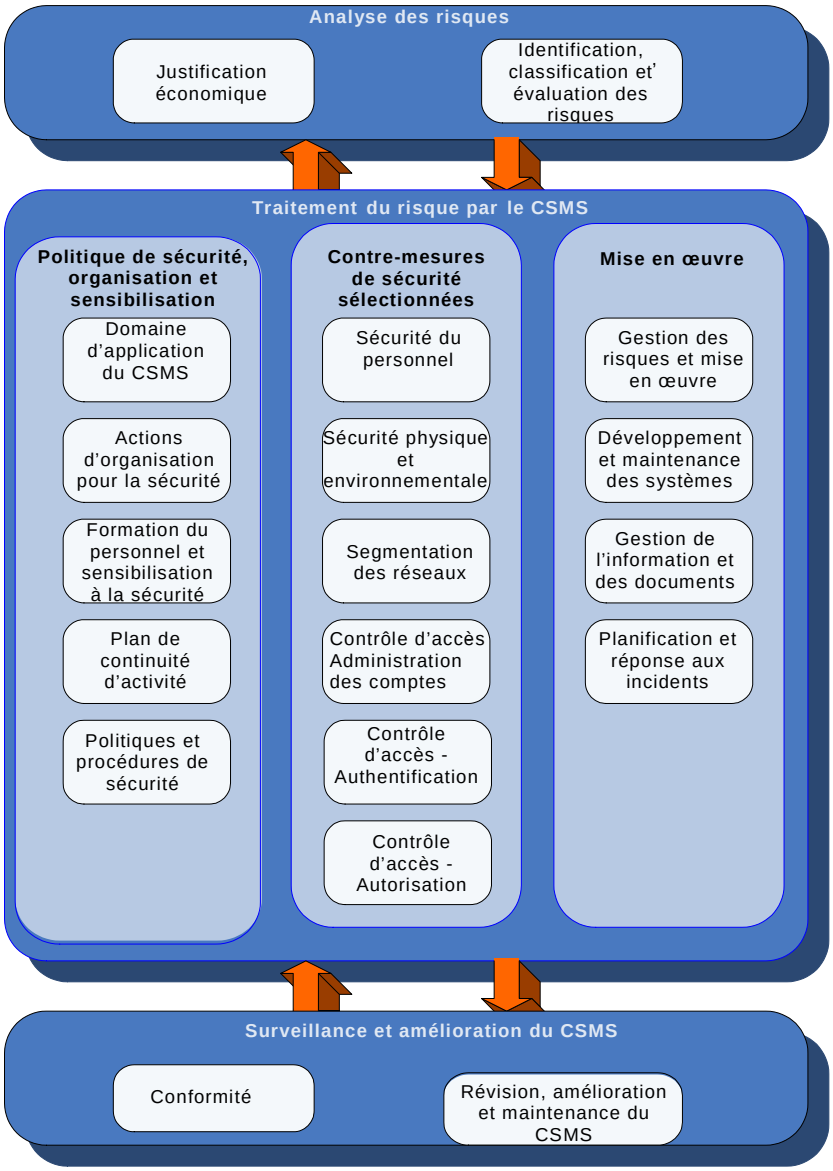



**Figure A.1 – Représentation graphique des éléments d'un système de gestion de la cyber-sécurité**

## A.2 Catégorie: Analyse des risques

### A.2.1 Description de la catégorie

La première catégorie principale du CSMS est l'analyse des risques. Cette catégorie donne la plupart des informations générales, qui se répercutent dans de nombreux autres éléments du CSMS. La Figure A.2 indique les deux éléments appartenant à cette catégorie:

- Justification économique, et
- Identification, classification et évaluation des risques.

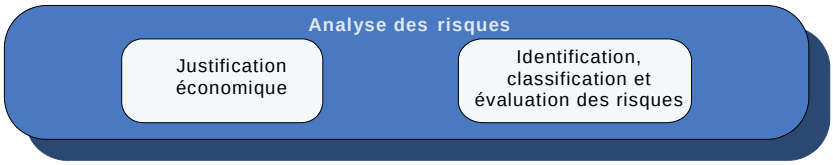



**Figure A.2 – Représentation graphique de la catégorie: Analyse des risques**

### A.2.2 Élément: Justification économique

#### A.2.2.1 Description de l'élément

Cet élément permet de faire en sorte que l'organisation comprenne l'importance de la cyber-sécurité pour le traitement de l'information utilisé dans les IACS. Cette compréhension repose sur la compréhension des rôles que le traitement de l'information joue dans la mission de l'organisation, des risques associés à cette mission, des coûts et autres impacts sur l'activité qu'entraîne la diminution de ces risques.

#### A.2.2.2 Risque de cyber-sécurité, justification économique et dossier d'activité

La première étape de la mise en œuvre d'un programme de cyber-sécurité pour les IACS consiste à développer une justification économique incontestable pour les besoins particuliers de l'organisation, afin de prendre en compte les cyber-risques. Une organisation peut construire la justification destinée aux CSMS des IACS et aux projets individuels associés, à partir des politiques existantes relatives à la sécurité, à la gestion générale des risques ou à l'adhésion aux exigences de la réglementation. D'autres organisations peuvent exiger que la justification économique prenne la forme d'un dossier d'activité formel ou informel pour les activités de gestion de la cyber-sécurité afin d'établir que le coût de l'atténuation des cyber-risques est justifié par les avantages financiers qu'elle offre. Utiliser une justification économique ou un dossier d'activité pour les premières étapes de la construction d'un CSMS dépendra d'une évaluation des risques, généralement de haut niveau. Une fois les risques reconnus, l'organisation est prête à prendre les mesures appropriées pour les atténuer. Les efforts pour réaliser une évaluation des risques plus systématique et plus détaillée (comme cela est décrit plus loin dans la présente norme) et les décisions individuelles au sujet des contre-mesures peuvent elles-mêmes nécessiter une justification économique, sans doute sous la forme d'un dossier d'activité.

La justification économique cerne les préoccupations de la direction concernant l'activité; elle repose sur l'expérience des personnes qui ont déjà eu affaire à la plupart de ces risques. Ce paragraphe traite des composants clés de la justification économique résultante et des ressources clés permettant d'identifier ces composants. Une justification économique peut avoir comme objet la justification d'une évaluation des risques détaillée ou de haut niveau, d'autres aspects spécifiques d'un CSMS complet tel qu'il est décrit ici, ou la mise en œuvre d'une contre-mesure unique.

L'expérience a montré que lorsqu'on se lance dans un programme de cyber-sécurité sans justification économique convenue, il y a fréquemment perte des ressources du programme au profit d'autres besoins de l'activité. Habituellement, ces autres besoins de l'activité présentent un avantage plus direct pour l'activité et une justification plus facile à comprendre.

#### A.2.2.3 Composants clés de la justification économique

La justification économique comprend quatre composants clés: les conséquences hiérarchisées pour l'activité, les menaces hiérarchisées, l'impact annuel estimé sur l'activité et le coût des contre-mesures.

a) Conséquences hiérarchisées pour l'activité

La liste des conséquences potentielles pour l'activité doit aboutir aux conséquences particulières pour l'activité que la direction supérieure considérera comme incontestables. Par exemple, une entreprise du secteur de la restauration qui ne manipule aucune substance toxique ou inflammable et traite ses produits à des températures et des pressions relativement basses ne se souciera probablement pas des dommages aux équipements ou des impacts sur l'environnement, mais se souciera probablement davantage des pertes de production et de la dégradation de la qualité des produits. Ici, l'idée repose sur les comptes rendus d'incidents passés ainsi que sur la connaissance de la façon dont les IACS sont effectivement utilisés dans le métier et sur la connaissance de l'impact potentiel que des modifications techniques non autorisées peuvent avoir sur l'activité. L'adhésion à la réglementation peut également être un sujet de préoccupation.

b) Menaces hiérarchisées

Il est nécessaire d'affiner la liste de menaces potentielles, si possible, afin qu'elle ne contienne que celles jugées crédibles. Par exemple, une entreprise du secteur de la restauration ne considèrera sans doute pas le terrorisme comme une menace crédible, mais elle se préoccupera bel et bien des virus, des vers et des employés mécontents. Ici, l'idée repose essentiellement sur les comptes rendus d'incidents qui ont eu lieu.

c) Impact annuel estimé sur l'activité

Il convient d'examiner attentivement les éléments de plus haute priorité figurant dans cette liste de conséquences hiérarchisées pour l'activité afin d'obtenir une estimation de l'impact annuel sur l'activité, de préférence, mais pas nécessairement, en termes financiers. Dans l'exemple de l'entreprise du secteur de la restauration, celle-ci a pu connaître un incident au cours duquel son réseau interne a été attaqué par un virus, incident que l'organisation chargée de la sécurité des informations a pu constater et qui avait eu un coût financier spécifique. Du fait que le réseau interne et le réseau de commande sont interconnectés, on peut concevoir qu'un virus émanant du réseau de commande puisse avoir un impact similaire sur l'activité. Ici, l'idée repose essentiellement sur les comptes rendus d'incidents passés. La conformité à la réglementation peut entraîner, en cas de non-conformité, des pénalités spécifiques soit financières, soit économiques.

d) Coût

Coût estimé des efforts humains et des contre-mesures techniques que cette justification économique apporte.

NOTE Une estimation de l'impact sur l'activité en termes financiers et des estimations du coût des contre-mesures sont exigées pour la création d'un dossier d'activité, mais une justification économique efficace peut ne pas inclure nécessairement ces informations.

De nombreuses ressources permettent d'obtenir les informations nécessaires à la constitution de cette justification économique: les ressources externes des organisations commerciales et les ressources internes des programmes de gestion de risques associés, au développement technique et aux opérations de l'activité.

Les ressources externes des organisations commerciales apportent souvent des suggestions utiles sur les facteurs qui ont le plus contribué à ce que leur direction soutienne leurs efforts, et sur les ressources qui se sont avérées les plus utiles dans leurs organisations. Ces facteurs peuvent différer d'un secteur d'activité à un autre, mais il peut exister des similitudes dans les rôles que peuvent jouer d'autres spécialistes de la gestion des risques.

Les ressources internes associées aux efforts de gestion des risques (c'est-à-dire la sécurité de l'information, les risques HSE, la sécurité physique et la continuité de l'activité) peuvent apporter dans l'organisation une assistance considérable de par leur expérience des incidents de ce type Ces informations sont utiles lorsqu'il s'agit de hiérarchiser les menaces et d'estimer les impacts sur l'activité. Ces ressources peuvent également donner une idée de la façon dont les responsables concentrent leurs efforts sur tel ou tel risque, et par conséquent donner une idée des responsables qui seront les plus appropriés ou réceptifs pour prendre le leadership.

Les ressources internes associées au développement et à l'utilisation des systèmes de commande peuvent donner des détails sur la façon dont les systèmes de commande sont effectivement utilisés dans l'organisation. Comment les réseaux sont-ils généralement cloisonnés? Comment les systèmes de combustion à haut risque ou les systèmes équipés pour la sécurité (SIS) sont-ils généralement conçus? Quelles sont les contre-mesures de sécurité qui sont déjà couramment utilisées? Si l'on garde à l'esprit les fusions et les acquisitions que l'organisation a déjà connues, il est également important de comprendre qu'un site particulier peut être tout à fait représentatif de l'unité d'activité, de la région ou de l'ensemble de l'organisation.

Ne pas oublier que lors des premières phases des opérations industrielles, l'accent était mis en premier lieu sur un ou deux problèmes de priorité élevée qui justifiaient un effort continuel. À mesure que le programme de cyber-sécurité IACS continue de se développer, d'autres éléments peuvent apparaître dans la liste et les priorités peuvent évoluer, parce que l'organisation applique une méthodologie d'analyse des risques plus rigoureuse. Il convient toutefois que ces évolutions ne diminuent pas le résultat de l'effort initial, qui a permis de justifier le lancement du programme.

#### A.2.2.4 Suggestions de contenu pour la justification économique IACS

Au sein de chaque organisation, la démarche consistant à développer un programme de cyber-sécurité efficace pour les IACS commence par le fait que des individus se rendent compte des risques encourus par l'organisation et se mettent à exprimer clairement ces risques de manière interne, pas simplement en termes techniques, mais en termes relatifs à l'activité et qui sont parlants pour la direction. Une justification économique n'est pas une évaluation des risques détaillée; il s'agit plutôt d'une description de haut niveau des risques, suffisante pour justifier les prochaines étapes planifiées de la construction d'un CSMS. La description peut être sommaire ou détaillée, en fonction des attentes des autorités qui prendront la décision pour l'organisation concernée.

Les conséquences négatives pour l'activité des cyber-attaques visant les IACS peuvent se décliner de la façon suivante:

- réduction ou perte de production sur un site ou plusieurs sites simultanément;
- blessures ou décès d'employés;
- blessures ou décès de personnes du voisinage;
- dommages aux équipements;
- dommages à l'environnement;
- non-respect des exigences de la réglementation;
- contamination du produit;
- responsabilités légales criminelles ou civiles;
- perte d'informations propriétaires ou confidentielles;
- perte d'image de la marque ou perte de confiance des clients;
- perte économique.

Quand on hiérarchise le risque que ces conséquences se produisent, il est également important de considérer la source ou la menace potentielle susceptible de lancer une cyber-attaque et la vraisemblance de la survenue de cet événement. Les cyber-menaces proviennent de sources qui peuvent être internes ou externes à l'organisation; les menaces peuvent être le résultat d'actions intentionnelles ou non intentionnelles; et les menaces peuvent viser une cible spécifique ou n'en viser aucune en particulier. Les incidents de cyber-sécurité peuvent être dus à différents types de sources de menaces, comme ce qui suit:

- Individus à la recherche de sensations fortes, amateurs ou personnes déséquilibrées éprouvant un sentiment de puissance, de maîtrise, d'importance personnelle ou de plaisir en réussissant à pénétrer les systèmes informatiques soit par des attaques non

dirigées (virus et vers), soit par des attaques dirigées (piratage) visant à voler ou détruire des informations ou à perturber les activités de l'organisation.

- Employés ou sous-traitants mécontents qui endommagent les systèmes ou volent des informations par vengeance ou par profit.
- Employés bien intentionnés qui, par inadvertance, modifient le mauvais contrôleur ou équipement opérationnel.
- Employés qui violent les politiques et procédures de qualité, sûreté ou sécurité pour satisfaire à d'autres besoins urgents (par exemple des impératifs de production).
- Terroristes habituellement motivés par des opinions politiques, pour qui les cyber-attaques constituent un moyen d'attaque peu coûteux et peu risqué, mais aux effets importants, en particulier lorsque ces attaques sont associées à des attaques physiques coordonnées.
- Malfaiteurs professionnels (y compris le crime organisé) dérobant des informations pour les revendre.
- Nations ou groupes adverses utilisant l'Internet comme arme militaire de guerre informatique pour perturber les capacités de commande, de contrôle et de communication d'un ennemi.

Des cas documentés donnent une idée de la façon dont l'une de ces sources de menaces a réussi à infliger des conséquences négatives pour l'activité, et à quelle fréquence elle le faisait. L'adoption rapide des nouvelles technologies de réseaux a conduit au développement de nouveaux outils permettant des cyber-attaques. Faute d'un système de signalement d'incident publiquement accessible et reconnu, il sera extrêmement difficile, dans un proche avenir, de déterminer la vraisemblance quantitative de l'apparition d'un type spécifique d'événement. La vraisemblance devra être évaluée qualitativement à partir de l'histoire interne de l'organisation en matière d'incidents, et des quelques cas qui ont été documentés publiquement. Voici quelques exemples de ces cas:

EXEMPLE 1 En janvier 2003, le vers SQL Slammer s'est répandu rapidement d'ordinateur à ordinateur à travers l'Internet et dans des réseaux privés. Il a pénétré un réseau informatique de la centrale nucléaire de Davis-Besse, dans l'Ohio, et a désactivé un système de surveillance pendant pratiquement cinq heures, alors que le personnel de la centrale était persuadé que le réseau était protégé par un pare-feu. Cela a pu se produire à cause d'une interconnexion non protégée entre l'usine et les réseaux de l'entreprise. Le vers SQL Slammer a coupé un réseau critique SCADA de l'installation après être passé d'un réseau de l'entreprise au réseau local (LAN) du centre de commande. Une autre installation a perdu le réseau à relais de trames qu'elle utilisait pour les communications, et certaines usines pétrochimiques ont perdu des interfaces homme-machine (IHM) et des historiques de données. Un centre d'appel à numéro d'urgence a été mis hors ligne, des vols aériens ont été retardés et annulés, et des distributeurs automatiques de billets ont été désactivés.

EXEMPLE 2 En 2001, pendant plusieurs mois, un sous-traitant mécontent du Queensland, en Australie, a mené une série de cyber-attaques contre un système de traitement d'eaux usées. L'une de ces attaques a entraîné le déversement de millions de litres d'eaux d'égout dans une rivière et un parc de la région. 46 intrusions ont eu lieu avant que l'auteur de ces actes ne soit arrêté.

EXEMPLE 3 En septembre 2001, un adolescent aurait piraté un serveur informatique du port de Houston pour attaquer une utilisatrice d'un forum de discussion féminin à la suite d'une dispute. Il a été affirmé que l'adolescent voulait mettre hors ligne l'ordinateur de cette femme en le bombardant d'une grande quantité de données inutiles, et qu'il devait utiliser un certain nombre de serveurs supplémentaires pour y parvenir. L'attaque a en réalité bombardé les systèmes de planification informatique du huitième plus grand port de la planète par des milliers de messages électroniques. Le service web du port, qui contenait des données cruciales pour les pilotes de navires, les compagnies d'amarrage et les entreprises de support chargées d'aider les navires à entrer et sortir du port, était devenu inaccessible.

L'organisation CERT a surveillé et recensé le nombre d'attaques subies par les systèmes reliés à l'Internet depuis 1988. Aucun des incidents signalés ne concernait les systèmes de commande. En 2004, elle a cessé de suivre le nombre d'attaques, car du fait de la multiplication des outils d'attaque automatisés, les attaques sont devenues très courantes et le nombre d'incidents signalés ne fournissait plus guère d'informations permettant d'évaluer la portée et l'impact des attaques. Un graphique des données concernant ces incidents est représenté à la Figure A.3 pour montrer l'augmentation considérable lors des 15 dernières années.

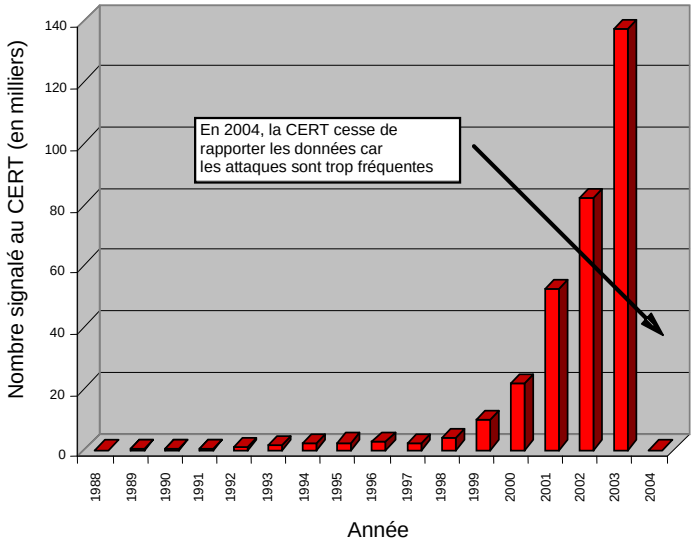



**Figure A.3 – Attaques subies et signalées par les systèmes informatiques jusqu'en 2004 (source: CERT)**

### A.2.2.5 Pratiques en support

#### A.2.2.5.1 Pratiques de base

Les pratiques de base sont les six actions suivantes:

a) Identifier et documenter les objectifs de l'activité, les processus d'activité critiques et les procédés informatiques critiques. Inclure les IACS et les interfaces avec les partenaires importants de la chaîne en cas de transfert, de stockage ou de traitement d'informations sensibles.

b) Identifier de quelle façon l'activité dépend des systèmes informatiques. Classer la dépendance de l'activité dans les catégories basse, moyenne, élevée, ou utiliser une variante du système de classement.

c) Identifier les différents scénarios de dommages dus à la perte de confidentialité, d'intégrité ou de disponibilité des informations. Inclure la manipulation des IACS et les conséquences de ces actions sur les activités qui utilisent ces systèmes. Inclure l'intégrité et la fiabilité HSE et opérationnelles pour les personnes qui font fonctionner les IACS. Capturer les risques associés à la chaîne de valeur et aux partenaires d'activité extérieurs. Ces risques comprennent souvent la perte ou l'altération d'informations sensibles. Exemple: l'interception d'informations associées aux expéditions de produits manufacturés, comme les types de matériaux, les quantités, les trajets d'expédition, le mode de transport, etc.

d) Développer des analyses d'impact sur l'activité pour la sécurité de l'IACS.

e) Développer des analyses d'impact sur l'activité pour la chaîne de valeur ou les partenaires d'activité extérieurs.

f) Déterminer le profil de tolérance des risques de l'organisation, défini en termes de:

   1) Sécurité du personnel (blessures graves ou décès);
   2) Perte ou impact financier, y compris les pénalités prévues par la réglementation;
   3) Conséquences environnementales et juridiques;
   4) Dégradation de l'image de l'entreprise;
   5) Impact sur l'ensemble des investisseurs;
   6) Perte de clientèle ou perte de confiance de la clientèle;
   7) Impact sur l'infrastructure.

NOTE La tolérance des risques dépend de l'activité. Pour exprimer les choses simplement, la tolérance des risques de l'organisation correspond à son seuil de tolérance du mal. La tolérance des risques peut être très faible (par exemple, une seule blessure grave peut ne pas être acceptable et doit être traitée immédiatement) en ce qui concerne la sécurité de la fabrication en usine ou peut être très élevée (par exemple en termes de perte de production) si l'organisation possède plusieurs sites de production d'une marchandise donnée. L'impact financier pour une activité peut ne pas être approprié pour d'autres activités. Il convient que les organisations menant différentes activités examinent l'interdépendance de ces activités lorsqu'il s'agit de déterminer la tolérance des risques.

Les responsables de la sécurité informatique connaissent en général le profil de tolérance des risques adopté dans l'organisation pour certaines conséquences, mais pas pour toutes. D'autres responsables chargés de la gestion des risques associés aux conséquences HSE connaissent le profil de tolérance des risques adopté dans l'organisation dans ces domaines. On doit déterminer le profil de tolérance des risques global en intégrant les informations provenant de ces sources ainsi que celles provenant de l'environnement IACS.

#### A.2.2.5.2 Pratiques additionnelles

Les pratiques additionnelles sont les trois actions suivantes:

a) Identifier et documenter les objectifs de l'activité, les processus d'activité critiques et les procédés informatiques (IT) critiques. L'idéal est de confier ce processus à une section transversale de l'organisation représentant les zones fonctionnelles ainsi que les unités d'activité de l'entreprise. Ce groupe est normalement créé et doté d'une charte managé par un cadre supérieur responsable de l'organisation IT ou par une équipe dirigeante composée de cadres supérieurs des différentes parties de l'organisation. Cette charte comprend spécifiquement les risques associés aux IACS.

b) Développer une analyse d'impact sur l'activité qui décrit les problèmes et les conséquences de l'inaction et les avantages de l'action. Si possible, on quantifiera ces actions en termes d'impacts financiers (c'est-à-dire les ventes perdues et les amendes), d'impacts sur le marché (c'est-à-dire la perte de confiance ou d'image auprès du public), ainsi que d'impacts HSE (c'est-à-dire les décharges dans l'environnement, les dommages causés aux équipements et les pertes en vies humaines). Si l'on considère en particulier des conséquences telles que la perte de l'image auprès du public, il est important de comprendre qu'un incident d'une activité particulière peut affecter l'organisation dans son ensemble.

c) Documenter et faire approuver (au niveau directorial approprié) les risques situés en dehors du domaine d'application du CSMS.

#### A.2.2.6 Ressources utilisées

Cet élément repose en partie sur des informations provenant des références suivantes, répertoriées dans la Bibliographie: [24], [26], [27], [30], [42].

### A.2.3 Élément: Identification, classification et évaluation des risques

#### A.2.3.1 Description de l'élément

Les organisations protègent leur capacité à remplir leur mission en identifiant, hiérarchisant et analysant, d'une manière systématique, les menaces, les vulnérabilités et les conséquences potentielles au moyen de méthodologies acceptées. Le risque est défini formellement comme étant une prévision de perte exprimée par la probabilité qu'une menace particulière exploite une vulnérabilité particulière avec une conséquence particulière (voir IEC/TS 62443-1-1). Comme décrit dans l'élément associé Gestion des risques et mise en œuvre (voir A.3.4.2), une organisation définit sa tolérance aux risques en termes de caractéristiques des menaces, des vulnérabilités et des conséquences potentielles qu'elle identifie. Puis l'organisation met en œuvre cette décision concernant la tolérance des risques en entreprenant les actions indiquées pour réduire la vraisemblance d'une menace contre la sécurité et/ou en réduisant les conséquences dans le cas d'une menace contre la sécurité qui aurait déjà été mise à exécution.

#### A.2.3.2 Cyber-risques pour les IACS

L'approche de gestion des risques présentée en A.2.2 s'applique d'une manière générale à tous les types de cyber-risques, mais aussi aux autres types de risques. La présente discussion concerne les aspects propres à l'analyse des cyber-risques encourus par les IACS.

Les différentes industries peuvent estimer que certains types d'impacts sur l'activité sont plus préoccupants et avoir l'impression que certains types de menaces sont plus vraisemblables, mais il convient que toutes les industries utilisant des IACS comprennent qu'elles entrent dans un nouveau domaine de risques. Dès l'instant où les IACS ont adopté les systèmes d'exploitation informatiques et technologies de réseau du commerce et où les utilisateurs ont interconnecté leurs réseaux privés et leurs réseaux IACS, le nombre de menaces a augmenté considérablement. Nous avons les risques associés aux informations traditionnelles (électroniques ou papier), aux systèmes et applications IT classiques, aux IACS, aux partenaires d'activité, aux co-entreprises, aux partenaires d'externalisation, etc.

Pour les risques encourus par les actifs informatiques traditionnels, on met l'accent sur la confidentialité, l'intégrité et la disponibilité des informations. Les risques encourus par les IACS sont différents, du fait que les opérateurs mettent également l'accent sur les facteurs HSE et la fiabilité opérationnelle, en plus de la traditionnelle protection de la confidentialité, de l'intégrité et de la disponibilité des informations. Avec les IACS, les priorités sont généralement inversées, l'accent étant mis dans cet ordre sur la disponibilité, l'intégrité et la confidentialité. Cela signifie qu'il convient, autant que possible, de coordonner l'évaluation des cyber-risques encourus par les IACS avec la sécurité physique et les facteurs HSE. Certaines organisations intègrent entièrement les efforts d'évaluation des risques relatifs à chacun de ces domaines. Les risques que l'on encourt en faisant appel à l'externalisation, à des sous-traitants extérieurs ou à d'autres partenaires important de la chaîne de fabrication. Ces risques concernent les informations sensibles émises, stockées ou traitées. L'intégration de ces partenaires d'activité dans les opérations d'une organisation ouvre la porte à des accès non intentionnels aux systèmes de l'entreprise.

Dans pratiquement chacun de ces cas, les opérations et technologies industrielles liées à la sécurité, développées pour les applications IT classiques n'ont pas été déployées pour les IACS, d'une part à cause d'une certaine ignorance, d'autre part à cause des contraintes réelles qui n'existent pas dans les applications IT classiques. L'objet de la présente norme est de traiter ces deux problèmes.

#### A.2.3.3 Processus d'évaluation des risques

##### A.2.3.3.1 Généralités

Une présentation des risques est nécessaire pour établir la justification économique d'un CSMS. Les priorités plus détaillées prises en compte par ce système sont déterminées d'après une méthodologie qui considère systématiquement le risque à un niveau de granularité plus élevé que ce que l'on évalue habituellement pour établir une justification économique initiale.

##### A.2.3.3.2 Évaluation des risques et évaluation des vulnérabilités

Dans la littérature générale, les termes évaluation des risques et évaluation des vulnérabilités sont parfois utilisés l'un pour l'autre. On peut différencier ces deux sortes d'analyses d'après les définitions de vulnérabilité et de risque données dans la présente norme. On se rappellera qu'une vulnérabilité est définie comme étant une faille ou une faiblesse dans la conception, la mise en œuvre ou l'utilisation et la gestion d'un système, qui pourrait être exploitée dans le but de violer l'intégrité ou la politique de sécurité du système (voir IEC/TS 62443-1-1). À titre d'exemple, si l'on observe que l'on ne change pas souvent les mots de passe dans une salle de commande, il s'agit là d'une vulnérabilité que l'on pourrait identifier dans une évaluation des vulnérabilités. Il peut exister différents risques associés à cette vulnérabilité, par exemple:

- Une faible vraisemblance que le mot de passe devienne bien connu dans l'usine au fil du temps et qu'un employé légitime non formé à l'utilisation du système de commande utilise le mot de passe pour tenter de résoudre un problème et provoque en entrant des données erronées une perte de production de plusieurs heures.
- Une faible vraisemblance qu'un ancien employé mécontent réussisse à franchir les pare-feu de défense et accède au réseau du système de commande à distance, se connecte à une IHM et effectue délibérément des actions pouvant interrompre la production pendant plusieurs jours.

Par conséquent, la façon dont ces termes sont utilisés dans la présente norme, une évaluation des risques produit en sortie un ensemble de risques, et une évaluation des vulnérabilités produit en sortie un ensemble de vulnérabilités, qui n'ont pas encore été analysées pour déterminer les risques qu'elles entraînent. Une évaluation des vulnérabilités est donc une entrée pour une évaluation des risques. Il faut noter que certaines méthodologies existantes, intitulées méthodes d'évaluation des vulnérabilités, comprennent des concepts de risque, mais d'autres non.

Si l'on revient à l'exemple ci-dessus du mot de passe de la salle de commande, il est clair qu'il existe également des risques liés au fait de changer périodiquement le mot de passe du système de commande, par exemple une possibilité faible que l'opérateur puisse oublier le nouveau mot de passe lors d'une situation d'urgence et soit incapable de se connecter pour résoudre un problème, avec pour conséquence des dommages collatéraux importants pour l'environnement. Le compromis entre les risques éliminés par une contre-mesure et les risques introduits par cette contre-mesure, comme dans le cas précédent, est décrit dans l'élément Gestion des risques et mise en œuvre de la présente norme (voir A.3.4.2).

#### A.2.3.3.3 Évaluation de haut niveau ou détaillée des risques

L'évaluation des risques peut être réalisée à plusieurs niveaux. La présente norme exige une évaluation des risques à deux niveaux, appelés évaluation de haut niveau des risques et évaluation détaillée des risques.

L'évaluation de haut niveau des risques examine quel pourrait être l'impact des types généraux de vulnérabilité de cyber-sécurité et la vraisemblance qu'une menace puisse s'exercer contre ces vulnérabilités, mais ne prend pas en compte de cas particuliers de ces vulnérabilités ou de contre-mesures connexes déjà en place. Des exemples de risques identifiés dans une évaluation des risques de haut niveau pourraient donc être:

- Une vraisemblance moyenne qu'une infection par malware se produise et provoque une congestion du réseau de commande et par conséquent un manque de visibilité du statut du procédé industriel dans la salle de commande, avec pour résultat un arrêt d'urgence potentiel et les coûts associés.
- Une faible vraisemblance qu'un sous-traitant ayant des intentions criminelles et accédant au support du réseau du système de commande puisse lire les informations sur ce support et réussisse à modifier les ordres de commande de façon à endommager l'installation.

L'évaluation de haut niveau est indispensable, car l'expérience a montré que si les organisations commencent par examiner les vulnérabilités détaillées, elles passent à côté du cyber-risque dans son ensemble et ont du mal à déterminer sur quoi elles doivent concentrer leurs efforts de cyber-sécurité. L'examen des risques à un niveau élevé peut permettre de concentrer les efforts sur les évaluations de vulnérabilités détaillées. L'évaluation de haut niveau peut normalement couvrir tous les réseaux de commande que possède l'organisation, par exemple en les répartissant en groupes possédant des caractéristiques communes. Toutes les ressources nécessaires peuvent ne pas être disponibles pour couvrir tous les IACS au niveau détaillé.

L'évaluation détaillée des risques, telle qu'elle est définie dans la présente norme, est étayée par une évaluation des vulnérabilités détaillée qui comprend le fait d'examiner des détails tels que les contre-mesures techniques existantes, le respect des procédures de gestion des

comptes, le statut des correctifs et des ports ouverts sur chacun des hôtes individuels d'un réseau de système de commande spécifique et les caractéristiques de connectivité des réseaux telles que la séparation par pare-feu et la configuration. Voici un exemple de ce que pourrait produire en sortie une évaluation détaillée des risques:

- Le raccordement direct de stations de travail techniques à la fois au réseau d'entreprise et au réseau du système de commande de l'installation sud, lequel contourne le pare-feu interne du réseau de commande, contribue au risque d'infection par malware du réseau de commande. En plus du fait que 50 % des hôtes du réseau de commande de l'installation sud sont dépourvus de protection antivirus, il en résulte une vraisemblance moyenne qu'un incident de congestion déclenché par un virus provoque une absence de visibilité du état du fonctionnement industriel dans la salle de commande et entraîne comme conséquence une fermeture d'urgence potentielle et les coûts associés.
- Tous les supports du réseau du système de commande (par exemple, les adresses 192.168.3.x) et les connexions aux autres réseaux, soit sont physiquement protégés par des murs, des plafonds ou des sols, soit se trouvent dans des salles fermées à clé accessibles aux trois administrateurs système autorisés de la salle de commande. Par conséquent, le risque d'une intrusion réussie sur ce support est faible.

Ces résultats d'évaluation des risques détaillée corroborent les résultats correspondants de l'évaluation de haut niveau, d'après les exemples ci-dessus. Cependant, l'évaluation des risques détaillée peut, dans de nombreux cas, déterminer que les risques sont plus faibles ou plus élevés que ce que l'évaluation de haut niveau permet de supposer. L'évaluation des risques détaillée peut également révéler des risques qui n'ont pas été envisagés dans l'évaluation de haut niveau. Enfin, du fait que l'évaluation détaillée identifie des vulnérabilités spécifiques, elle fournit une orientation quant à la façon dont une organisation peut traiter les risques jugés inacceptables.

#### A.2.3.3.4 Types de méthodologies d'évaluation des risques

##### A.2.3.3.4.1 Généralités

Il existe différentes méthodes d'évaluation des risques qui ont été développées et mises sur le marché par différentes organisations. On peut en général les classifier d'après deux facteurs: la façon dont elles caractérisent les risques individuels (qualitativement ou quantitativement) et la façon dont elles structurent l'exercice d'identification des risques (basé sur les scénarios ou basé sur les actifs).

##### A.2.3.3.4.2 Qualitative ou quantitative

L'évaluation qualitative des risques utilise habituellement les informations fournies en entrée par les employés expérimentés et/ou les experts, pour produire des informations concernant la vraisemblance et la gravité des menaces spécifiques ayant un impact sur des actifs spécifiques. De plus, les différents niveaux de vraisemblance et de gravité sont identifiés par des classes générales telles que "élevé", "moyen" et "faible", plutôt que par des probabilités spécifiques ou des impacts économiques. L'évaluation des risques qualitative est préférable en l'absence d'informations fiables sur la vraisemblance de menaces spécifiques qui affectent des actifs spécifiques, ou permettent d'estimer l'impact global des dommages occasionnés aux actifs spécifiques.

L'évaluation quantitative des risques utilise habituellement des ensembles de données complets permettant de documenter la rapidité à laquelle les actifs sont endommagés en fonction de l'exposition à des combinaisons définies de menaces et de vulnérabilités. Si cette information est disponible, elle peut permettre de fournir des estimations de risques plus précises que les méthodes d'évaluation qualitatives des risques. Du fait de l'exposition récente des IACS aux menaces de cyber-sécurité, de la rareté relative des incidents et de l'évolution rapide de la nature des menaces, il n'existe pas encore d'ensembles de données complets facilitant l'évaluation des menaces de cyber-sécurité encourues par les IACS. À ce stade, l'évaluation des risques qualitative est la méthode préférable pour évaluer ces risques.

#### A.2.3.3.4.3 Basée sur les scénarios ou basée sur les actifs

Quand on effectue une évaluation des risques, il est habituellement utile d'orienter les réflexions du participant sur l'un des deux aspects suivants: les scénarios suivant lesquels les menaces exploitent les vulnérabilités pour affecter les actifs, et les actifs eux-mêmes. L'approche basée sur les scénarios tire parti de l'expérience retirée des incidents réels ou de ce qui était presque des incidents. Cependant, l'approche peut ne pas être suffisamment pertinente pour permettre de découvrir des menaces ou des vulnérabilités susceptibles de toucher des actifs sensibles qui n'ont jamais été menacés auparavant. L'approche basée sur les actifs tire parti de la connaissance des systèmes et méthodes de travail d'une organisation, et des actifs particuliers dont la dégradation aurait un impact économique élevé. Cette approche peut cependant ne pas être suffisamment pertinente pour permettre de découvrir des types de menaces ou de vulnérabilités qui mettraient ces actifs en danger, ou des scénarios qui impliqueraient plus d'un actif. Quelle que soit l'approche générale utilisée, il est recommandé d'inclure certain aspects de l'autre approche pour une évaluation des risques plus approfondie.

EXEMPLE Comme exemple d'intégration de méthodes basées sur les scénarios et de méthodes basées sur les actifs, prenons le cas d'une organisation qui a identifié comme actifs ses dispositifs, ses applications et ses données. Dans la prochaine étape, l'organisation dresse la liste des scénarios possibles concernant ces actifs et détermine les conséquences de la façon suivante. Les scénarios pour les applications sont très similaires aux scénarios représentés pour les dispositifs.

a) Scénarios pour les dispositifs

   1) Scénario: Un utilisateur non autorisé accède localement à un dispositif IACS

      Quelle est la conséquence si quelqu'un se rend sur le dispositif et effectue les tâches autorisées sur ce dispositif?

   2) Scénario: Accès distant à un dispositif IACS par un utilisateur non autorisé

      Quelle est la conséquence si un utilisateur non autorisé accède à distance à ce dispositif et effectue une des tâches autorisées sur ce dispositif?

   3) Scénario: Dispositif IACS désactivé ou détruit

      Quelle est la conséquence d'un cyber-incident empêchant le dispositif d'effectuer la totalité de ses fonctions normales ou un sous-ensemble de celles-ci?

b) Scénarios sur les données

   1) Scénario: Vol de données d'IACS

      Quelle est la conséquence si quelqu'un vole cet ensemble de données?

      - L'ensemble de données a-t-il une valeur de propriété intellectuelle élevée?
      - L'ensemble de données a-t-il de la valeur pour l'activité d'un concurrent?
      - Si l'ensemble de données était diffusé publiquement, est-ce que cela produirait une situation embarrassante?
      - L'ensemble de données est-il nécessaire à l'adhésion à la réglementation?
      - L'ensemble de données est-il en relation avec un litige?

   2) Scénario: Corruption de données d'IACS

      Quelles sont les conséquences potentielles si:

      - L'ensemble de données a été intercepté et modifié entre la source et la destination?
      - L'ensemble de données a été corrompu à la source?
      - L'ensemble de données est-il nécessaire à l'adhésion à la réglementation?
      - L'ensemble de données est-il en relation avec un litige?

   3) Scénario: Refus de service aux données d'IACS

      Quelle est la conséquence si l'utilisateur des données n'est pas à même d'accéder à l'ensemble de données d'IACS?

NOTE Un groupe peut entreprendre une évaluation des risques basée sur les scénarios en partant de descriptions de scénarios d'incidents puis en déterminant les conséquences du scénario, comme indiqué dans cet exemple, ou commencer par créer une liste de conséquences indésirables, puis travailler à rebours pour développer des scénarios d'incidents possibles susceptibles de produire ces conséquences. On peut également combiner ces approches.

#### A.2.3.3.5 Choisir la méthodologie d'évaluation des risques

Choisir la bonne méthodologie d'évaluation des risques pour une organisation est très subjectif, car cela dépend d'un certain nombre de questions. Nombre de ces méthodologies sont disponibles dans le commerce. Certaines peuvent être utilisées gratuitement; d'autres nécessitent une licence d'utilisation. Évaluer ces méthodologies pour trouver la plus adaptée à une organisation donnée peut être une tâche difficile. La plupart de ces méthodologies ont en commun le fait que le risque est une combinaison de la vraisemblance qu'un événement se produise et des conséquences de cet événement.

La difficulté réside dans le fait de déterminer comment attribuer des nombres quantitatifs à la vraisemblance, laquelle s'exprime de manière assez similaire à la probabilité. L'expérience industrielle en matière de sécurité des procédés et d'accidents fournit une grande quantité de données quantitatives historiques à partir desquelles on peut déduire des valeurs de probabilités. Mais chiffrer de façon appropriée la vraisemblance d'un cyber-incident spécifique n'est pas chose facile, d'une part à cause du manque de données historiques, et d'autre part parce que le passé peut ne pas nécessairement prévoir l'avenir dès lors qu'une vulnérabilité est connue d'attaquants potentiels. Du fait de cette difficulté, de nombreuses entreprises et associations commerciales font le choix de développer leur propre méthodologie pour résoudre les problèmes de menace et de vulnérabilité présentant pour elles une certaine importance, d'une manière conforme à leur culture. C'est pour cette même raison que la présente norme utilise le terme *vraisemblance*, qui se rapporte aux estimations des capacités et intentions humaines, plutôt que le terme habituel *probabilité*, qui se rapporte à l'apparition d'événements naturels non influencés par l'intervention humaine.

Certaines méthodologies intègrent bien les évaluations de risques de haut niveau. Certaines intègrent bien les évaluations de risques détaillées, en permettant d'entrer des résultats d'évaluations de vulnérabilités, et peuvent aussi fournir directement des instructions pour l'évaluation des vulnérabilités détaillée. Pour une organisation, il est judicieux d'employer une méthodologie intégrant de façon cohérente à la fois les évaluations de risques de haut niveau et les évaluations de risques détaillées.

EXEMPLE Le Chemical Information Technology Center (ChemITC) du American Chemistry Council est un exemple d'association commerciale ayant apporté son aide pour la sélection de méthodologies appropriées en publiant un document intitulé "Report on Cyber Security Vulnerability Assessment Methodologies Version 2.0" (Rapport sur les méthodologies d'évaluation des vulnérabilités de cyber-sécurité, version 2.0). [27] Ce document examine différents éléments extraits de onze méthodologies différentes et les compare à un ensemble de critères importants dans une méthodologie universelle des risques de cyber-sécurité pour permettre d'évaluer les systèmes informatiques de l'activité, les IACS et les systèmes de chaîne de valeur. Le rapport fournit des avis utiles pour le choix d'une méthodologie. Une partie des instructions a été incluse dans ce qui suit grâce à la permission du CSCSP.

a) Étape 1 – Filtrage

La première étape consiste à examiner la présentation des méthodologies sélectionnées. L'objet de cette étape est de filtrer les méthodologies intéressantes au moyen de critères tels que la facilité d'utilisation, la complexité, le domaine d'application, les besoins en ressources et le type de méthodologie (voir [27], Annexe IV).

b) Étape 2 – Sélection

Une fois les méthodologies identifiées, sélectionner celles qui sont adaptées aux besoins de l'organisation (voir [27], pièce jointe II). La pièce jointe II identifie les critères particuliers qui ont été utilisés pour évaluer la méthodologie. Les critères énumérés ici s'appliquent à un domaine de traitement de l'information beaucoup plus vaste que celui des IACS. Une méthodologie destinée à un sous-ensemble des critères utilisés dans l'étude du ChemITC peut être nécessaire. Il est utile de comprendre la différence entre les besoins de l'organisation et les critères d'évaluation lorsque l'on étudie les résumés des différentes méthodologies. Étudier ensuite les résumés correspondants pour obtenir des informations plus détaillées qui contribueront au choix éclairé d'une méthodologie (voir [27], Annexe V).

Le résumé de chacune des méthodologies aborde les sujets suivants:

- méthodologie d'évaluation des vulnérabilités en matière de cyber-sécurité,
- examinateurs,
- date,
- adresse web,
- observations générales,
- forces, d'après les critères d'évaluation courants,

- lacunes, d'après les critères d'évaluation courants,
- comment cette méthodologie pourrait être utilisée,
- limitations sur l'utilisation de la méthodologie, et
- révisions suggérées.

c) Étape 3 – Validation (option)

En cas d'incertitude ou de difficulté dans le choix de la méthodologie, examiner les tableaux de critères techniques présentés dans le document de référence de la méthodologie pour valider le ou les choix de l'organisation (voir [27], pièce jointe II). Il existe des tableaux de critères techniques pour chacune des méthodologies. Cette étape est optionnelle car elle ne fait que fournir des données d'évaluation encore plus spécifiques.

d) Étape 4 – Acquérir la méthodologie sélectionnée

Une fois le nombre de méthodologies sélectionnées réduit à un, se procurer la méthodologie auprès du fournisseur. Les adresses web indiquées dans la bibliographie constituent un bon point de départ.

#### A.2.3.3.6 Évaluation des risques de haut niveau – Identification des risques

Une fois qu'un ensemble de parties prenantes clés a été identifié et a reçu une formation sur la nature des IACS, ces personnes effectuent une évaluation des risques de haut niveau en suivant la méthodologie sélectionnée par l'organisation. Ce processus d'évaluation clarifie la nature des risques individuels qu'encourt l'organisation du fait de l'utilisation des IACS. Cette clarification est nécessaire pour permettre de choisir les contre-mesures les plus économiques à concevoir et déployer pour contribuer à justifier le coût de ce déploiement. Si cette tâche est la première étape d'une évaluation de risques, elle NE constitue PAS pour autant une évaluation détaillée des vulnérabilités ou des menaces. Elle comprend normalement une session d'analyse des risques destinée à rassembler des informations fournies par les parties prenantes et exploite les conséquences de haut niveau pour l'activité qui auront pu avoir été identifiées dans la justification économique.

Le document que doit produire la séance d'analyse des risques est une liste de scénarios qui décrivent la façon dont une menace particulière pourrait exploiter un type de vulnérabilité particulier et endommager certains actifs, avec pour résultat des conséquences négatives identifiées pour l'activité. La même séance peut également d'aborder l'étalonnage des niveaux de conséquence et la hiérarchisation des risques par niveau de tolérance.

Les parties prenantes qui possèdent une expérience des applications IACS dans les unités d'activité et les personnes responsables de la gestion des risques associés doivent participer à la démarche d'évaluation des risques pour apporter leur expertise et leur expérience.

Pour utiliser au mieux le temps des participants, il est normalement nécessaire de prévoir une demi-journée ou une journée complète pour la séance d'analyse des risques, à laquelle doivent participer toutes les parties prenantes. Cette séance d'analyse des risques comprend deux phases: les informations de fond et l'identification des risques.

Quelle que soit la méthode d'évaluation des risques finalement utilisée, il est également important de fournir des informations de fond aux participants de la séance d'analyse des risques avant de procéder à l'identification des risques. Les informations de fond comprennent généralement une présentation de la justification et de la charte d'activité, une présentation des architectures et des fonctions des IACS et une présentation des types spécifiques des incidents qui se sont produits dans l'organisation ou des incidents publiés qui se sont produits dans d'autres organisations.

Pour que la séance soit réussie, il est également important que les participants comprennent les définitions des mots risques et vulnérabilités, faute de quoi la séance permettra probablement d'identifier les vulnérabilités, mais pourrait ne pas réussir à identifier les risques. À cette fin, il est utile de présenter des exemples. Par exemple, une vulnérabilité pourra être une authentification faible sur l'IHM du système de commande. La menace correspondante pourra être le fait qu'un employé inexpérimenté puisse actionner l'IHM sans être supervisé et configurer des paramètres dangereux. La conséquence pourrait être une coupure de la production due à la mise en route de contrôles de sécurité. Les organisations

tombent souvent dans le piège consistant à énumérer les cyber-vulnérabilités, pour travailler ensuite à les atténuer.

#### A.2.3.3.7 Évaluation des risques de haut niveau – Classification des risques

##### A.2.3.3.7.1 Généralités

La liste des scénarios résultant de la séance d'analyse des risques décrit différents risques auxquels les organisations sont exposées du fait des menaces que les IACS peuvent subir. L'un des devoirs de la direction de l'entreprise est de gérer l'ensemble des risques auxquels ses organisations sont exposées. Pour faciliter cette démarche, il est nécessaire d'identifier et de hiérarchiser les risques. Ce paragraphe décrit les trois étapes nécessaires au développement d'un cadre de travail permettant de hiérarchiser les risques individuels afin de pouvoir justifier les actions correctives appropriées.

##### A.2.3.3.7.2 L'équation des risques

Avant de décrire le cadre de travail de la hiérarchisation et de l'étalonnage des risques, il est important de comprendre un concept élémentaire de l'analyse des risques (par exemple, l'équation des risques).

La vraisemblance qu'un événement se produise prend en compte d'une part la vraisemblance qu'une menace susceptible de causer une action soit exécutée et d'autre part la vraisemblance qu'une vulnérabilité qui autorise cette action soit effectivement exploitée par la menace. Par exemple, pour qu'un virus paralyse un réseau, il doit d'abord atteindre le réseau, puis déjouer les contrôles antivirus du réseau. Si la vraisemblance est exprimée de manière similaire à une probabilité, alors:

$$Vraisemblance_{Apparition\_événement} = Vraisemblance_{Exécution\_menace} \times Vraisemblance_{Vulnérabilité\_exploitée} \quad \text{(A.1)}$$

Comme décrit ci-dessus, le risque est constitué d'une part d'une vraisemblance et d'autre part d'une conséquence, la conséquence étant l'impact négatif subi par l'organisation du fait du dommage spécifique produit par la menace ou la vulnérabilité spécifique au(x) actif(s) de l'organisation.

$$Risque = Vraisemblance_{Apparition\_événement} \times Conséquence \quad \text{(A.2)}$$

##### A.2.3.3.7.3 Étalonnage des échelles de vraisemblance et de conséquence

Des systèmes de gestion des risques ont été développés dans la plupart des organisations pour leur permettre de faire face à toutes sortes de risques. Dans certains cas, l'utilisation de ces systèmes a été dictée par les exigences de la réglementation. Ces systèmes de gestion des risques utilisent la même équation des risques pour hiérarchiser les risques que font encourir à l'organisation un même type de menaces à différents actifs (par exemple, sécurité des informations) ou différentes menaces aux mêmes actifs (c'est-à-dire la continuité d'activité, la sécurité des opérations industrielles, la sécurité environnementale et la sécurité physique). Dans la plupart des organisations, ces systèmes de gestion des risques ont déjà développé des échelles de vraisemblance et de conséquence.

Le Tableau A.1 représente une échelle de vraisemblance typique. Cette échelle n'est qu'un exemple; l'organisation doit déterminer par elle-même les valeurs réelles utilisées dans cette échelle.

**Tableau A.1 – Échelle de vraisemblance typique**

| Vraisemblance | |
|---|---|
| **Catégorie** | **Description** |
| Élevée | Une menace/vulnérabilité dont l'apparition est probable au cours de la prochaine année. |
| Moyenne | Une menace/vulnérabilité dont l'apparition est probable au cours des 10 prochaines années. |
| Basse | Une menace/vulnérabilité pour laquelle il n'y a aucun antécédent et dont la vraisemblance d'apparition est estimée improbable. |

La plupart des organisations estiment qu'il est difficile de convenir d'une vraisemblance, et il n'existe que très peu d'informations permettant d'y parvenir. Il est évident que si les opinions divergent sur ce facteur, les investissements effectués par le CSMS pourront varier du tout au tout. Même si tout le monde n'est pas d'accord avec l'évaluation finale de la vraisemblance, il existe tout de même un avantage à l'utiliser, qui est que les hypothèses utilisées pour enclencher les investissements du CSMS sont claires et visibles par tous. Du fait que la vraisemblance est un facteur essentiel, en ce qui concerne les risques, sur lequel l'organisation n'a que très peu d'informations et de contrôle, il est important de s'informer des améliorations des données dont dispose l'industrie et qui permettraient d'apporter de la précision à ce facteur.

Pour tenter de résoudre le problème du défaut de consensus, certaines organisations utilisent les méthodes suivantes:

- Utiliser une probabilité de 100 % pour la vraisemblance et ne considérer ainsi que les conséquences, ou faire cela pour certains types de conséquences telles que les conséquences HSE;
- Convenir d'une plage de probabilités ou de catégories de vraisemblance, puis travailler le processus de hiérarchisation en utilisant ces plages;
- Rechercher une plus grande précision en consultant les données dont dispose l'industrie sur les attaques contre les IACS;
- Rechercher une plus grande précision en rassemblant des données sur des incidents internes;
- Séparer la vraisemblance en deux facteurs – la vraisemblance qu'un adversaire tente une attaque et la vraisemblance que cette attaque réussisse. Séparer ces facteurs peut contribuer à clarifier l'origine véritable du désaccord. Si tout le monde peut convenir qu'une tentative va réussir et que l'argument du risque faible repose sur l'espoir qu'aucune tentative n'aura lieu, la teneur de la discussion peut, de ce fait, changer.

La conséquence est habituellement mesurée en termes différents pour différents types de risques. Le Tableau A.2 représente une échelle de conséquence typique. Cet exemple illustre la façon dont l'évaluation des cyber-risques peut prendre en compte la sécurité des procédés et d'autres risques organisationnels. Comme ci-dessus, cette échelle n'est qu'un exemple, l'organisation devant étalonner sa propre échelle.

Il est important de faire preuve d'un haut niveau d'honnêteté intellectuelle quand on évalue les conséquences. Au cours de l'évaluation, identifier les hypothèses qui ont un impact sur le niveau de conséquence. Par exemple, on peut raisonnablement considérer que tous les verrouillages de sécurité et les systèmes de coupure sont en place pour minimiser l'impact d'un événement, étant donné que la vraisemblance d'un cyber-événement combiné à un accident sans rapport, qui désactiverait les systèmes de sécurité, est très faible. Cependant, quand on fait cette hypothèse, on doit également examiner s'il existe un risque de cyber-attaque intentionnelle, profitant de la défaillance accidentelle des systèmes de sécurité, ou un risque d'attaque physique ou de cyber-attaque coordonnée provoquant cette défaillance. Les autres hypothèses possibles que l'on peut évoquer sont que les pratiques opérationnelles

sont suivies comme elles le sont dans tout fonctionnement normal, et que les procédures de fermeture fondamentales sont suivies. Il est important que les sites évaluent honnêtement les risques, en gardant à l'esprit la sophistication et l'état du système de commande et des opérations associées, ainsi que le fait que l'installation dépend de ce système pour fonctionner.

L'étalonnage des conséquences doit obligatoirement s'effectuer dans le respect des intérêts et des politiques de l'organisation qui effectue l'évaluation des risques. Les risques qu'encourent les IACS peuvent être très influencés par les dangers associés aux opérations industrielles commandées par ces IACS, mais il est important de ne pas confondre les dangers encourus par l'organisation avec ceux encourus par la société. Les opérations industrielles peuvent ne pas employer de substances dangereuses, mais produire un produit de valeur très demandé, qui génère des profits importants pour l'entreprise. Un incident de sécurité IACS provoquant des perturbations dans les opérations, conduisant à la production de produits hors spécification et invendables pendant plusieurs jours, peut avoir un impact financier considérable pour l'entreprise. Pour cette entreprise, les IACS ont un niveau de risque élevé, même si la société peut estimer qu'au contraire, le risque est faible car il n'y a pas d'impact de type santé, sécurité ou environnement pour le grand public. De manière similaire, cette même organisation pourrait également considérer une perturbation dans les opérations industrielles d'une installation de production manipulant des matériaux dangereux comme une conséquence à risque élevé, même si elle n'a pas d'impact sur la production, à cause des politiques internes et/ou des réglementations externes concernant la sécurité publique.

Avant de constituer un groupe qui sera chargé d'étalonner les risques individuels, il faut clarifier les échelles de vraisemblance et de conséquence pour pouvoir donner une marche à suivre à l'équipe effectuant l'évaluation des risques.

**Tableau A.2 – Échelle de conséquence typique**

| Conséquence | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Zone de risque | | | | | | | | | Impact national |
| | Planification de continuité d'activité | | Sécurité des informations | | | Sécurité des opérations industrielles | | Sécurité de l'environnement | | |
| Catégorie | Interruption de la fabrication dans un site | Interruption de la fabrication sur plusieurs sites | Coût (millions de $ US) | Justice | Confiance publique | Personnes – sur le site | Personnes – en dehors du site | Environnement | | Infrastructure et services |
| **A (élevée)** | > 7 jours | > 1 jour | > 500 | Acte criminel | Perte d'image pour la marque | Décès | Décès ou incident grave pour la communauté | Citation par une agence régionale ou nationale ou dommages importants à long terme sur une zone étendue | | Touche un certain nombre de secteurs d'activité ou perturbe sensiblement les services de la communauté |
| **B (moyenne)** | > 2 jours | > 1 heure | > 5 | Délit | Perte de confiance de la clientèle | Arrêt de travail ou blessure grave | Plaintes ou impact sur la communauté locale | Citation par une agence locale | | Peut toucher un secteur d'activité à un niveau supérieur à celui d'une entreprise unique. Peut toucher les services d'une communauté |
| **C (basse)** | < 1 jour | < 1 heure | < 5 | Néant | Néant | Premiers secours ou blessure à consigner | Pas de plaintes | Dégagements limités et confinés, trop faibles pour nécessiter des rapports | | Peu ou pas d'impact sur les secteurs d'activité au-delà de l'entreprise individuelle. Peu ou pas d'impact sur les services de la communauté |

#### A.2.3.3.7.4 Niveau de risque

Le produit final d'une évaluation qualitative de risques consiste en une liste d'actifs ou de scénarios, avec un classement des niveaux de risque généraux. On développe habituellement cela dans un tableau similaire au Tableau A.3 présenté ci-dessous, qui définit trois niveaux de risque basés sur trois niveaux de vraisemblance et de conséquence. Chaque risque identifié lors de l'évaluation des risques se voit attribuer un niveau de risque. Ici aussi, il ne s'agit que d'un exemple, que l'organisation devra examiner plus en profondeur.

**Tableau A.3 – Tableau typique des niveaux de risque**

| | | Catégorie de conséquence | | |
|---|---|---|---|---|
| | | **A** | **B** | **C** |
| **Vraisemblance** | **Élevée** | Risque élevé | Risque élevé | Risque moyen |
| | **Moyenne** | Risque élevé | Risque moyen | Risque faible |
| | **Faible** | Risque moyen | Risque faible | Risque faible |

Les niveaux de risque (élevé, moyen et faible) correspondent chacun à une combinaison particulière de vraisemblances et de conséquences. Une organisation définit une politique de tolérance des risques relative à chaque niveau de risque, qui correspondra à un niveau particulier de réponse de la part de l'entreprise. L'approche réelle pour résoudre le risque peut consister à utiliser des contre-mesures identifiées. Il convient que les responsables de l'entreprise préparent une version initiale de ce tableau avant de lancer le processus d'analyse des risques. Il s'agit là de la méthode recommandée pour faire en sorte que la démarche d'évaluation des risques fournisse des résultats qui faciliteront la prise de décision et entraîneront la prise de mesures utiles de la part de l'organisation.

Voir A.3.4.2 pour toute autre information sur la définition d'une politique de tolérance des risques et la façon d'utiliser la politique de tolérance des risques et les résultats de l'évaluation des risques pour gérer les risques.

### A.2.3.3.8 Évaluation des risques détaillée

#### A.2.3.3.8.1 Généralités

Une analyse détaillée des risques se concentre sur les réseaux et dispositifs IACS individuels, et prend en compte une évaluation des vulnérabilités techniques détaillée de ces actifs et l'efficacité des contre-mesures existantes. Il peut ne pas être pratique pour les organisations d'effectuer l'évaluation détaillée des risques pour tous leurs actifs IACS en même temps – dans ce cas, une organisation rassemblera suffisamment d'informations à propos de ses IACS pour être à même de hiérarchiser ces systèmes, afin de déterminer ceux qui doivent être analysés en premier par la démarche d'évaluation détaillée des vulnérabilités et des risques.

L'évaluation détaillée des risques identifie les risques, puis les hiérarchise. Il convient d'identifier les risques pour chaque IACS. Une fois les risques identifiés, une organisation peut choisir de hiérarchiser tous les risques décelés sur l'ensemble de ces systèmes, de hiérarchiser les risques individuellement pour chaque système ou de hiérarchiser les risques décelés dans les sous-ensembles des IACS étudiés, par exemple tous les IACS d'un site particulier. Du fait que la hiérarchisation entraîne finalement des décisions sur les actions à entreprendre et des investissements pour renforcer la cyber-sécurité, il convient que la portée de la hiérarchisation s'aligne sur la portée du budget et l'autorité décisionnaire en place dans l'organisation pour réaliser ces investissements. Par exemple, si tous les IACS supportant une ligne de produits spécifique sont gérés et budgétés en tant que groupe, les risques encourus par l'ensemble de ces IACS seraient hiérarchisés en même temps pour appuyer le processus de décision du responsable.

#### A.2.3.3.8.2 Caractérisation des IACS clés

L'identification et la hiérarchisation des risques encourus par les IACS nécessitent que l'organisation localise et identifie les IACS clés et leurs dispositifs, ainsi que les caractéristiques des systèmes générant des risques. Faute d'un inventaire des dispositifs et réseaux des IACS, il est difficile d'évaluer et de hiérarchiser les emplacements pour lesquels des mesures de sécurité sont nécessaires et pour lesquels elles auront le plus d'impact.

L'équipe doit se réunir avec le personnel des IACS pour identifier les différents IACS qui sont utilisés sur l'ensemble du site et qui commandent les sites distants. Il convient de mettre l'accent sur les systèmes, pas simplement sur les dispositifs, ces systèmes comprenant, mais sans s'y limiter, les systèmes de commande, les systèmes de mesure et les systèmes de surveillance qui utilisent un dispositif IHM central. Inclure les zones où se déroulent des opérations industrielles, ainsi que les zones de service public telles que les centrales électriques et les installations de traitement des déchets.

Comme cela a été indiqué auparavant, l'objectif consiste à identifier les principaux dispositifs et les types de dispositifs qui sont utilisés et fonctionnent collectivement pour faire fonctionner l'équipement commandé. À ce stade du développement du programme de sécurité, il n'est pas important de développer un inventaire complet de chacun des dispositifs des IACS, car cet inventaire sera utilisé pour prendre des décisions fermes sur les risques relatifs que les dispositifs de commande font encourir aux opérations industrielles. À titre d'exemple, il est important de savoir:

- Si les instruments de terrain et les communications entre l'émetteur de terrain et les contrôleurs sont analogiques ou numériques.
- Si les dispositifs/systèmes sont connectés les uns aux autres, et les types de réseaux utilisés.
- Si les dispositifs sont situés dans une zone sécurisée telle qu'un bâtiment ou une installation clôturée, ou si les dispositifs sont situés à distance.
- Si les dispositifs de commande sont soumis à un contrôle réglementaire.
- Si la perte ou le dysfonctionnement du dispositif/système a un impact significatif sur l'équipement commandé, aussi bien en termes d'activité ou financiers qu'en termes HSE.

Il convient que l'identification résultante des dispositifs/systèmes démontre l'étendue de l'impact que subirait l'équipement commandé au cas où les dispositifs ne parviendraient plus à commander les opérations industrielles pour lesquelles on les utilise, et leur vulnérabilité relative en matière de sécurité (du fait de facteurs physiques, de facteurs liés au réseau ou autres). Ce type d'information peut permettre de comprendre les risques relatifs qu'encourent les opérations industrielles. A ce stade il n'est pas nécessaire d'effectuer un inventaire complet pour identifier les quantités exactes de chaque sorte de dispositif.

#### A.2.3.3.8.3 Grouper les dispositifs et les systèmes et faire un inventaire

Au fur et à mesure que l'équipe identifie les dispositifs/systèmes individuels, il peut être utile de placer les éléments dans un groupement logique des équipements. Dans les installations IACS modernes, cette collection d'équipements fonctionne comme un système intégré servant à commander les différentes activités des opérations industrielles. Le nombre de systèmes de commande logique varie énormément d'une entreprise à l'autre. Dans une entreprise moyenne ou grande, il peut y avoir plusieurs centaines d'IACS logiques composés de milliers de dispositifs individuels et de systèmes de bas niveau.

Les entreprises moyennes et grandes gérant les problèmes de cyber-sécurité à l'échelon global de l'entreprise peuvent avoir tout intérêt à enregistrer la liste des systèmes logiques dans une base de données interrogeable. Les DCS peuvent être organisés par ligne, unité, cellule ou véhicule au sein d'un site géographique local ou distant. Les systèmes SCADA peuvent être organisés par centre de commande, site distant et équipement de commande associé. La base de données sera plus utile si les données sont rassemblées dans un format

normalisé, qui facilitera la comparaison des différents systèmes entre eux. La Figure A.4 est un exemple de format normalisé, qui peut être facile à créer sous forme de tableur ou de base de données. Elle a pour objet d'inciter à réfléchir au type d'information qui pourra être utilisé par la suite dans les activités de hiérarchisation des systèmes et d'évaluation des risques détaillée.

**Industrial automation and control system network characterization**

Business _____
Site _____
Operating unit _____
Site IT contact _____ Phone # _____
Site process control contact _____ Phone # _____
Last updated _____

**PLEASE ANSWER THE FOLLOWING QUESTIONS :**

_____ **Are manufacturing and control systems currently interfaced to site or corporate LANs?**
_____ **Are manufacturing and control systems remotely accessed from outside the IACS domain?**

Process control domain

_____ Total number of IP addressable nodes
_____ Number of IP addressable nodes to be accessed from outside process control domain
_____ Number of concurrent users inside IACS domain
_____ Number of concurrent users inside IACS domain requiring access to external resources
_____ Number of total users outside IACS domain requiring access to process control resources
_____ Number of concurrent users outside IACS domain requiring access to process control resources
IP addressing (check all that apply)
_____ DHCP _____ Public addresses used (i.e. x.x.x.x)
_____ Static _____ Private addresses used (192.168.x.x)

Control platforms

_____ Number of control platforms
_____ Control platform type (PLC, DCS, PC)
Control platform vendor(s) _____ _____
Control platform model(s) _____ _____

Operator consoles and HMI devices

_____ Number of operator consoles
Operator console vendor(s) _____ _____
Operator console model(s) _____ _____
Operator console operating system(s) _____ _____

Application nodes (check all that apply)

_____ Proccess management and control server
_____ SCADA
_____ OPC server
_____ Engineering workstation
_____ Batch server
_____ Other _____

Network security barriers in-use
Type (firewalls, routers, VLANS, etc.) _____

Anticipated network security support (check all that apply)

_____ Site resources
_____ External (3rd party)

Site network (answer yes / no)

_____ Current site network topology diagrams available and up-to-date?
_____ Are process control nodes on isolated LAN segment?
_____ Site information security policy in place?
_____ Security office audit completed (if yes, date completed _____ )
_____ Does site use two-factor authentication?
_____ Security office risk assessment completed (if yes, date completed _____ )

Remote access requirements (check all that apply)

_____ Via site / corporate LAN
_____ Via dial-up modem
_____ Via internet
_____ Via local dial-up modem directly tied to manufacturing and control node(s)

Local egress requirements (check all that apply)

_____ To site applications and resources (document management systems, quality systems, business systems)
_____ To corporate applications and resources (document management systems, quality systems, business systems)
_____ To internet sites

**Figure A.4 – Exemple de feuille de collecte de données concernant les IACS logiques**

Il convient d'être attentif lors de l'identification des dispositifs/systèmes de commande des automatismes industriels et de diriger son attention au-delà des dispositifs qui exécutent les commandes directes. Le système ou le réseau peut ne pas se limiter aux automates ou aux

DCS. Dans une installation de fabrication ou de production intégrée, le réseau des IACS est composé de dispositifs qui sont utilisés directement pour fabriquer, inspecter, gérer et expédier des produits et peut comprendre, entre autres, les composants suivants:

- des DCS et les dispositifs associés;
- des systèmes SCADA et les dispositifs associés;
- des automates programmables et les dispositifs associés;
- des stations IHM;
- des SIS et les dispositifs associés;
- des ordinateurs d'atelier (à usage spécial);
- des systèmes de gestion des informations procédé (PIM) et des systèmes d'exécution de fabrication (MES);
- des systèmes de modélisation des commandes des automatismes industriels;
- des systèmes experts;
- des systèmes d'inspection;
- des systèmes de manipulation et de suivi de matériaux;
- des analyseurs;
- des systèmes de jaugeage;
- des systèmes de traitement de lots;
- des systèmes de surveillance et/ou de gestion d'alimentation électrique;
- des systèmes de télémétrie distante;
- les systèmes de communication utilisés pour la communication avec les dispositifs distants;
- des systèmes de condition de fonctionnement normalisé (SOC) et de procédure de fonctionnement normalisé (SOP);
- des systèmes de gestion de documents;
- des ordinateurs de développement de programmes;
- des systèmes de commande HVAC;
- des passerelles de communication de réseau (c'est-à-dire des commutateurs, des concentrateurs et des routeurs);
- des dispositifs de protection de réseau (c'est-à-dire des pare-feu et des systèmes de détection d'intrusion).

Ne pas oublier d'inclure tous les dispositifs en réseau dotés d'unités centrales de traitement, critiques pour le maintien de la production. L'objet de cette étape, l'inventaire, est de déceler les dispositifs qui sont vulnérables aux attaques véhiculées par les réseaux, afin qu'ils puissent être inclus dans l'évaluation des risques détaillée.

NOTE Ce n'est pas à ce stade que l'on décide des dispositifs qu'il convient d'isoler ou de séparer du réseau local (LAN). Dans le doute, il vaut mieux inclure trop de dispositifs que pas assez. Une fois que l'équipe chargée de l'évaluation a effectué l'évaluation des risques et mieux compris l'ensemble des vulnérabilités, il convient qu'elle détermine si des solutions d'atténuation des risques sont réellement nécessaires et à quel endroit il convient d'installer les différents dispositifs.

Il existe dans le commerce différents outils qui permettent de réaliser des inventaires pour des entreprises qui fonctionnent en réseau, pour identifier et documenter l'ensemble des matériels, systèmes et logiciels présents sur le réseau. Avant d'utiliser ce type d'application, on doit prendre soin d'identifier les IACS. Avant d'utiliser l'un de ces produits, effectuer une évaluation de son fonctionnement et de l'impact qu'il peut avoir sur les équipements de commande connectés.

L'évaluation de l'outil peut consister à le soumettre à essai dans des environnements de systèmes de commande similaires, mais situés hors ligne et non utilisés dans la production, pour s'assurer qu'il n'a pas d'effet négatif sur le fonctionnement du système de commande et n'est pas susceptible d'interrompre la production. Les dispositifs non utilisés dans la production peuvent ne pas avoir d'impact sur les systèmes de production, mais ils peuvent envoyer des informations susceptibles de provoquer (cela s'est déjà produit) des pannes ou des dysfonctionnements dans les systèmes de commande. L'impact peut être dû à la nature des informations et/ou au trafic ou à la charge subi(e) par les systèmes. Si cet impact peut être acceptable dans les systèmes IT, il ne l'est pas dans les IACS.

#### A.2.3.3.8.4 Développement de schémas simples du réseau

Un schéma simple du réseau facilitera le regroupement des différents dispositifs et systèmes d'automatisation et de commande industrielle en un système de commande logique identifiable. Il convient que le schéma englobe les dispositifs identifiés au moyen de la feuille de collecte de données concernant les IACS logiques, décrite en A.2.3.3.8.2. Il convient que le schéma tente de capturer l'architecture réseau logique de base, comme par exemple les approches relatives à la connectivité, ainsi que certains éléments de base de l'architecture réseau physique, comme l'emplacement des dispositifs.

Avant d'effectuer la hiérarchisation des IACS ou une évaluation des risques détaillée, il est important que l'équipe ait une compréhension claire de l'étendue et des frontières du système à évaluer. Le schéma du réseau est un outil qui permet de mieux visualiser le réseau et qui facilite l'exécution de l'évaluation des risques. Il peut s'agir d'un schéma de principe très simple représentant les dispositifs, les systèmes et les connexions des interfaces, ou d'un schéma plus détaillé comme celui représenté sur la Figure A.5. Les deux approches permettent d'atteindre les objectifs plus facilement. Si des zones et des conduits ont été établis, il convient de décrire ces éléments au moyen de schémas simples du réseau. (Davantage d'explications sur le développement des zones et des conduits peuvent être trouvées en A.3.3.4.).

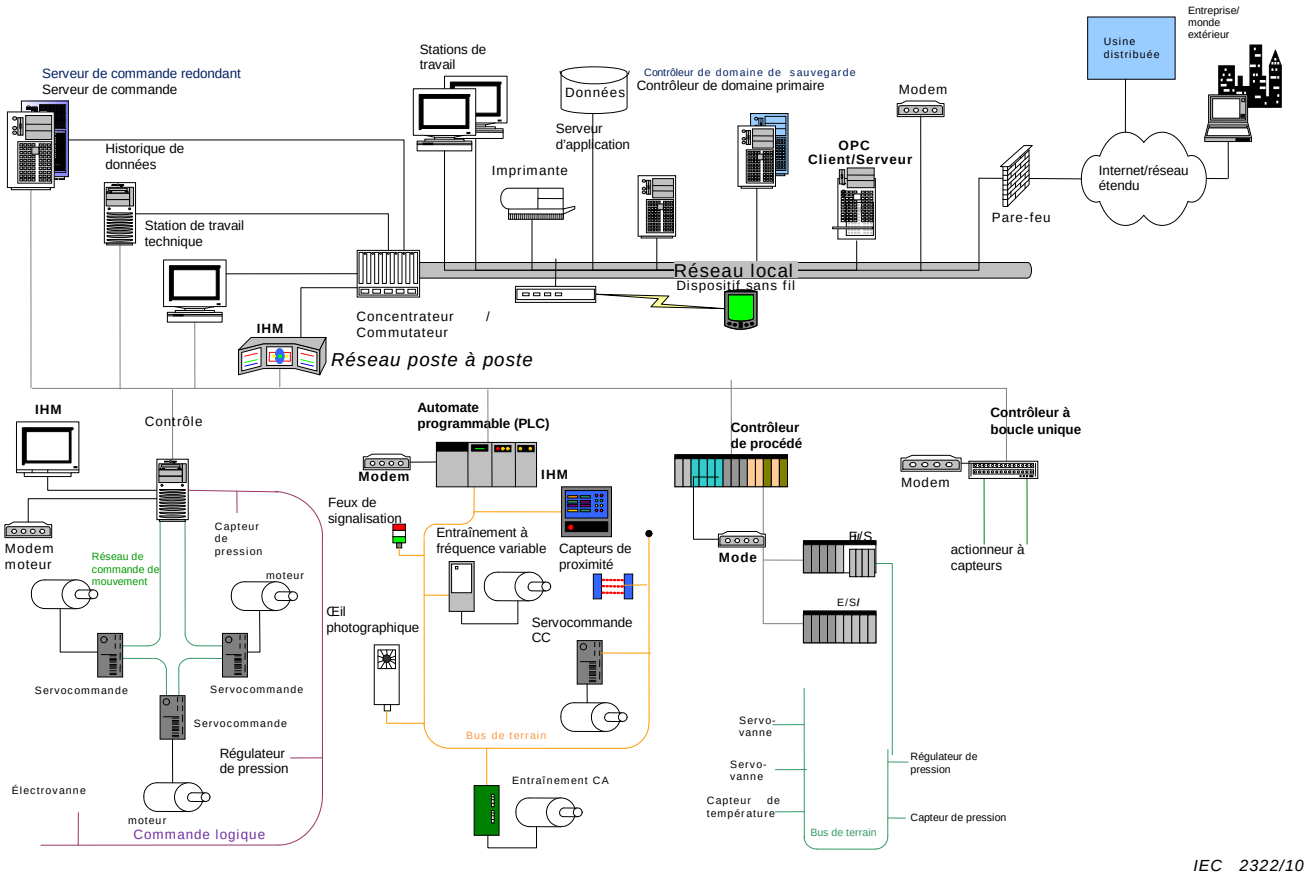



**Figure A.5 – Exemple de schéma graphique élaboré d'un réseau logique**

Les schémas simples du réseau sont un point de départ et représentent une vue correspondant à un instant donné dans le temps. L'expérience des évaluations de vulnérabilités détaillées montre que pratiquement toutes les évaluations font apparaître des connexions qui n'avaient pas été identifiées dans le processus de réalisation du schéma initial. Il convient donc que ces schémas ne constituent pas la seule base pour évaluer la connectivité, sans qu'il n'y ait davantage de validation physique détaillée. Ils sont très utiles pour mesurer l'étendue de l'effort d'évaluation des risques et définir les zones et les conduits comme décrit dans la CEI/TS 62443-1-1.

#### A.2.3.3.8.5 Évaluation préalable de l'ensemble des risques encourus par chaque système identifié

Une fois que la liste des dispositifs, actifs et réseaux IACS a été constituée, il est nécessaire d'effectuer une évaluation préalable du niveau de risque relatif associé aux systèmes, afin qu'ils puissent être hiérarchisés pour l'évaluation des risques détaillée. Si l'évaluation des risques détaillée doit être effectuée sur tous les IACS ou si l'évaluation des risques de haut niveau a fourni suffisamment d'informations pour permettre de hiérarchiser les IACS individuels par risque, cette étape n'est pas nécessaire.

Chaque système individuel doit être évalué pour permettre de comprendre les conséquences financières et HSE identifiées dans l'évaluation des risques de haut niveau au cas où il aurait été porté atteinte à la disponibilité, l'intégrité ou la confidentialité du système. Il est également nécessaire d'affecter une mesure d'échelle à cette évaluation.

Le personnel connaissant les IACS doit évaluer la sélection. Normalement, le personnel des IACS et l'informaticien apporte ses connaissances sur les dispositifs et les systèmes utilisés, tandis que le personnel chargé des opérations apporte les éclaircissements nécessaires sur

les conséquences d'un incident de sécurité. Cette équipe d'évaluation doit travailler en harmonie pour évaluer la sélection.

L'équipe développe une échelle de haut niveau pour estimer quantitativement le risque global associé à chaque système. L'échelle peut être aussi simple qu'une échelle à trois niveaux (élevé, moyen, faible) ou une échelle de 1 à 10, et elle doit établir les critères de chacun des niveaux de l'échelle des risques.

L'équipe doit prendre une décision ferme quant au niveau de risque associé à chaque système en examinant les conséquences financières et HSE au cas où il serait porté atteinte à la disponibilité, l'intégrité ou la confidentialité du système. Il convient que l'équipe enregistre l'évaluation des risques de haut niveau du système logique dans la liste d'inventaire développée précédemment. L'établissement de niveaux de tolérance des risques facilite la hiérarchisation des actifs réels de l'environnement IACS.

Les résultats de cette évaluation préalable constitueront une entrée importante pour la décision d'effectuer une évaluation des vulnérabilités détaillée pour un IACS particulier. Une évaluation des vulnérabilités complète doit être effectuée:

- Si l'on constate que l'IACS est actuellement connecté au réseau de l'entreprise ou à des réseaux extérieurs (par exemple l'Internet ou des modems). Une évaluation des risques détaillée permettra de mieux comprendre les vulnérabilités et la stratégie appropriée pour la réduction des risques.
- Si l'on constate que le système est actuellement supporté à distance.
- Il est attendu que l'un des deux critères ci-dessus soit vérifié dans un proche avenir. Dans ce cas, il convient que l'évaluation des vulnérabilités soit effectuée avant les étapes conduisant à cette position de risque élevé.

#### A.2.3.3.8.6 Hiérarchisation des systèmes

Le paragraphe précédent suggérait d'affecter un niveau vulnérabilité/risque à chacun des IACS logiques identifiés. Cette échelle d'estimation est un bon point de départ pour le processus de hiérarchisation. Il existe cependant plusieurs éléments supplémentaires à prendre en compte au moment de déterminer sur quoi l'on doit se concentrer en premier dans la démarche d'évaluation des risques détaillée, comme par exemple:

- les risques encourus par l'entreprise (par exemple HSE ou financiers);
- les endroits où le processus d'évaluation a le plus de chance d'être efficace;
- le coût des contre-mesures potentielles nécessaires;
- les coûts financiers et les coûts encourus autres que financier;
- le personnel de support compétent et disponible pour le système particulier;
- la région géographique;
- les directives ou les sensibilités du syndicat professionnel membre;
- les contraintes politiques nationales ou locales;
- le personnel de support externe ou appartenant à l'entreprise;
- le support sur site pour réaliser l'effort;
- l'historique des problèmes de cyber-sécurité connus.

Il n'y a pas de bonne ou de mauvaise approche. Les valeurs sont différentes d'une entreprise à l'autre. L'important, c'est d'utiliser les mêmes principes pour la hiérarchisation, d'un site à l'autre. Enregistrer les décisions concernant la hiérarchisation et la base sur laquelle elles reposent.

#### A.2.3.3.8.7 Identification des vulnérabilités et hiérarchisation des risques

L'étape suivante du processus d'évaluation des risques consiste maintenant à effectuer l'évaluation des risques détaillée sur les systèmes hiérarchisés. La plupart des méthodologies utilisent une approche consistant à diviser le système en éléments plus petits et à examiner les risques associés à ces plus petits éléments, qui constituent le système global.

Il convient que l'évaluation des risques détaillée traite les menaces portant atteinte à la sécurité physique ou à la cyber-sécurité, les menaces internes et externes, et considère le matériel, les logiciels et les informations comme sources de vulnérabilités.

Il est impératif que ce soit une équipe de personnes qui effectue cette évaluation, l'objectif étant de donner à celle-ci une perspective aussi étendue que possible. Il convient que l'équipe soit composée au minimum d'une personne responsable des opérations du site, d'une personne des IACS du site, d'un informaticien du site et d'un responsable des réseaux du site. Les autres personnes que l'on peut envisager d'inclure sont les experts de la sécurité physique, de la sécurité des systèmes d'informations, les experts juridiques, les experts de l'activité (opérations, maintenance, développement technique, etc.), les spécialistes des ressources humaines, les experts des questions HSE et les revendeurs de matériel. Ces personnes sont parfaitement placées pour reconnaître les vulnérabilités et les conséquences des risques dans leurs propres zones.

Si le but est de comprendre les menaces et les conséquences associées à un système particulier, il est tout à fait vrai qu'un objectif essentiel est de parvenir à comparer les résultats de l'évaluation d'un système/site à ceux d'un autre système/site de l'organisation. Pouvoir le faire dépend du degré d'uniformité avec lequel la méthodologie est appliquée. Voici quelques approches qui ont fait leur preuve:

- utiliser une personne clé pour diriger le processus d'évaluation sur chaque site;
- utiliser une petite équipe de personnes qui dirigera les évaluations pour un emplacement géographique, une unité d'activité, etc., ces personnes ayant déjà travaillé ensemble dans d'autres évaluations;
- utiliser de bons documents de formation, comprenant des procédures et des exercices qui mettront à niveau les équipes d'individus chargées des évaluations sur les différents sites;
- utiliser un formulaire commun ou une base de données commune pour enregistrer les résultats des évaluations;
- examiner d'une manière centralisée tous les résultats des évaluations pour vérifier s'ils sont réalistes et s'ils peuvent être comparés à ceux obtenus sur des systèmes similaires.

En effectuant l'évaluation, tenir compte de tous les aspects des IACS, notamment les modifications imprévues sur la configuration du système, effectuées pour la maintenance, les fournisseurs qui se connectent temporairement au système pour le support, et même les modifications de conception mineures d'un fournisseur, qui pourraient introduire de nouvelles vulnérabilités par le biais de pièces détachées ou lors des mises à niveau, et qu'il convient de prendre en compte et/ou de soumettre à essai de la même manière que les composants du système original.

L'évaluation doit porter sur les systèmes comportant une interface avec les IACS et vérifier qu'ils ne portent pas atteinte à la sécurité des IACS, et vice versa. Exemples: systèmes de développement comportant des fonctions de développement en ligne et systèmes environnementaux et d'alimentation dont le dysfonctionnement entraînerait des risques inacceptables.

Dans certains cas, la vulnérabilité peut être imputable au revendeur. Il peut être nécessaire de soumettre l'assurance qualité et le contrôle de conception du revendeur à une évaluation

des vulnérabilités. Cette étape est particulièrement importante lorsque l'on commande des pièces détachées ou lors des mises à niveau.

À ce stade du processus d'évaluation, il convient d'effectuer un examen détaillé du réseau d'un point de vue physique et opérationnel pour détecter toutes les connexions qui n'apparaissent pas dans les schémas simples initiaux du réseau. De nombreuses évaluations permettront de détecter ces connexions.

Les sources potentielles de vulnérabilités suivantes, relatives à la connectivité des réseaux, ont été identifiées auparavant comme des faiblesses dans certains systèmes, qu'il convient d'identifier et d'examiner:

- les points d'accès sans fil, en particulier les technologies médiocrement sécurisées telles que les anciennes versions de l'IEEE 802.11;
- les connexions par modems, en particulier celles qui ne comportent de procédure de rappel et sont dépourvues de chiffrement;
- les programmes d'accès distant (par exemple, pcAnywhere®[3] et Timbuktu®), généralement utilisés par les experts à l'intérieur ou à l'extérieur de l'entité pour le support des systèmes ou des opérations. Ces applications peuvent donner toute latitude à des individus non autorisés pour accéder aux commandes et aux configurations;
- les technologies d'affichage de fenêtres à distance telles que X Windows®;
- les connexions intranet;
- les connexions Internet;
- les réseaux de télémétrie;
- toute connexion de réseau à des systèmes qui ne font pas directement partie des IACS;
- toute connexion de réseau utilisée pour connecter des pièces du système SCADA ou du système de commande, qui ne font pas partie d'un réseau IACS dédié et physiquement sécurisé. Autrement dit, tout réseau déployé au-delà de la frontière d'une zone de sécurité particulière ou traversant des zones non sécurisées, ou utilisé à la fois pour les IACS et pour d'autres fonctions. Les équipements inclus dans les connexions de réseau comprennent la télémétrie radio et les services externalisés tels que le relais de trames utilisé pour la communication entre zones géographiquement séparées.

Un certain nombre de ressources de l'industrie traitent de la sécurité des systèmes de commande et fournissent une liste de vulnérabilités courantes à rechercher au cours d'une évaluation des vulnérabilités détaillée (voir [27] et [29]).

Le résultat final produit par l'équipe est une liste de vulnérabilités hiérarchisées en fonction de leur impact sur les risques. Une fois que les vulnérabilités ont été identifiées, l'équipe associe ensuite ces vulnérabilités aux menaces, aux conséquences et aux vraisemblances de réalisation de ces menaces et d'exercice de ces vulnérabilités. Cette analyse prend en compte l'atténuation potentielle due aux mesures de sécurité physiques. Les vulnérabilités qui contribuent aux risques de plus haut niveau sont normalement celles sur lesquelles il est le plus facile de se mettre d'accord. Pour terminer le processus d'évaluation des vulnérabilités, il convient que la méthodologie de l'équipe comprenne une méthode convenue permettant de déterminer comment hiérarchiser les vulnérabilités qui contribuent à un grand nombre de risques de niveau moyen et de bas niveau.

---

[3] pcAnywhere®, Timbuktu® et X Windows® sont des exemples de produits adaptés disponibles dans le commerce. Ces informations sont données pour la commodité des utilisateurs de la présente norme et ne constituent en aucune façon une recommandation par l'ISA.

Les résultats des évaluations de risques détaillées doivent être documentés, et les actions effectuées selon les recommandations issues de ces résultats (voir A.3.4.2).

La documentation des vulnérabilités décelées au cours de l'évaluation des risques détaillée comprend, pour chaque vulnérabilité décelée, la date de l'évaluation, l'identification des actifs concernés, la description de la vulnérabilité, le nom de la personne qui a observé la vulnérabilité et tous les outils ou méthodes qu'elle a utilisés pour le faire. En plus des vulnérabilités décelées, il convient que la documentation de l'évaluation des risques détaillée indique les vulnérabilités qui ont été recherchées mais non décelées, et de quelle façon cette recherche a été effectuée pour chaque actif évalué. Cela peut prendre la forme d'une simple check-list. La documentation des vulnérabilités s'avère extrêmement utile lors de toute mise à jour de l'évaluation des risques ou lorsque des questions particulières se posent au sujet des actifs. Les check-lists et résultats antérieurs des évaluations de vulnérabilités forment une base de départ permettant d'améliorer les évaluations de vulnérabilités futures et une base pour parvenir à une certaine uniformité dans l'organisation. Il convient que l'organisation les considère avec ce point de vue et évite de les considérer comme une définition statique du contenu de ce type d'évaluation.

Les tâches et la documentation liées aux processus d'évaluation des risques de haut niveau et détaillée, décrits dans ce paragraphe, et le processus de gestion des risques de A.3.4.2 peuvent être intégrés pour répondre plus efficacement aux besoins d'une organisation particulière.

Il convient de mettre à jour et de revalider périodiquement les résultats des évaluations de risques détaillées. En outre, étant donné qu'une évaluation des risques détaillée peut devenir obsolète du fait des évolutions de l'environnement du système de commande, il convient d'incorporer dans le programme de gestion des changements le déclenchement de démarches de mise à jour des évaluations de risques. Il s'agit là d'un point essentiel, car la plupart des organisations trouvent qu'il est plus facile d'établir une base de départ pour la cyber-sécurité que de la faire évoluer dans le temps (voir A.4.3).

#### A.2.3.3.8.8 Pièges à éviter

Au cours de l'évaluation, il convient d'effectuer les actions suivantes, afin d'éviter les pièges courants qui peuvent faire dérailler le processus d'évaluation:

a) Concevoir la solution au cours de l'évaluation

   L'évaluation a pour objet d'indiquer quels risques existent, pas de demander à l'équipe de concevoir la solution. On peut gaspiller beaucoup de temps à essayer de résoudre le problème et à débattre des différentes approches possibles quand on évalue un actif particulier. Il convient de mettre l'accent sur la compréhension des risques et des conséquences qui existent effectivement ou qui pourraient exister dans un futur prévisible, comme dans le cas d'un projet en cours de réalisation consistant à ajouter un nouveau modèle de dispositif au moyen d'une interface de réseau.

b) Minimiser ou exagérer la conséquence

   Il convient d'apporter une évaluation honnête de la conséquence d'un incident touchant un matériel ou un logiciel particulier ou une information particulière. Il convient de ne pas minimiser les conséquences pour éviter d'entreprendre les actions d'atténuation des risques de sécurité appropriées qui permettent de réduire les risques. Ce qui peut revêtir une grande importance pour un individu parce que cela affecte directement son travail peut avoir un niveau de conséquence très différent pour l'organisation dans son ensemble.

c) Ne pas parvenir à un consensus sur les résultats de l'évaluation des risques

   Il est très important de parvenir à un accord sur les risques et les conséquences. Il est bien plus difficile de parvenir à un accord sur les contre-mesures si l'équipe n'a pas une compréhension commune du risque et un accord sur son importance.

d) Évaluer le système sans tenir compte des résultats d'évaluations de systèmes similaires

Il est important de vérifier que les résultats sont appropriés et sont en accord avec les résultats des processus d'évaluation similaires menés sur d'autres sites. Les conclusions tirées d'évaluations antérieures de systèmes similaires et les vulnérabilités identifiées peuvent être très bénéfiques pour l'évaluation du système dont on s'occupe.

#### A.2.3.3.8.9 Interrelations avec les mesures de sécurité physique

La cyber-sécurité et la sécurité physique peuvent être étroitement liées. Dans certaines situations, elles peuvent fonctionner comme des niveaux de protection indépendants, tandis que dans d'autres elles dépendent étroitement l'une de l'autre. Perdre l'une peut entraîner la perte des deux niveaux de protection. Au cours de l'évaluation détaillée d'un système, il convient de garder à l'esprit leur interaction et la façon dont elle peut affecter les conséquences.

Dans certaines industries, il est de pratique courante d'avoir un SIS en plus de l'IACS. Si le SIS est à base de relais, la vraisemblance qu'il soit affecté par un cyber-événement affectant l'IACS est faible. On peut compter sur le SIS pour remplir sa fonction de sécurité, et la conséquence d'un cyber-événement peut être contenue et réduite. Cependant, si le SIS est à base de circuits électroniques et est relié au même réseau que l'IACS (certaines industries proscrivent cette pratique), la vraisemblance d'un cyber-incident affectant les deux systèmes est bien plus élevée et les conséquences pourraient être plus importantes.

Un autre exemple pourrait être celui d'un système d'accès par badge à une salle de commande verrouillée. Dans une situation normale, le système de contrôle d'accès offre une sécurité supplémentaire aux systèmes de commande. Cependant, dans le cas d'une surcharge à refus de service (DoS) du réseau, le système de contrôle d'accès de la porte peut ne pas fonctionner et empêcher l'opérateur d'accéder à la console de l'opérateur de la salle de commande. La même surcharge de réseau DoS pourrait affecter également la console de l'opérateur. Dans cette situation, ce cyber-incident unique empêche doublement de répondre au dispositif de commande et pourrait augmenter la conséquence de l'incident.

En définitive, il convient que les méthodologies d'évaluation des risques de cyber-sécurité soient incorporées dans les méthodologies d'évaluation des risques physiques et des risques du site.

#### A.2.3.3.8.10 Évaluation des risques et cycle de vie des IACS

Les paragraphes précédents décrivent comment le processus d'évaluation des risques peut être effectué sur les IACS existants, au moment où l'on commence à établir un CSMS, puis appliqué périodiquement par la suite. L'évaluation des risques a une efficacité maximale et n'entraîne que des perturbations minimes quand on l'applique de manière similaire lors des différentes étapes du cycle de vie de l'IACS, *avant* que celui-ci ne fonctionne en mode production:

a) Durant le développement d'un nouvel IACS ou d'un IACS mis à jour

   Il convient de considérer à l'avance les cyber-risques avant de mettre en œuvre un nouvel IACS ou un IACS modifié, car l'expérience montre qu'il est toujours plus facile et plus économique de se pencher sur la sécurité lors de la phase de conception que de l'ajouter par la suite. Le processus d'évaluation des risques de haut niveau se déroule de la même façon pour un système futur que ce qui a été décrit ci-dessus pour un système existant. L'idéal est d'effectuer l'évaluation parallèlement à la conception de haut niveau et d'examiner simultanément les résultats de la conception envisagée et de l'évaluation des risques. On peut également effectuer une évaluation des risques détaillée parallèlement à la conception détaillée, bien que les vulnérabilités identifiées soient hypothétiques et ne soient pas dans tous les cas aussi spécifiques que dans un système déjà mis en œuvre. Ainsi, l'évaluation des risques menée au cours du développement peut entraîner des décisions concernant les contre-mesures qu'il convient de mettre en place et les améliorations que l'on souhaite apporter aux IACS, dans le but de réduire au maximum les surprises qui suivent la mise en œuvre.

b) Durant la mise en œuvre d'un nouvel IACS ou d'un IACS mis à jour

Même quand on fait attention aux risques lors de la phase de développement, les détails de la mise en œuvre peuvent introduire des vulnérabilités inattendues. Dans le meilleur des cas, le processus d'acceptation d'un nouvel IACS ou d'un IACS mis à jour comprend non seulement des essais, mais aussi une analyse des vulnérabilités détaillée, effectuée de la façon décrite précédemment. Ainsi, par exemple, une organisation peut avoir à déterminer si elle peut ou non mettre en route un nouveau système ou un système mis à jour avant que le correctif d'une vulnérabilité décelée récemment ne soit disponible pour le système d'exploitation sous-jacent.

c) Durant la mise hors service d'un IACS

La décision de mettre hors service ou de conserver un IACS ou les composants d'un IACS dépend de nombreux facteurs tels que le coût, le souhait de disposer de nouvelles fonctionnalités ou de nouvelles capacités, et le fait que le revendeur continue ou non d'assurer un support de qualité. L'impact sur la cyber-sécurité est également un facteur à évaluer au cours de cette prise de décision. Les nouveaux composants et les nouvelles architectures peuvent améliorer la fonctionnalité de sécurité et/ou introduire de nouvelles vulnérabilités qui devront être prises en compte. Une évaluation des cyber-risques au cours de laquelle on analyse une décision de mise hors service examine donc à la fois le scénario du remplacement de l'ancien système et le scénario du maintien de l'ancien système pendant un certain temps.

Lors de la mise hors service d'un IACS, on met à jour les évaluations des risques de haut niveau et détaillées pour deux raisons: 1) le retrait de l'IACS peut avoir une incidence sur la vulnérabilité de certains IACS qui sont restés en place et 2) si l'IACS est remplacé par un nouveau système, de nouvelles vulnérabilités peuvent faire leur apparition, comme cela a été évoqué précédemment. Par exemple, la connectivité réseau d'un IACS qu'on laisse en place peut avoir été toujours effectuée par l'intermédiaire de l'IACS que l'on retire. Cela signifie que l'on met en place une nouvelle conception de connectivité pour l'IACS qui reste, et qu'il convient d'évaluer les vulnérabilités et les risques associés à cette configuration.

#### A.2.3.4 Pratiques en support

##### A.2.3.4.1 Pratiques de base

Les pratiques de base sont les dix actions suivantes:

a) Établir les critères permettant d'identifier quels dispositifs composent les IACS.

b) Identifier les dispositifs qui supportent les procédés d'activité et opérations IACS critiques, y compris les systèmes informatiques qui supportent ces procédés de l'activité et les opérations IACS.

c) Classifier les actifs et composants logiques selon leur disponibilité, leur intégrité et leur confidentialité, ainsi que leur impact HSE.

d) Hiérarchiser les activités d'évaluation des risques selon les conséquences (par exemple, les opérations industrielles présentant des dangers élevés et connus sont traitées avec une priorité élevée).

e) Déterminer l'étendue des frontières du système que l'on évalue, en identifiant tous les actifs et composants critiques.

f) Développer un schéma de réseau des IACS (voir A.2.3.3.8.4).

g) Comprendre que les risques, la tolérance des risques et l'acceptabilité des contre-mesures peut varier selon la région géographique ou l'entreprise.

h) Maintenir un enregistrement à jour de tous les dispositifs entrant dans la composition des IACS, en vue des évaluations futures.

i) Effectuer une évaluation des risques à chacune des étapes du cycle de vie de la technologie (développement, mise en œuvre, mise à jour et mise hors service).

j) Identifier la fréquence des réévaluations ou des critères de déclenchement basés sur les évolutions de la technologie, de l'organisation ou des opérations industrielles.

#### A.2.3.4.2 Pratiques additionnelles

Les quatre actions suivantes sont les pratiques additionnelles:

a) Identifier et classifier les actifs pour faciliter la définition des risques encourus par l'entreprise. Il convient que les facteurs sur lesquels il est important de mettre l'accent soient les personnes impliquées et les technologies utilisées. La création d'une check-list facilite le regroupement des actifs en différentes catégories (voir A.2.3.3.8.3).

b) Classifier les actifs individuels en fonction des implications pour la sécurité que représentent la disponibilité, l'intégrité et la confidentialité. Un actif peut avoir différents niveaux de classification pour chacune de ces catégories.

EXEMPLE Classification d'un type spécifique de données:

- Disponibilité: faible – le système ne nécessite pas de fonctionnement continu. Le système n'est pas intégré à un procédé dangereux. Un délai d'un ou deux jours reste acceptable.
- Intégrité: moyenne – les données sont vérifiées à différents stades et toute modification qu'elles peuvent subir est détectée.
- Confidentialité: très élevée – il convient que les données critiques de l'activité soient maintenues au niveau de confidentialité le plus élevé.

c) Établir la vraisemblance (c'est-à-dire la probabilité ou la fréquence estimée) qu'une menace particulière réussira à s'exécuter, d'après le niveau actuel des contrôles. Il est important de regarder s'il existe d'autres sortes de contrôles, qui peuvent être habituellement en place dans les processus de fabrication ou les opérations, et qui compléteraient les contrôles de cyber-sécurité pour réduire la vraisemblance de l'apparition de la conséquence. Ceux-ci comprennent des SIS indépendants et d'autres techniques PSM telles que des dispositifs de sauvegarde passifs, auxiliaires et indépendants. La fréquence estimée est liée directement à la vulnérabilité globale et aux menaces; elle peut être exprimée quantitativement sous forme de pourcentage ou, plus subjectivement, sous l'une des formes suivantes: élevée, moyenne, faible.

d) Définir, d'après l'évaluation des risques encourus par les IACS ou l'activité, les conséquences ou l'impact d'une tentative d'exécution de menace réussie.

#### A.2.3.5 Ressources utilisées

Cet élément repose en partie sur des informations provenant des références suivantes, répertoriées dans la Bibliographie:[24], [26], [27], [28], [29], [30], [33], [42].

## A.3 Catégorie: Traitement des risques avec le CSMS

### A.3.1 Description de la catégorie

La deuxième catégorie principale du CSMS est le traitement des risques avec le CSMS. Cette catégorie englobe l'ensemble des exigences et des informations contenues dans le CSMS. Elle comprend trois groupes d'éléments:

- Politique, organisation et sensibilisation concernant la sécurité,
- Contre-mesures de sécurité sélectionnées, et
- Mise en œuvre.

### A.3.2 Groupe d'éléments: Politique, organisation et sensibilisation à la sécurité

#### A.3.2.1 Description du groupe d'éléments

Le premier groupe d'éléments de cette catégorie traite du développement des politiques de cyber-sécurité élémentaires, des organisations responsables de la cyber-sécurité et de la sensibilisation, au sein de l'organisation, aux problèmes liés à la cyber-sécurité. La Figure A.6 est une représentation graphique des cinq éléments contenus dans le groupe d'éléments:

- Domaine d'application du CSMS,

- Actions d'organisation pour la sécurité,
- Formation du personnel et sensibilisation à la sécurité,
- Plan de continuité d'activité, et
- Politiques et procédures de sécurité.

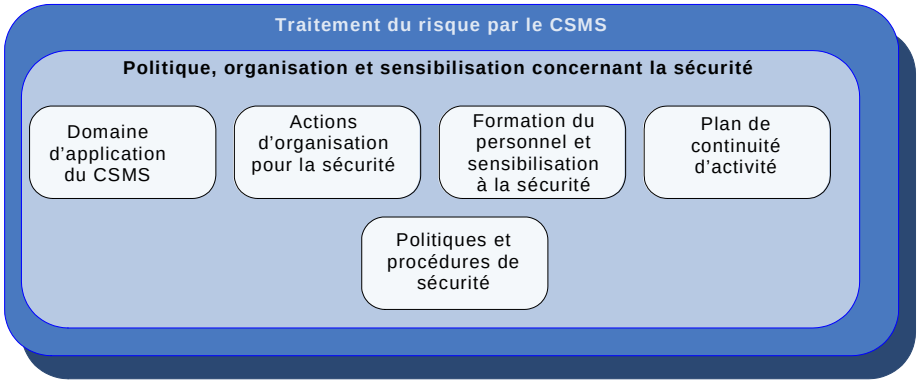



**Figure A.6 – Vue graphique du groupe d'éléments: Politique, organisation et sensibilisation concernant la sécurité**

### A.3.2.2 Élément: domaine d'application du CSMS

#### A.3.2.2.1 Description de l'élément

Une fois que la justification économique est établie et que l'appui de la direction supérieure est obtenu, l'étape suivante consiste à développer un domaine d'application formel ou une charte. Il convient que ce domaine d'application explique ce qui doit être réalisé (en termes d'activité) et quand cela doit être réalisé. Il définit l'entité spécifiquement concernée.

Il convient que cet énoncé de domaine d'application soit détenu par un membre de la direction supérieure impliqué dans le programme, ou une équipe de gestion qui sera chargée de guider l'équipe pendant le développement du programme. La personne désignée aura la responsabilité ultime de s'assurer de l'exécution du programme, comprenant les communications, le financement, la mise en œuvre et l'audit.

Finalement, le CSMS doit couvrir toutes les unités d'activité et toutes les zones géographiques de l'organisation. Si l'adhésion de la direction supérieure ne peut pas être initialement obtenue pour ce domaine d'application, il faut définir un domaine d'application plus restreint et se baser sur celui-ci pour construire la crédibilité et démontrer la valeur du CSMS.

#### A.3.2.2.2 Développement du domaine d'application du CSMS

La direction doit comprendre les limites dans lesquelles le CSMS s'applique à l'organisation et établir une orientation et des priorités pour le CSMS. En développant un domaine d'application clairement défini, la direction peut exprimer plus facilement ses buts et ses objectifs concernant le CSMS.

Il convient que le domaine d'application englobe tous les aspects de l'IACS, les points d'intégration avec les partenaires d'activité, les clients et les fournisseurs. Il convient qu'un cadre de gestion (par exemple, une organisation) soit établi pour initier et contrôler la mise en œuvre et les opérations en cours pour la cyber-sécurité dans la société.

Une organisation responsable de la détermination et de la communication des politiques d'entreprise relatives à la cyber-sécurité est importante pour protéger les actifs de l'entreprise dans le cadre de la cyber-sécurité. Les entreprises doivent reconnaître que dans l'univers professionnel actuel basé sur Internet, la connectivité des informations électroniques fait partie intégrante du monde du travail et par conséquent, la cyber-sécurité est essentielle. Les transactions commerciales sont non seulement contenues derrière le pare-feu Internet de l'organisation, mais sont également étendues aux clients, fournisseurs, sous-traitants externes et partenaires d'externalisation.

Le domaine d'application global doit être clarifié dans trois domaines différents: l'activité, l'architecture et l'aspect fonctionnel.

Du point de vue de l'activité, le domaine d'application doit répondre à des questions telles que:

- Quelles sont les entreprises incluses?
- Quelles sont les unités d'activité incluses?
- Quelles sont les zones géographiques incluses?
- Quels sont les sites spécifiques inclus?

Du point de vue architectural, le domaine d'application doit répondre à des questions telles que:

- Quels sont les systèmes informatiques et les réseaux concernés?
- Les systèmes SCADA de surveillance de distribution seront-ils inclus?
- Les systèmes informatiques non liés à la production (pris en charge ou non par le service informatique) dans la fabrication seront-ils inclus?
- Les systèmes d'exécution de fabrication (MES) seront-ils inclus?
- Les systèmes de gestion de brûleur et SIS seront-ils inclus?
- Les systèmes robotisés seront-ils inclus?
- Les connexions avec les fournisseurs ou clients seront-elles incluses?

Du point de vue fonctionnel, le domaine d'application peut être divisé dans les deux catégories suivantes:

a) Activités de gestion des risques directs

Il s'agit d'activités qui impliquent l'évaluation, la communication et la hiérarchisation des risques. Des exemples comprennent la désignation des responsables locaux de la cyber-sécurité, la collecte et la maintenance d'un inventaire des actifs, le développement et la maintenance de l'architecture du réseau, la conduite des audits internes ou externes et la présentation de ces résultats au niveau de l'unité d'activité ou de l'entreprise.

b) Projets associés à la gestion des risques

Il s'agit d'activités basées sur la réduction des risques identifiés par les activités de gestion des risques. Ces solutions de gestion des risques indirects se présentent sous forme de projets qui sont liés dans le temps et du développement et déploiement de services en cours.

Afin de clarifier le domaine d'application fonctionnel, il convient de prendre en compte des questions telles que:

- Comment le domaine d'application de ce travail est-il lié aux systèmes de gestion des risques existants?
- Comment le domaine d'application de ces travaux est-il lié aux politiques de sécurité des informations qui s'appliquent déjà à ces systèmes et à ces organisations?

- Comment le domaine d'application de ce travail est-il lié aux normes et aux procédures techniques qui s'appliquent déjà aux composants architecturaux spécifiques (c'est-à-dire, les systèmes de commande de processus de base, les systèmes SCADA, le SIS, les systèmes de gestion de brûleur et les systèmes robotisés)?
- Comment le domaine d'application de ce travail est-il lié aux projets qui sont déjà financés?
- Comment le domaine d'application de ce travail est-il lié aux services existants?

L'appui de la direction garantit l'entérinement de l'effort par les dirigeants qui sont responsables d'assigner des ressources pour gérer et mettre en œuvre les tâches visant à réduire les risques pour l'IACS.

Il convient que ce domaine d'application soit détenu par un membre de la direction supérieure du programme, ou une équipe de gestion qui sera chargée de guider l'équipe pendant le développement du programme. La personne désignée aura la responsabilité ultime de s'assurer de l'exécution du programme, comprenant les communications, le financement, la mise en œuvre et l'audit.

Avec l'appui et l'adhésion de la direction supérieure, il convient que les parties prenantes soient identifiées et que leur temps de travail consacré à l'amélioration de la sécurité soit imputé. Les parties prenantes sont responsables de l'avancement de l'initiative de sécurité. Avec l'appui de la direction supérieure, les parties prenantes lancent les activités suivantes et mobilisent les ressources appropriées pour exécuter les tâches. Il convient de former une équipe intégrée qui implique les systèmes informatiques bureautiques et professionnels conventionnels, l'IACS et les systèmes qui interagissent avec les clients, les fournisseurs et les prestataires de transport. La charte et le domaine d'application précédemment mentionnés doivent spécifier les personnes devant être impliquées afin d'atteindre les objectifs de l'initiative.

La direction supérieure pourra éventuellement identifier un chef de projet dont la mission sera de rassembler les acteurs appropriés pour travailler sur le projet de sécurité. Cette personne doit avoir un niveau élevé de compréhension de l'état actuel des procédures de cyber-sécurité dans l'entreprise. En supposant que l'objectif est d'améliorer les politiques et procédures de cyber-sécurité pour l'IACS, il convient que le chef de projet cherche à identifier les domaines qui peuvent être affectés par les incidents de cyber-sécurité de l'IACS et identifier les personnes clés qui sont reconnues en tant que responsable/chargés de ces domaines. Il convient que l'accent soit mis sur l'identification des personnes ayant le rôle approprié, indépendamment de l'organisation de laquelle elles dépendent.

Il est important de noter que ces personnes peuvent être présentes dans différentes structures organisationnelles de l'entreprise dans des organisations différentes. L'objectif est de développer un CSMS rentable qui tire parti des processus d'activité et organisations existants plutôt que de créer une organisation entièrement nouvelle. Il convient que les personnes qui ont déjà le rôle et l'expérience appropriés soient sélectionnées dès que possible. La résolution des conflits entre domaines peut constituer une activité importante de cette équipe de parties prenantes.

Il convient que l'équipe centrale de parties prenantes soit multifonctions par nature et rassemble des compétences qui ne sont typiquement pas présentes chez une seule et unique personne. Il convient que l'équipe comprenne des personnes ayant les rôles suivants:

- une/des personne(s) IACS qui peuvent mettre en œuvre et prendre en charge les dispositifs IACS;
- une/des personne(s) opérationnelle(s) responsables de la fabrication des produits et de satisfaire aux commandes des clients;
- une/des personne(s) chargées de la gestion de la sécurité des procédés dont la tâche est de s'assurer qu'aucun incident HSE ne se produit;

- une/des personne(s) de la fonction informatique qui peuvent être responsables de la conception et la mise en œuvre de réseau, du support des ordinateurs de bureau et des serveurs, et similaire;
- une/des personne(s) en charge de la sécurité associées à la sécurité physique et informatique sur le site;
- des ressources additionnelles qui peuvent être dans les fonctions juridiques, des ressources humaines, de l'assistance aux clients ou de l'exécution des commandes.

L'ensemble de parties prenantes peut changer au cours du temps ou bien des individus spécifiques peuvent avoir des rôles plus importants au cours des différentes phases ou des activités de développement du CSMS. Il n'est pas important de savoir quelle organisation conduit le projet, mais plutôt que le chef de projet possède les compétences appropriées pour travailler en équipe dans un objectif commun. Les organisations parentes auxquelles les personnes ci-dessus sont assignées ont chacune quelque chose à apporter et contribuent aux décisions et à la configuration finale du CSMS.

#### A.3.2.2.3 Pratiques suggérées

##### A.3.2.2.3.1 Pratiques de base

Les trois actions suivantes sont des pratiques de base:

a) Décrire la/les organisation(s) responsable(s) d'établir, communiquer et surveiller la cyber-sécurité au sein de l'entreprise.

b) Définir le domaine d'application du CSMS, comprenant:

- systèmes d'information – comprenant l'ensemble des systèmes d'exploitation, bases de données, applications, activités de coentreprises et de tiers;
- IACS – comprenant tous les systèmes de commande de processus, systèmes SCADA, PLC, DCS, postes de travail de configuration et systèmes d'information de fabrication ou de laboratoire pour les données en temps réel et historiques;
- réseaux, réseaux locaux (LAN), réseaux étendus (WAN) – comprenant le matériel, les applications, les pare-feu, les systèmes de détection d'intrusion, et autres;
- points d'intégration avec les fournisseurs d'assistance et de service;
- responsabilités des utilisateurs, comprenant les politiques pour gérer l'authentification et la capacité à être audité;
- protection des informations, comprenant les exigences d'accès et les responsabilités individuelles;
- gestion des risques – comprenant des processus pour identifier et réduire les risques et documenter le risque résiduel;
- reprise après sinistre – comprenant l'identification des logiciels/services critiques;
- exigences de formation;
- conformité, adhésion et audit;
- identification des actifs.

c) La caractérisation de l'organisation responsable pour le CSMS, comprenant:

- structure de l'organisation;
- localisation;
- budget;
- rôles et responsabilités associés aux processus du CSMS.

##### A.3.2.2.3.2 Pratiques additionnelles

Les cinq actions suivantes sont des pratiques additionnelles:

a) Faire approuver le domaine d'application et les responsabilités du CSMS par la direction.

b) Avoir une compréhension claire des rôles et responsabilités associés à la/les organisation(s) responsable(s) de certains aspects du CSMS.

c) Documenter le domaine d'application du CSMS avec des paragraphes séparés concernant des composants spécifiques.

d) Aborder les exigences et responsabilités relatives à l'activité, juridiques (par exemple, la confidentialité des données), et réglementaires.

e) Identifier et documenter la dépendance de la sécurité des procédés vis-à-vis de la cyber-sécurité et des pratiques et procédures de sécurité physique comprenant un cadre pour l'interaction organisationnelle.

#### A.3.2.2.4 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [24], [26].

### A.3.2.3 Élément: Actions d'organisation pour la sécurité

#### A.3.2.3.1 Description de l'élément

Il convient que les entreprises établissent une organisation, structure, ou réseau de personnes ayant des responsabilités dans la sécurité globale en tenant compte du fait qu'il convient que des composantes de sécurité physiques ainsi que des composantes de cyber-sécurité soient mises en œuvre.

Il est important d'établir les responsabilités afin de mettre en œuvre une orientation et une supervision de la cyber-sécurité d'une organisation. La cyber-sécurité, dans le sens le plus large, concerne non seulement les données, mais également les systèmes (matériels et logiciels) qui génèrent ou stockent ces informations et comprend également des éléments de sécurité physique. Il convient que l'IACS, les partenaires importants de la chaîne, les sous-traitants, les partenaires de coentreprise, les partenaires d'externalisation et les spécialistes de la sécurité physique soient considérés par l'organisation comme faisant partie de la structure de sécurité globale et soient donc inclus dans le domaine de responsabilité.

#### A.3.2.3.2 Construction d'un cadre organisationnel pour la sécurité

L'adhésion à un programme de sécurité commence par le haut. La direction supérieure doit démontrer une adhésion claire à la cyber-sécurité. La cyber-sécurité est une responsabilité de l'entreprise partagée par tous les membres de l'entreprise et en particulier, par les membres leaders des équipes d'activité, de fabrication, les équipes d'informatique et le management. Des programmes de cyber-sécurité avec un appui visible de la direction supérieure et l'adhésion des dirigeants de l'organisation ont plus de chances d'obtenir une conformité, de fonctionner plus efficacement et d'obtenir un succès rapide.

Il convient d'établir un cadre de gestion pour initier et contrôler la mise en œuvre d'un programme de sécurité global. Il convient que le domaine d'application et les responsabilités de la cyber-sécurité pour les organisations comprennent la sécurité physique et la cyber-sécurité pour les systèmes IT, les fournisseurs d'IACS, les sous-traitants, les partenaires d'externalisation et les composants importants de la chaîne et de l'organisation. Il convient qu'un programme de sécurité global comprenne des opérations de coentreprise.

Il convient que les organisations établissent un cadre dans lequel la direction supérieure valide la politique de cyber-sécurité, attribue les rôles de sécurité et coordonne la mise en œuvre de cyber-sécurité dans l'ensemble de l'organisation. Ce cadre peut être confronté à des défis organisationnels intéressants. De nombreuses entreprises sont organisées dans une matrice tridimensionnelle dans laquelle une dimension est le secteur d'activité, une deuxième dimension est la fonction ou la discipline et une troisième dimension est la zone géographique. Les dirigeants individuels ont généralement des responsabilités pour une partie de l'organisation globale. Étant donné qu'un système n'est pas plus sûr que son maillon

le plus faible, un système de cyber-sécurité doit être développé pour l'ensemble du domaine géographique couvert par l'organisation.

La cyber-sécurité traite différents risques qui peuvent généralement être classés en problèmes de disponibilité, d'intégrité ou de confidentialité. Les problèmes de disponibilité sont typiquement gérés par un programme de planification de continuité d'activité ou un programme de sécurité réseau. Les problèmes d'intégrité dans un contexte de fabrication sont typiquement gérés par un programme de sécurité des procédés ou d'assurance qualité. Les problèmes de confidentialité sont typiquement gérés par un programme de sécurité des informations. Étant donné que la cyber-sécurité affecte de nombreux domaines de risque différents, il peut être déconseillé qu'un responsable unique ait le niveau de responsabilité nécessaire pour autoriser un programme de cyber-sécurité pour tous les IACS. Il sera souvent nécessaire de rassembler et convaincre un petit groupe de dirigeants qui n'ont peut-être jamais collaboré aussi étroitement pour prendre une décision consensuelle.

Une organisation globale (par exemple, une entreprise) ou des sous-organisations individuelles au sein de l'entreprise peuvent rechercher la conformité à la présente norme. Si l'entreprise entière doit être conforme, le risque est évalué dans l'ensemble de l'entreprise. Dans ce cas, par exemple, des usines individuelles dans l'entreprise peuvent conduire des évaluations des risques spécifiques, mais utiliseront une méthodologie d'évaluation des risques commune qui permet la compilation de ces évaluations au niveau de l'entreprise. Par conséquent, si une entreprise a pour objectif une conformité globale, elle devra définir des lignes directrices pour soutenir ce projet, même si des sous-organisations individuelles telles que des usines font une grande partie du travail.

Une autre possibilité est que l'entreprise ne souhaite pas satisfaire globalement à la norme, mais plutôt que ses sous-organisations à un certain niveau se conforment individuellement ou que certaines sous-organisations entreprennent de satisfaire à la norme de leur propre initiative. Dans tous les cas, l'entreprise doit toujours aider ces sous-organisations à satisfaire à des exigences spécifiques de la norme qui sont gérées au niveau de l'entreprise, telles que la définition des architectures au niveau de l'entreprise, la sélection des employés et la définition des contrats avec les fournisseurs de service. Selon ces scénarios, par exemple, une usine individuelle pourrait avoir sa propre méthodologie d'évaluation des risques, déterminer ses propres priorités d'action et le projet pourrait être soutenu par la direction de l'usine. Dans ces cas, l'entreprise n'évalue pas sa propre conformité globale à la norme, bien qu'elle puisse potentiellement évaluer la conformité d'usines individuelles. Cette stratégie serait particulièrement adaptée pour une compagnie très diverse et décentralisée ou une autre entreprise.

#### A.3.2.3.3 Démarrage et obtention de soutien

Pour que la direction supérieure soutienne efficacement un programme de cyber-sécurité, elle doit être convaincue que les coûts du programme engagés sur leurs budgets seront inférieurs à l'impact de la menace sur leurs domaines de responsabilité. Il peut être nécessaire de développer une justification économique ou une analyse de cas pour gérer les risques liés à la cyber-sécurité afin de convaincre la direction de soutenir le programme. Les responsabilités budgétaires et les domaines de responsabilité doivent être clarifiés au sein de la direction supérieure.

En raison des contraintes de temps, de nombreux membres de la direction supérieure utilisent des conseillers pour trier les problèmes importants qu'ils doivent traiter eux-mêmes des problèmes que d'autres sont plus à même de traiter. Ces individus sont des "gardiens". Dans les grandes organisations, il est fréquent que des organisations du personnel soient utilisées par la direction supérieure pour générer des recommandations pour des aspects techniquement complexes. Il peut être nécessaire de travailler initialement avec ces organisations du personnel pour collecter suffisamment d'informations pour effectuer l'analyse de cas. Ces organisations peuvent également apporter une vision sur des situations dans lesquelles la direction supérieure gère couramment des types de risques spécifiques.

La direction supérieure pourra éventuellement identifier un chef de projet dont la mission sera de rassembler les acteurs appropriés pour travailler sur le projet de sécurité. Cette personne doit avoir un niveau élevé de compréhension de l'état actuel des procédures de cyber-sécurité dans l'entreprise. Il est important de noter qu'un CSMS réellement intégré met en œuvre des systèmes informatiques de bureau et d'entreprise conventionnels, des IACS et des systèmes de chaîne de valeur qui interagissent avec les clients, les fournisseurs les prestataires de transport. La charte et le domaine d'application précédemment mentionnés mettent l'accent sur qui doit être impliqué pour satisfaire aux objectifs du projet.

Il convient que le chef de projet recherche les domaines qui peuvent être affectés par les incidents de cyber-sécurité de l'IACS et identifie les personnes clés qui sont reconnues en tant que responsables de ces domaines. Il convient de mettre l'accent sur l'identification des personnes dans le rôle approprié, indépendamment de l'organisation à laquelle elles sont assignées.

Il est important de noter que ces personnes peuvent être présentes dans différentes structures organisationnelles de l'entreprise et dans des organisations différentes. L'objectif est de développer un CSMS économique qui met en œuvre les processus d'activité et organisations existants plutôt que créer une organisation entièrement nouvelle. Il convient que les personnes qui ont déjà le rôle et l'expérience appropriés soient sélectionnées dès que possible. La résolution des conflits entre domaines peut constituer une activité importante de cette équipe de parties prenantes.

Il convient que l'équipe centrale de parties prenantes soit multifonctions par nature et rassemble des compétences qui ne sont typiquement pas présentes chez une seule et unique personne. Il convient que l'équipe comprenne des personnes ayant les rôles suivants:

- une/des personne(s) IACS qui peuvent mettre en œuvre et prendre en charge les dispositifs IACS;
- une/des personne(s) opérationnelle(s) responsables de la fabrication des produits et de satisfaire aux commandes des clients;
- une/des personne(s) chargées de la gestion de la sécurité des procédés dont la tâche est de s'assurer qu'aucun incident d'hygiène, sécurité et environnement ne se produit;
- une/des personne(s) de la fonction informatique qui peuvent être responsables de la conception et la mise en œuvre de réseau, du support des ordinateurs de bureau et des serveurs, et autres;
- une/des personne(s) en charge de la sécurité associées à la sécurité physique et informatique sur le site;
- des ressources additionnelles qui peuvent être dans les fonctions juridiques, les ressources humaines, l'assistance aux clients ou l'exécution des commandes.

L'ensemble de parties prenantes peut changer au cours du temps ou bien des individus spécifiques peuvent avoir des rôles plus importants au cours des différentes phases ou des activités au cours du développement du CSMS. Il n'est pas important de savoir quelle organisation de l'entreprise conduit le projet, mais plutôt que le chef de projet possède les compétences appropriées pour travailler en équipe dans un objectif commun. Les organisations parentes auxquelles les personnes ci-dessus sont assignées ont chacune quelque chose à apporter et contribuent aux décisions et à la configuration finale du CSMS.

Une pratique courante pour convaincre la direction supérieure consiste à soumettre à essai de nouveaux programmes dans une petite région géographique ou sur un site particulier afin de démontrer que les nouveaux programmes/procédures fonctionnent avant d'engager des ressources importantes. Cette approche peut être efficace pour convaincre la direction supérieure ou présenter l'analyse de cas à la direction supérieure.

Une fois que les membres appropriés de la direction supérieure ont été identifiés, il est important de décider si le CSMS doit leur être présenté collectivement ou s'ils doivent être approchés individuellement. Il est plus efficace de tous les convaincre simultanément, mais ils

peuvent ne pas être tous réceptifs aux arguments avancés en même temps. S'il est nécessaire de persuader une équipe dirigeante, il est utile d'identifier un allié au sein de cette équipe pour examiner la présentation et apporter ses commentaires avant d'effectuer la présentation à l'équipe complète. En raison du nombre de domaines de risque différents qui sont affectés par la cyber-sécurité, il est fréquent de devoir persuader plusieurs équipes dirigeantes.

Si les coûts du programme de cyber-sécurité ne peuvent pas être déterminés initialement en raison de l'absence d'inventaire informatique ou de l'absence de contre-mesures normalisées, un deuxième cycle de présentations peut être nécessaire une fois que ces coûts sont déterminés plus précisément. À ce stade, l'accent doit être mis sur la mise en œuvre d'un système pour équilibrer les coûts des contre-mesures avec les coûts des risques. Généralement, les informations disponibles à ce stade sont insuffisantes pour demander un budget spécifique pour la mise en œuvre de contre-mesures.

#### A.3.2.3.4 Pratiques en support

##### A.3.2.3.4.1 Pratiques de base

Les cinq actions suivantes sont des pratiques de base:

a) Obtenir l'adhésion de la direction supérieure pour définir un cadre organisationnel pour traiter la sécurité.

b) Assigner la responsabilité pour la cyber-sécurité et la sécurité physique au personnel ayant un niveau de financement approprié pour mettre en œuvre les politiques de sécurité.

c) Constituer une équipe de sécurité au niveau de l'entreprise (ou organisation) pour assurer une orientation, une adhésion et une supervision claires. L'équipe peut être un réseau informel, une structure organisationnelle ou hiérarchique couvrant différents services ou organisations de l'entreprise. Cette équipe assigne des responsabilités et veille à ce que des processus d'activité soient en place pour protéger les actifs et informations de l'entreprise.

d) Établir ou modifier les contrats pour prendre en compte les politiques et les procédures de cyber-sécurité et de sécurité physique des partenaires d'activité, sous-traitants, partenaires d'externalisation, et autres. Les politiques de sécurité et les procédures de ces partenaires externes affectent la sécurité de l'IACS.

e) La coordination ou l'intégration de l'organisation de la sécurité physique en cas de chevauchement et/ou synergie entre les risques de sécurité physique et de cyber-sécurité.

##### A.3.2.3.4.2 Pratiques additionnelles

Les quatre actions suivantes sont des pratiques additionnelles:

a) Établir la responsabilité de la cyber-sécurité de l'IACS:

- Une personne spécifique de l'une quelconque des différentes fonctions est responsable de la cyber-sécurité pour l'ensemble de l'organisation. Elle dirige une équipe multifonctionnelle représentant les différentes unités d'activité et services fonctionnels. L'équipe démontre son adhésion à la cyber-sécurité et définit une orientation claire pour l'organisation. Cela comprend la propriété des actifs et des opérations industrielles ainsi que la mise à disposition des ressources appropriées pour répondre aux besoins de sécurité.
- Une équipe distincte est responsable de la sécurité de l'IACS au sein d'une organisation de fabrication ou d'ingénierie. Bien que cette approche présente l'avantage de sensibiliser la direction aux risques associés à l'IACS, les bénéfices d'une telle approche peuvent être nuls si cette équipe n'est pas étroitement coordonnée avec les responsables de la sécurité informatique conventionnelle des actifs et de la sécurité physique.

- Une équipe de sécurité globale est responsable des actifs physiques et logiques. Dans cette structure hiérarchique, la sécurité est gérée par une organisation unique avec des équipes séparées responsables des systèmes physiques et des systèmes d'information. Cette approche est utile dans les petites organisations dans lesquelles les ressources peuvent être limitées.

b) Coordonner les efforts avec les agences réglementaires, les législateurs, et les fournisseurs de service Internet ainsi que d'autres organisations concernées par les menaces terroristes et autres. Les organisations qui ont établi des relations avec du personnel local d'intervention en cas urgence étendent ces relations de manière à inclure le partage d'informations ainsi que la réponse aux incidents de cyber-sécurité.

c) Soumettre les fournisseurs externes qui ont un impact sur la sécurité de l'organisation aux mêmes politiques et procédures de sécurité afin de maintenir le niveau global de sécurité d'IACS. Il convient que les politiques et procédures de sécurité des fournisseurs de deuxième et troisième niveau soient également conformes aux politiques et procédures de cyber-sécurité de l'entreprise si elles affectent la sécurité de l'IACS:

- il convient que les entreprises prennent en compte le risque de sécurité augmenté par l'externalisation d'une partie du processus de prise de décision pour déterminer quelles opérations externaliser et le choix des partenaires d'externalisation;
- les contrats avec des fournisseurs externes régissant les accès physiques et logiques;
- il convient que les attentes de confidentialité ou de non divulgation et les droits de propriété intellectuelle soient clairement définis;
- il convient que des procédures de gestion des modifications soient clairement définies.

d) Supprimer l'accès des fournisseurs externes à la conclusion/finalisation du contrat. L'application de cette mesure en temps opportun est essentielle et doit être clairement stipulée dans le contrat.

#### A.3.2.3.5 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [23], [26], [30], [43].

### A.3.2.4 Élément: Formation du personnel et sensibilisation à la sécurité

#### A.3.2.4.1 Description de l'élément

La sensibilisation à la sécurité de l'ensemble du personnel est un outil essentiel pour réduire les risques de cyber-sécurité. Un personnel informé et vigilant est l'une des lignes défensives les plus importantes de la sécurisation d'un système. En ce qui concerne les IACS, l'importance accordée à la cyber-sécurité doit être égale à celle de la sécurité et l'intégrité opérationnelles, car les conséquences peuvent être tout aussi désastreuses. Il est par conséquent essentiel que l'ensemble du personnel (employés, sous-traitants et tiers) comprenne l'importance de la sécurité pour maintenir le bon fonctionnement du système. Des programmes de formation et de sensibilisation à la sécurité apportent à l'ensemble du personnel (employés, intérimaires et sous-traitants) les informations permettant d'identifier, d'examiner, de prendre en charge et, s'il y a lieu, de corriger les vulnérabilités et les menaces subies par les IACS, et contribuer à faire en sorte que leurs propres pratiques de travail comprennent des contre-mesures efficaces. Il convient que l'ensemble du personnel reçoive une formation technique adéquate liée aux menaces et vulnérabilités connues du matériel, des logiciels et du piratage psychologique. Les programmes de formation à la cyber-sécurité et de sensibilisation à la sécurité sont plus efficaces lorsqu'ils sont adaptés au public, cohérents avec la politique de l'entreprise et communiqués périodiquement. La formation est un moyen de communiquer des messages clés au personnel en temps opportun. Un programme de formation efficace peut aider les employés à comprendre quels sont les contrôles de sécurité nouveaux ou mis à jour requis et générer des idées qu'ils peuvent utiliser pour réduire les risques et l'impact sur l'organisation si des méthodes de contrôle ne sont pas incorporées.

#### A.3.2.4.2 Développement d'un programme de formation du personnel et établissement de la sensibilisation à la sécurité

Une formation d'un type quelconque est une activité qui couvre pratiquement l'ensemble de la période durant laquelle un CSMS est développé et mis en œuvre. Elle commence une fois que le domaine d'application du projet est clairement défini et que l'équipe de parties prenantes est identifiée. L'objectif du programme de formation est d'apporter au personnel les informations nécessaires pour être sensibilisé aux menaces possibles pour le système et leurs responsabilités pour le fonctionnement sûr et sécurisé des installations de production.

Il convient que l'organisation conçoive et développe un programme de formation de cyber-sécurité dans le cadre du programme de formation global de l'organisation. Il convient que la formation comprenne deux phases: 1) formation générale pour l'ensemble du personnel et 2) formation à base de rôles pour les fonctions et les responsabilités spécifiques. Avant de commencer le développement du programme de formation, il est important d'identifier le domaine d'application et les limites de la formation et de définir les différents rôles au sein de l'organisation.

Il convient que le programme de formation général soit développé pour l'ensemble du personnel. Il convient que les utilisateurs soient formés aux procédures de sécurité appropriées, à l'utilisation correcte des installations de traitement des informations et à la manipulation correcte des informations afin de réduire les risques au minimum. Il convient que la formation comprenne en outre les responsabilités légales, les contrôles d'activité et les responsabilités individuelles de sécurité.

Il convient que la formation à base de rôles soit focalisée sur les risques de sécurité et les responsabilités associées au rôle spécifique d'une personne au sein de l'organisation. Ces personnes requièrent une formation plus spécifique et intensive. Il convient de faire appel à des experts en la matière pour contribuer à cette formation. La formation à base de rôles peut être conduite en salle de formation, sur Internet ou sur le terrain. Cette formation peut également comporter des formations assurées par des fournisseurs pour une discussion approfondie des outils et des expositions associées.

Il convient que le programme comprenne un moyen d'examen et de révision du programme, comme requis et un moyen pour évaluer l'efficacité du programme. De plus, il convient de définir un intervalle pour une formation périodique de rappel.

L'adhésion de la direction à la formation et à l'assurance d'une sensibilisation adéquate à la cyber-sécurité est essentielle pour assurer un environnement informatique stable et fiable pour les secteurs IT et IACS. En particulier pour l'environnement IACS, un environnement informatique stable et fiable contribue à maintenir le fonctionnement sûr de l'équipement sous contrôle et à réduire les incidents HSE. Il convient que celui-ci soit sous la forme de ressources pour développer et organiser la formation et la mise à disposition du personnel pour participer à celle-ci.

Après le développement d'un programme de formation à la cyber-sécurité, il convient que l'organisation dispense la formation appropriée à l'ensemble du personnel. Il convient que des programmes de formation soient mis en œuvre dans des emplacements et à des moments qui permettent au personnel d'être formé sans affecter ses autres responsabilités.

Il convient de dispenser une formation générale dans le cadre de la formation des nouveaux employés et du personnel sous-traitant, temporaire et tiers. Il convient que la formation requise des personnes soit adaptée avec le niveau de contact qu'ils ont avec l'organisation. Une formation spécialisée peut être dispensée comme suit:

a) Formation des parties prenantes

   La formation est adaptée pour l'équipe de parties prenantes ainsi que la communauté des personnes dans la communauté des IACS qui seront finalement affectées. L'équipe de parties prenantes requiert une formation spécifique sur le type de risques qui sont pris en

compte, le domaine d'application et la charte que la direction a approuvée, les informations générales sur les incidents qui se sont produits sur ces systèmes au sein de l'organisation ou dans l'industrie en général et sur les types d'architectures et de systèmes qui sont utilisés au sein de l'organisation. Une formation en salle formelle n'est pas nécessaire pour partager ces informations. Des présentations lors de réunions professionnelles, des sessions de communication et des annonces par courrier électronique sont des exemples de moyens pour partager les informations.

b) Formation des employés en préparation pour de nouveaux rôles

Une formation est nécessaire pour les employés qui se préparent à prendre de nouvelles fonctions dans le système de gestion des risques directs ou dans les projets associés à la gestion des risques. Pratiquement tous les membres de la communauté IACS recevront certaines formations au cours de cette phase. Une partie des rôles de gestion des risques directs comprend des responsabilités d'auto-évaluation ou d'audits internes.

c) Formation des auditeurs

Une formation est nécessaire pour aider les auditeurs à comprendre la nature des systèmes et des réseaux qu'ils auditent ainsi que les politiques spécifiques qui ont été créées.

d) Formation continue

Il existe un besoin continu de formation à tous les niveaux en raison de l'arrivée de nouveaux employés et de personnel tiers, en raison du besoin d'effectuer des mises à jour étant donné que les politiques et les services sont modifiés au fil du temps et de dispenser des formations de rappel afin d'assurer que le personnel reste compétent dans ses rôles et ses responsabilités.

Il est important de valider que le personnel est sensibilisé à ses rôles et ses responsabilités dans le cadre du programme de formation. La validation de la sensibilisation à la sécurité remplit deux fonctions: 1) elle contribue à déterminer la bonne compréhension du programme de cyber-sécurité de l'organisation par le personnel et 2) elle contribue à évaluer l'efficacité du programme de formation. La validation peut être effectuée par plusieurs moyens comprenant une épreuve écrite sur le contenu de la formation, des évaluations de cours, l'exécution de tâches sous surveillance ou des changements documentés de comportement vis-à-vis de la sécurité. Il convient qu'une méthode de validation soit convenue au cours du développement du programme de formation et communiquée au personnel.

Il convient de tenir à jour des dossiers de formation des employés et des plans de mise à jour des formations, et de les consulter régulièrement. La documentation de la formation peut aider l'organisation à s'assurer que tout le personnel a la formation requise pour ses rôles et ses responsabilités spécifiques. Elle peut également contribuer à déterminer si une formation additionnelle est nécessaire et quand une formation de rappel périodique est requise.

Les vulnérabilités, menaces et mesures de sécurité évoluent au cours du temps. Ces changements requièrent des modifications du contenu du programme de formation. Il convient que le programme de formation soit examiné périodiquement (par exemple, chaque année) afin de vérifier son efficacité, son applicabilité, son contenu et sa cohérence avec les outils actuellement utilisés, les pratiques de l'entreprise et la législation et le programme est révisé si nécessaire. Des abonnements à des services d'alerte de sécurité peuvent contribuer à maintenir une connaissance à jour des vulnérabilités et des expositions récemment identifiées.

#### A.3.2.4.3 Pratiques en support

##### A.3.2.4.3.1 Pratiques de base

Les sept actions suivantes sont des pratiques de base:

a) Prendre en compte les différents rôles associés au maintien d'un environnement de systèmes fiables dans les curriculums de formation de cyber-sécurité.

b) Conduire des formations en salle ou sur le terrain pour prendre en compte les exigences pour chaque rôle.

c) Valider la compréhension d'un utilisateur par des évaluations et/ou examens du cours.

d) Disposer d'experts en la matière pour chaque cours qui peuvent donner des informations additionnelles et des conseils.

e) Réviser et valider périodiquement le curriculum de formation et évaluer son efficacité.

f) Communiquer des messages clés à l'ensemble du personnel en temps opportun via un programme de communication de sensibilisation à la sécurité.

g) Former initialement l'ensemble du personnel et périodiquement par la suite (par exemple, chaque année).

Bien qu'aucune de ces pratiques de base ne soit spécifique à la formation de sécurité IACS, l'accent et le contenu des programmes de formation doivent démontrer la relation entre la sécurité IACS et les conséquences HSE.

#### A.3.2.4.3.2 Pratiques additionnelles

Les sept actions suivantes sont des pratiques additionnelles:

a) Établir une formation de cyber-sécurité en tant que composant de l'organisation de formation globale de l'entreprise pour tous les employés.

b) Adapter les curriculums de formation de cyber-sécurité avec une évolution du support suivant le rôle attribué dans l'organisation.

c) Maintenir et examiner les dossiers de formation des employés et les programmes de mise à niveau de façon périodique suivant leur position/rôle.

d) Mettre en œuvre la formation de cyber-sécurité dispensée par les fournisseurs.

e) Établir le calendrier, la fréquence et le contenu du programme de communication de sensibilisation à la sécurité dans un document afin d'améliorer la compréhension par l'organisation des contrôles de cyber-sécurité.

f) Inclure une présentation du programme de communication de sensibilisation à la sécurité pour l'ensemble du personnel afin de s'assurer qu'il est sensibilisé aux pratiques de sécurité dès le premier jour.

g) Évaluer chaque année l'efficacité, l'applicabilité, le contenu et la cohérence du programme de formation et de sensibilisation à la sécurité avec les outils actuellement utilisés et les pratiques d'entreprise.

#### A.3.2.4.4 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [2], [23], [24], [26].

### A.3.2.5 Élément: Plan de continuité d'activité

#### A.3.2.5.1 Description de l'élément

Un plan de continuité d'activité identifie les procédures pour maintenir ou rétablir les opérations d'activité essentielles lors d'une reprise après une défaillance significative. L'objectif du plan de continuité d'activité est de donner un plan d'action pour répondre aux conséquences des sinistres, des défaillances de sécurité et des pertes de service pour une activité. Un plan de continuité d'activité détaillé garantit que les systèmes IACS critiques pour l'activité peuvent être restaurés et utilisés dès que possible après l'occurrence d'une défaillance significative.

#### A.3.2.5.2 Domaine d'application du plan de continuité d'activité

Avant de développer le plan de continuité d'activité, il est important de comprendre à quel moment il convient que le plan soit utilisé et quels types de situations s'appliquent. Les

interruptions non planifiées peuvent prendre la forme d'un sinistre naturel (c'est-à-dire, un ouragan, une tornade, un tremblement de terre ou des inondations), un événement d'origine humaine involontaire (c'est-à-dire, dommage matériel accidentel, incendie ou explosion ou erreur de l'opérateur), un événement d'origine humaine intentionnel (c'est-à-dire, attaque à l'explosif, par arme à feu, vandalisme, piratage informatique ou virus) ou une défaillance d'équipement. Du point de vue de l'interruption de service, la reprise peut prendre typiquement plusieurs minutes ou plusieurs heures pour de nombreuses pannes mécaniques, à plusieurs jours, semaines ou mois pour un sinistre naturel. Étant donné que la fiabilité et la maintenance électrique/mécanique constituent une discipline séparée, certaines organisations choisissent de définir une continuité d'activité en excluant ces sources de défaillance. Étant donné que la continuité d'activité concerne principalement les implications à long terme des interruptions de production, certaines organisations choisissent d'appliquer une limite d'interruption minimale sur les risques à prendre en compte. Pour la cyber-sécurité des IACS, il est recommandé qu'aucune de ces contraintes ne soit appliquée. Il convient de prendre en compte les interruptions à long terme (reprise après sinistre) et à court terme (reprise opérationnelle). Le plan comprend en outre d'autres aspects d'une reprise après sinistre, tels que la gestion d'urgence, les ressources humaines et les relations avec les médias ou la presse.

Étant donné que ces interruptions potentielles impliquent des événements d'origine humaine, il est également important de travailler en collaboration avec l'organisation de la sécurité physique pour comprendre les risques relatifs de ces événements et les contre-mesures de sécurité physique en place pour les prévenir. Il est également important pour la sécurité physique que l'organisation identifie les aspects d'un IACS d'un site de production qui peuvent présenter des risques de niveau supérieur.

#### A.3.2.5.3 Planification du processus de continuité d'activité

Avant de générer un plan pour traiter des interruptions potentielles, il est important de spécifier les objectifs de la reprise pour les différents systèmes et sous-systèmes concernés sur la base des besoins typiques de l'activité. La reprise du système implique la reprise de toutes les liaisons de communication et les fonctionnalités de l'IACS et est généralement spécifié en termes d'objectif de temps de reprise ou de temps avant reprise de ces liaisons et fonctionnalités. La reprise de données met en œuvre la reprise des données décrivant les conditions de production ou de produit précédentes et elle est généralement spécifiée en termes d'objectif de point de reprise ou de durée maximale pendant laquelle une absence de données peut être tolérée.

Une fois que les objectifs de reprise sont définis, il convient qu'une liste d'interruptions potentielles soit créée et une procédure de reprise développée et documentée. Pour la plupart des reprises à une plus petite échelle, les activités de réparation et de remplacement basées sur un inventaire des pièces de rechange critiques peuvent s'avérer suffisantes pour satisfaire aux objectifs de reprise. Dans d'autres cas, des plans d'intervention doivent être développés. En raison du coût potentiel de ces plans d'intervention, il convient que ceux-ci soient examinés avec les dirigeants responsables de la planification de continuité d'activité afin de vérifier qu'ils sont justifiés.

Il convient d'identifier les exigences pour une équipe de continuité d'activité et de former une telle équipe. Il convient que l'équipe comprenne les propriétaires de l'IACS et des autres opérations industrielles. En cas d'interruption majeure, il convient que cette équipe détermine la priorité des systèmes d'activité et des systèmes IACS critiques pour rétablir les opérations.

Il convient de développer un programme pour soumettre à essai tout ou une partie des procédures de reprise. Les procédures pour un sous-système sont souvent soumises à essai à échéance annuelle et le sous-système spécifique est mis en rotation de sorte que l'ensemble des procédures du système soient finalement soumises à essai sur une période de 5 à 10 ans. Ces fréquences ne sont que des exemples et doivent être déterminées par l'organisation dans le cadre du processus de planification.

Il convient d'apporter une attention particulière à la vérification des sauvegardes pour les données de configuration du système et les données de produit ou de production. Non seulement il convient de soumettre à essai celles-ci lors de leur production, mais il convient également que les procédures suivies pour leur stockage soient examinées périodiquement afin de vérifier que les sauvegardes et les données de support sont utilisables et exactes. Il convient de conserver ces sauvegardes dans des conditions environnementales qui ne les rendent pas inutilisables et dans un lieu sûr où elles peuvent être rapidement obtenues par des personnes autorisées en cas de besoin.

En cas d'incident, l'organisation peut être amenée à fournir des éléments à des investigateurs, qui peuvent être internes ou externes à l'organisation.

Le plan de continuité d'activité doit être réexaminé au fil du temps et révisé afin de refléter les changements dans l'organigramme, l'organisation, le modèle d'activité, l'industrie, et autres.

#### A.3.2.5.4 Pratiques en support

##### A.3.2.5.4.1 Pratiques de base

Les dix-neuf actions suivantes sont des pratiques de base:

a) Former une équipe de continuité d'activité impliquant les principales parties prenantes dans l'organisation (c'est-à-dire, les propriétaires de l'entreprise, le personnel informatique et le personnel IACS) pour développer le plan.

b) Déterminer la priorité des activités critiques et de l'IACS sur la base de la nature du système et du temps nécessaire pour la restauration. Cela dépend des objectifs de tolérance des risques et de reprise de l'organisation.

c) Déterminer la quantité requise de temps/ressources pour la restauration du système, l'emplacement des fichiers de sauvegarde, le matériel, la fréquence des sauvegardes, le besoin de disques de secours, et autres, afin d'assurer que les systèmes critiques puissent être restaurés en cas de situation de catastrophe.

d) Faire en sorte que les enregistrements associés aux procédures de gestion et de sauvegarde/reprise de documents soient aisément disponibles de plusieurs façons depuis des emplacements multiples (c'est-à-dire, des copies électroniques stockées en lieu sûr et des copies papier sur site et dans une installation protégée) de sorte qu'il n'y ait pas de point de défaillance unique.

e) Prendre en compte l'impact possible sur des tiers tels que les coentreprises et les chaînes logistiques.

f) Déterminer le besoin d'assurance d'activité additionnelle.

g) Définir les rôles et responsabilités spécifiques pour chaque partie du plan. Certaines organisations divisent l'équipe en sous-équipes dépendant d'un comité de coordination. Des exemples de sous-équipes comprennent l'évaluation des dommages, la restauration et la reprise, les communications (internes et externes) et les réponses d'urgence.

h) Assigner la responsabilité de l'initiation du plan de continuité d'activité et définir clairement les circonstances dans lesquelles le plan doit être activé.

i) Détailler dans quelles circonstances des mesures d'urgence spécifiques doivent être prises. Le choix de mesures varie suivant le scénario spécifique. Prendre en compte les conséquences d'un sinistre informatique ou IACS ayant un impact physique sur les installations de production.

j) Définir le type, le nombre et l'identité des ressources nécessaires et leurs attributions.

k) Détailler les méthodes de communication pour les membres de l'équipe en tenant compte des événements de perte de courrier électronique, coupure téléphonique, etc., en cas de sinistre à grande échelle.

l) Définir la fréquence et la méthode pour soumettre à essai, valider et évaluer le plan de continuité et l'utilisation de ces résultats pour améliorer et mettre à jour le plan pour augmenter l'efficacité.

m) Détailler les risques associés à l'application du plan de continuité et comment ceux-ci peuvent être pris en compte et/ou réduits.

n) Identifier les données qui requièrent une manipulation et une protection spéciales, ainsi que les informations qui sont essentielles pour la continuité d'activité.

o) Établir des procédures intermédiaires pour continuer les opérations minimales d'activité. Des objectifs de production réduits peuvent être appropriés pendant cette période intermédiaire.

p) Identifier et stocker les systèmes de sauvegarde (matériel, logiciel et documentation) en lieu sûr.

q) Soumettre à essai les systèmes de sauvegarde selon un échéancier prédéfini pour un fonctionnement correct du système et une restauration correcte des données.

r) Identifier et/ou stocker les fournitures requises en appui de l'équipe de réponse d'urgence et faciliter les opérations d'activité de restauration (par exemple, eau en bouteille, douches de décontamination et conteneurs d'air ou masques respiratoires d'urgence).

s) Définir le processus de reprise des opérations normales.

#### A.3.2.5.4.2 Pratiques additionnelles

Les neuf actions suivantes sont des pratiques additionnelles:

a) Hiérarchiser les systèmes informatiques et IACS en fonction de leur conséquence pour l'activité ou les opérations, sur la base de la tolérance des risques de l'organisation. L'IACS peut avoir un impact sur les systèmes IT qui pourrait être négligé sans un examen et une hiérarchisation globale des systèmes dans leur ensemble. Il convient que la planification en cas de sinistre et les plans de reprise tiennent compte des interactions entre ces systèmes.

b) Localiser les sauvegardes de système critiques à des emplacements géographiques différents. Si cela n'est pas faisable, stocker les données de sauvegarde et l'équipement de secours à un emplacement qui n'est pas sujet au même sinistre physique que le système primaire (c'est-à-dire, en hauteur pour les inondations ou bunker en béton pour les tempêtes).

c) Soumettre à essai et mettre à jour les plans de continuité d'activité, périodiquement ou selon le besoin.

d) Relier les plans de continuité d'activité à un système de gestion des modifications afin d'assurer que le plan de continuité d'activité est mis à jour en cas de modification significative du système ou de changement consécutif pour l'activité.

e) Soumettre à essai les plans de communication périodiquement ou selon le besoin et attribuer la responsabilité de maintenir à jour les listes d'appel.

f) Fournir des informations de contact critique à l'équipe centrale (carte conservée par chaque membre de l'équipe).

g) Chaque membre de l'équipe doit conserver des copies papier du plan à son domicile.

h) Mettre en place des procédures et/ou des contrats pour acheter du matériel, des logiciels et des fournitures supplémentaires, si nécessaire. Il est important que le plan de continuité équilibre les temps de remplacement pour les IACS avec les temps de remplacement pour l'équipement contrôlé. Dans certains cas, un équipement peut avoir des délais de réparation/remplacement longs qui dépassent largement le temps de remplacement des systèmes de commande.

i) Établir à l'avance des contrats de niveau de service avec les fournisseurs pour un service de reprise après sinistre.

#### A.3.2.5.5 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [23], [37], [48], [51].

### A.3.2.6 Élément: Politiques et procédures de sécurité

#### A.3.2.6.1 Description de l'élément

Chaque système de gestion comprend des ensembles d'exigences globales qui doivent être satisfaites par le système et des listes des organisations soumises à ces exigences. Dans la présente norme, ces exigences sont appelées politiques. Elles comprennent également des descriptions de la façon selon laquelle les individus et les organisations satisfont aux exigences du système de gestion. Dans la présente norme, ces descriptions sont appelées procédures.

Pour un CSMS, les politiques contiennent des instructions générales sur les exigences relatives à la cyber-sécurité au sein de l'organisation. Elles contiennent des directives concernant la manière dont une organisation définit la cyber-sécurité, met en œuvre son programme de cyber-sécurité et gère la tolérance des risques. Les politiques pour le CSMS sont créées à partir de politiques d'entreprise de niveau supérieur, à partir desquelles elles dérivent leur autorité. Les politiques intègrent les conséquences négatives d'une non-conformité, comprenant éventuellement des licenciements, voire des poursuites pénales.

Les procédures détaillent la manière dont les politiques du CSMS sont mises en œuvre au sein de l'organisation. Elles peuvent ne pas être aussi strictes que les politiques et peuvent comprendre des dispositions pour prendre en compte des exceptions étant donné qu'il est très difficile de définir des procédures pour traiter de manière appropriée l'ensemble des situations ou événements possibles.

Il convient que les politiques et procédures du CSMS rédigées par l'organisation définissent clairement les rôles et responsabilités du personnel dans la sécurisation des actifs de l'organisation.

#### A.3.2.6.2 Développement de politiques de sécurité

Il convient que les politiques de sécurité pour l'organisation ne soient pas envisagées comme une tâche linéaire. Une fois que les étapes initiales de développement de politique ont été effectuées, l'organisation doit examiner et analyser l'efficacité de ces politiques, puis les affiner si nécessaire. Il convient de ne pas développer ces politiques de façon isolée des autres systèmes de gestion des risques au sein de l'organisation.

Le développement et la mise en œuvre de politiques de sécurité requiert l'adhésion de la direction supérieure de tous les secteurs de l'organisation ayant des responsabilités pour ces types de systèmes. En définissant et en soutenant une politique de sécurité, la direction supérieure peut démontrer son adhésion à son amélioration continue. L'adhésion de la direction en ce qui concerne les politiques de sécurité implique la reconnaissance par les dirigeants de l'organisation que la politique de sécurité est une responsabilité de l'entreprise qui est partagée par tous les membres de l'équipe dirigeante et est une politique qui comprend des composantes physiques et informatiques. Les procédures de sécurité doivent être incorporées dans les stratégies globales d'activité et être approuvées par la direction.

De nombreuses organisations IACS ont des politiques existantes en place pour des systèmes tels que la sécurité, la sécurité physique, l'IT et le comportement des employés. Au début du processus de développement d'un CSMS, il est important de tenter d'intégrer les politiques de cyber-sécurité dans ce système avec les politiques et procédures existantes. Cela peut nécessiter dans de nombreux cas la modification des politiques dans d'autres systèmes de gestion des risques. Par exemple, des systèmes existants de gestion des risques peuvent avoir déjà caractérisé les risques ou établi des niveaux de tolérance des risques qui doivent être pris en compte dans le développement du nouveau CSMS. Une description de la combinaison des politiques et des systèmes de gestion des risques peut être trouvée dans la CEI/TS 62443-1-1, 5.6. Les politiques de sécurité relatives aux risques des IACS concernent également un large éventail de problèmes allant des exigences de la direction organisationnelle aux exigences techniques détaillées de configuration du système. Il est recommandé que ces politiques soient séparées en sous-groupes appropriés afin de les

rendre plus accessibles aux lecteurs qui peuvent être intéressés uniquement par des sujets spécifiques.

Dans de nombreux cas, les politiques et les procédures de sécurité peuvent être considérées comme des contre-mesures pour gérer les risques. Celles-ci peuvent prendre plusieurs formes, depuis les procédures administratives jusqu'aux outils de sécurité automatisés. L'objectif est de rendre le coût global des contre-mesures inférieur à l'impact global du risque. Réduire le coût pour mettre en œuvre les contre-mesures tout en obtenant le même niveau de réduction des risques donne plus de valeur à l'organisation. Pour les cas où cette économie d'échelle existe, la discipline IT gère les technologies pour lesquelles cet effet d'échelle peut être exploité. Par conséquent, les politiques de sécurité détaillées de la discipline IT doivent être examinées pour être éventuellement appliquées de nouveau dans l'espace de l'IACS.

Au cours du développement des politiques de cyber-sécurité, il est important de prendre en compte les exigences de conformité ainsi que le processus d'audit. Étant donné que l'IACS doit être évalué pour sa conformité aux politiques de sécurité, il est nécessaire de s'assurer que les politiques définies ne soient pas en conflit avec d'autres politiques de gestion des risques, éventuellement plus importantes. Par exemple, une politique de sécurité est créée et requiert que tous les ordinateurs de bureau soient protégés par mot de passe dans une centrale nucléaire. Cette politique globale requiert également que toutes les stations d'opérateur dans la salle de commande soient protégées par mot de passe, mais ces stations d'opérateur doivent être ouvertes en raison des règlements sur la sécurité. La politique relative aux mots de passe pour les ordinateurs de bureau conduirait le système à ne plus être conforme aux politiques HSE. Il convient que la politique de cyber-sécurité soit rédigée initialement en tenant compte de l'effet qu'elle aurait sur les différents systèmes d'un site particulier. Une meilleure approche consisterait à définir une politique qui spécifie que les ordinateurs de bureau soient protégés contre une utilisation non autorisée et que des procédures puissent exiger la protection par mot de passe dans certains cas tout en préconisant l'isolement physique dans d'autres situations.

#### A.3.2.6.3 Détermination de la tolérance de l'organisation aux risques

Il convient qu'une organisation définisse une politique de tolérance des risques liée aux niveaux de risque, correspondant à une combinaison particulière de vraisemblance et de conséquences. Cette politique peut être basée sur une évaluation qualitative des risques constituée d'une liste d'actifs ou de scénarios avec une vraisemblance globale et un classement des conséquences, qui sont définis et assignés comme faisant partie du processus d'évaluation des risques de l'organisation (voir A.2.3).

Dans l'exemple type de matrice de niveau de risque décrit dans le Tableau A.3, les vraisemblances et les conséquences ont été décomposées en trois niveaux. Le niveau de risque a également été décomposé en trois niveaux. Les niveaux de risque dans chaque bloc (Haut, Moyen et Bas) correspondent à une combinaison particulière de vraisemblance et de conséquence. Une organisation définit une politique de tolérance des risques associée à chaque niveau, qui correspond à un niveau particulier de réponse de l'entreprise au risque. Par exemple, des risques classés de niveau Haut peuvent être résolus en 6 mois; aucun effort spécifique ne sera consacré aux risques classés de niveau Bas; et un effort intermédiaire sera consacré aux risques de niveau Moyen. En d'autres termes, l'organisation a établi qu'elle peut tolérer un risque de niveau Haut pendant 6 mois au maximum.

#### A.3.2.6.4 Examen et révision des politiques de cyber-sécurité

Il convient que les politiques de cyber-sécurité soient examinées périodiquement et validées afin de confirmer qu'elles sont à jour et suivies et révisées de manière appropriée afin de veiller à ce qu'elles restent appropriées. Lorsque les politiques de cyber-sécurité sont à un niveau supérieur, il convient qu'elles ne soient pas nécessairement mises à jour aussi souvent car elles décrivent plutôt "le quoi" que "le comment". Bien que l'aspect "comment" de la procédure puisse changer en cas de nouvelles menaces ou techniques, la raison pour laquelle le système est protégé reste relativement constante.

#### A.3.2.6.5 Déploiement de politiques de cyber-sécurité

Pendant la création de politiques de cyber-sécurité, il convient que le procédé pour déployer celles-ci soit défini. Par exemple, des politiques de sécurité peuvent être publiées sur l'intranet de l'entreprise et les utilisateurs peuvent être formés sur les effets de la politique sur leur activité. Les politiques sont le fondement du CSMS. Par conséquent, il convient que le système pour le déploiement soit cohérent avec la mise en œuvre du système de gestion.

#### A.3.2.6.6 Pratiques en support

##### A.3.2.6.6.1 Pratiques de base

Les cinq actions suivantes sont des pratiques de base:

a) Obtenir l'adhésion, l'implication et l'appui de la direction lors de la création et de la mise en vigueur de politiques de cyber-sécurité.

b) Exiger l'examen et l'approbation par toutes les unités d'activité et services concernés, y compris la direction opérationnelle.

c) Publier des documents écrits décrivant les politiques de cyber-sécurité.

d) Examiner, valider et réviser périodiquement les politiques afin de confirmer qu'elles sont à jour et appliquées.

e) Communiquer et disséminer des politiques de cyber-sécurité à l'ensemble du personnel.

##### A.3.2.6.6.2 Pratiques additionnelles

Les dix actions suivantes sont des pratiques additionnelles:

a) Créer des politiques cohérentes avec un cycle de vie déterminé par l'organisation. Les politiques ne sont pas constamment modifiées et ne sont pas non plus modifiées en réaction à des sujets d'actualité.

b) Créer des politiques de support concernant des rôles ou groupes spécifiques qui définissent comment la politique de niveau supérieur est mise en œuvre pour chacun de ces groupes. Par exemple, le contrôle d'accès physique et les restrictions par mot de passe peuvent être inadaptés dans certaines situations de commande industrielle. Des protections procédurales exceptionnelles peuvent être nécessaires pour compenser cette situation.

c) Créer des politiques de sécurité pour gérer différents problèmes de sécurité, comprenant la diminution des risques et le changement de comportement du personnel concernant la cyber-sécurité.

d) Aligner les politiques de sécurité avec les politiques et stratégies organisationnelles globales.

e) Intégrer les politiques de cyber-sécurité avec ou dans le cadre d'une politique de sécurité globale qui concerne également des éléments physiques.

f) Identifier comment les politiques sont mises en vigueur et par qui.

g) Déterminer comment les utilisateurs doivent se conformer aux dispositions des politiques.

h) Établir un cadre de gestion de politique cohérent.

i) Identifier les politiques qui s'appliquent à des utilisateurs ou des groupes d'utilisateurs spécifiques.

j) Déterminer comment mesurer les exigences de conformité pour les politiques.

#### A.3.2.6.7 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [23], [26], [30], [43].

### A.3.3 Groupe d'éléments: Contre-mesures de sécurité sélectionnées

#### A.3.3.1 Description du groupe d'éléments

Le deuxième groupe d'éléments de cette catégorie est Contre-mesures de sécurité sélectionnées. Les éléments de ce groupe traitent de certains des principaux types de contrôles de sécurité qui font partie d'un CSMS bien conçu. Le présent document ne cherche pas à décrire la mise en œuvre complète de n'importe quelle des contre-mesures de sécurité sélectionnées. Il décrit de nombreux aspects de politique, de procédure et de pratique liés à ces contre-mesures de sécurité particulières. La Figure A.7 montre une représentation graphique des six éléments de ce groupe d'éléments:

- Sécurité du personnel,
- Sécurité physique et environnementale,
- Segmentation des réseaux,
- Contrôle d'accès – Administration des comptes,
- Contrôle d'accès – Authentification, et
- Contrôle d'accès – Autorisation

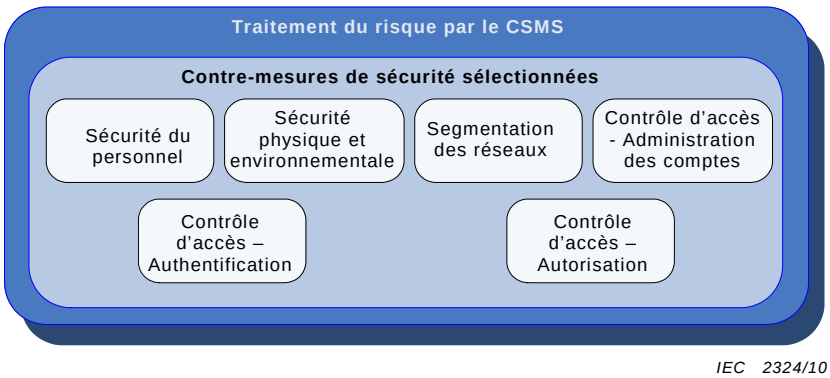



**Figure A.7 – Vue graphique du groupe d'éléments: Contre-mesures de sécurité sélectionnées**

Un CSMS est le système via lequel les contre-mesures de sécurité d'une organisation sont choisies et maintenues. Par conséquent, des contre-mesures particulières sont considérées comme une conséquence de ce système plutôt qu'une partie du CSMS lui-même. Cependant, les contre-mesures décrites dans ce paragraphe ont été incluses dans la présente norme parce que leur application est fondamentale pour la formulation de la politique de sécurité et de l'architecture. Pour cette raison, il convient de les mettre en avant lors de la création d'un CSMS.

#### A.3.3.2 Élément: Sécurité du personnel

##### A.3.3.2.1 Description de l'élément

La sécurité du personnel met en œuvre l'évaluation du personnel potentiel et actuel afin de déterminer s'il remplit ses responsabilités pour la sécurité de l'IACS dans l'organisation et l'établissement et la communication de ses responsabilités à ces fins. Les employés, sous-traitants ou personnel intérimaire qui ont accès à des informations sensibles sur les opérations industrielles ou aux réseaux, matériel et logiciels d'IACS constituent une exposition potentielle au risque si des informations sensibles sont divulguées, modifiées ou si un accès non autorisé aux systèmes IT ou IACS est accordé.

#### A.3.3.2.2 Exigences relatives à la sécurité du personnel

Dans de nombreuses organisations, les exigences de sécurité du personnel ont été régies par des risques liés à des menaces internes et l'éventualité d'accidents causés par une un détail négligé ou par un personnel inadapté pour un poste en raison d'un manque de compétences appropriées ou de l'utilisation de substances qui pourraient altérer leur jugement. La mise en œuvre de politiques de sécurité du personnel peut permettre de réduire ces types de problèmes.

Lors du développement d'un programme visant à assurer la sécurité du personnel, il est important d'inclure le personnel qui peut accéder à tous les systèmes dans le domaine d'application et ne pas limiter le projet au personnel utilisant des installations de salle informatique conventionnelles.

Les ordinateurs dans les opérations IACS sont des outils exploités pour utiliser les installations de façon productive et sûre. Le personnel qui utilise les systèmes est au cœur des opérations et il convient de tout mettre en œuvre pour s'assurer que ces personnes sont qualifiées et adaptées pour ces postes. Ce processus commence à la phase de recrutement et continue jusqu'au départ de l'entreprise. Il requiert une attention constante de la direction et des collègues de travail afin de veiller à ce que le système soit utilisé en toute sécurité.

Il convient qu'une politique de sécurité du personnel énonce clairement l'adhésion de l'organisation à la sécurité et les responsabilités du personnel relatives à la sécurité. Il convient qu'elle aborde les responsabilités relatives à la sécurité de l'ensemble du personnel (employés individuels et organisation) du recrutement à la sortie de l'entreprise, en particulier pour les postes sensibles. (Cela inclut les employés, les employés potentiels, les employés sous contrat, les sous-traitants et les services de l'entreprise telle que les relations humaines.)

Il convient que l'ensemble du personnel, y compris les nouveaux embauchés et les transferts internes à des postes sensibles (par exemple, ceux nécessitant un accès privilégié), soit soumis à une sélection au cours du processus de demande d'emploi. Il convient que cette sélection comprenne le contrôle de l'identité, des références personnelles et professionnelles et des diplômes universitaires. La sélection peut également comprendre l'historique des emprunts bancaires, l'activité criminelle et le dépistage de drogue étant donné que ces informations peuvent être utiles dans la détermination de la conformité du candidat (dans le cadre de la législation locale). Les tiers, sous-traitants et autres sont soumis à une sélection au moins aussi rigoureuse que les employés à des postes comparables. Les employés et sous-traitants peuvent également être soumis à un contrôle continu concernant, par exemple, les activités financières, criminelles et liées à la drogue. En raison de la quantité de données sensibles relatives aux opérations industrielles et aux risques HSE potentiels dans certains environnements d'IACS, il peut être nécessaire de contrôler un groupe étendu d'employés qui ont accès à l'IACS. Les ouvriers d'usine peuvent nécessiter le même niveau de contrôle et d'enquête qu'un administrateur type de système IT. Les termes "sélection" et "contrôles généraux" sont laissés intentionnellement indéfinis de sorte que l'organisation puisse déterminer le niveau de filtrage à effectuer sur le personnel. "Postes sensibles" est également laissé indéfini par l'organisation parce que des postes peuvent avoir peu ou pas d'effet sur la sécurité du système.

Au cours du processus de candidature, il convient que les termes et conditions d'embauche énoncent clairement les responsabilités des employés en ce qui concerne la cyber-sécurité. Il convient que ces responsabilités se prolongent pendant une période de temps raisonnable après que la personne ait quitté l'entreprise. Lorsque l'entreprise fait appel à des prestataires ou travaille avec du personnel sous-traitant, il convient de documenter leurs responsabilités de sécurité dans tout contrat. Dans la mesure du possible, il convient que leurs responsabilités soient spécifiques et mesurables.

Il convient que le personnel soit sensibilisé aux objectifs de sécurité de l'organisation et à ses responsabilités à l'aide d'énoncés clairement documentés et communiqués par l'organisation. Le personnel doit accepter ses responsabilités respectives afin d'assurer un fonctionnement

sûr et fiable de l'organisation. Les organisations peuvent envisager que l'ensemble du personnel des installations de traitement des informations signe un accord de confidentialité ou de non-divulgation. Il convient que tout accord de confidentialité soit examiné et signé par les employés dans le cadre du processus initial d'embauche. Il convient que les sous-traitants, le personnel occasionnel ou les employés intérimaires non couverts par un accord de non-divulgation formel signent également un accord de confidentialité avant de commencer à travailler.

Il convient que les organisations créent des rôles de poste basés sur la séparation des missions afin de veiller à ce que l'accès aux informations soit basé sur les besoins réels et que l'exécution des étapes opérationnelles à haut risque requière plus d'une personne. Il convient que ces missions soient réparties au sein du personnel afin de maintenir les séparations des pouvoirs appropriées, de sorte qu'aucun individu isolé n'ait un contrôle total sur des actions qui modifient le comportement fonctionnel de l'IACS. Il convient que les rôles et responsabilités en termes de sécurité pour un poste donné soient périodiquement examinés et révisés afin de satisfaire aux besoins changeants de l'entreprise.

Il convient que le personnel reste vigilant vis-à-vis des situations qui peuvent conduire à des incidents de sécurité. Les entreprises doivent former l'encadrement à détecter un comportement du personnel pouvant conduire à des vols, des violations, des erreurs ou d'autres problèmes de sécurité. Il convient d'établir une procédure disciplinaire en cas de violations de cyber-sécurité et de communiquer celle-ci au personnel. Il convient qu'elle soit conforme aux mesures légales et répressives contre de tels crimes en vigueur dans le pays.

#### A.3.3.2.3 Pratiques en support

##### A.3.3.2.3.1 Pratiques de base

Les huit actions suivantes sont des pratiques de base:

a) Sélectionner le personnel au cours de la phase de recrutement, par exemple effectuer des vérifications générales avant embauche ou mutation à des postes sensibles, en particulier pour les fonctions sensibles.

b) Enquêter sur le personnel, en particulier aux postes sensibles, sur une base périodique afin de détecter les problèmes financiers, une activité criminelle ou des problèmes liés a la drogue.

c) Communiquer les termes et conditions d'emploi ou de contrat à l'ensemble du personnel en spécifiant la responsabilité d'un individu relative à la cyber-sécurité.

d) Documenter et communiquer périodiquement les objectifs de sécurité de l'organisation et les responsabilités du personnel.

e) Demander au personnel d'accepter ses responsabilités respectives afin d'assurer un fonctionnement sûr et fiable de l'organisation.

f) Répartir les missions au sein du personnel afin de maintenir les séparations des pouvoirs appropriées.

g) Demander au personnel de signer un accord de confidentialité ou de non-divulgation.

h) Établir une procédure disciplinaire pour le personnel en cas de violation des politiques de sécurité de l'organisation.

##### A.3.3.2.3.2 Pratiques additionnelles

Les deux actions suivantes sont des pratiques additionnelles:

a) Créer des rôles de poste basés sur la séparation des missions afin de veiller à ce que l'accès aux informations soit basé sur les besoins réels et que l'exécution des étapes opérationnelles à haut risque requière plus d'une personne.

b) Documenter les responsabilités de sécurité et inclure celles-ci dans les descriptions de poste, les contrats ou d'autres contrats avec des tiers.

#### A.3.3.2.4 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [2], [23], [26], [30], [43].

### A.3.3.3 Élément: Sécurité physique et environnementale

#### A.3.3.3.1 Description de l'élément

La sécurité environnementale et physique concerne la création d'un environnement sécurisé pour la protection des actifs tangibles ou physiques (c'est-à-dire, des ordinateurs, des réseaux des informations et des équipements opérationnels) contre les dommages, pertes, accès non autorisés ou utilisation incorrecte. La sécurité environnementale et physique des systèmes d'information est une discipline bien établie qui tire ses connaissances d'autres domaines de la sécurité physique ou des installations. Il convient de concevoir des mesures de sécurité environnementale et physique en complément des mesures de cyber-sécurité prises pour protéger ces actifs.

Les mesures de sécurité environnementale et physique sont différentes, mais liées étant donné que toutes deux visent à protéger les actifs d'une organisation contre les menaces. Les mesures de sécurité physique garantissent que les actifs d'une organisation sont protégés contre les accès non autorisés, pertes, dommages, utilisations incorrectes et autres. Les mesures de sécurité environnementale garantissent que les actifs d'une organisation sont protégés contre toute condition environnementale qui les rendrait inutilisables ou endommagerait les informations qu'ils contiennent.

Bien que les politiques et procédures de cyber-sécurité soient importantes pour la protection appropriée des systèmes d'information et de commande, pour une protection vraiment efficace, il convient de les compléter par le niveau de sécurité physique approprié. Par exemple, le maintien de contrôles stricts tels que l'authentification et le contrôle d'accès a un très faible effet de protection de l'intégrité du système s'il est possible de pénétrer dans des installations et d'enlever ou d'endommager physiquement des supports électroniques.

#### A.3.3.3.2 Considérations relatives à la sécurité physique et environnementale

##### A.3.3.3.2.1 Généralités

Dans de nombreuses organisations, les exigences de sécurité environnementale et de périmètre physique ont été motivées par des risques relatifs aux actifs physiques de l'organisation et peuvent ne pas satisfaire aux exigences de cyber-sécurité. En raison de l'intégration d'organisations multiples sur des sites spécifiques (c'est-à-dire, des partenaires, des sous-traitants et des tiers), une protection additionnelle de sécurité physique pour les actifs IACS peut être nécessaire. Dans des installations d'IACS, la sécurité physique est plus particulièrement focalisée sur la protection des actifs IACS que sur les informations opérationnelles elles-mêmes. Le souci n'est pas tant le vol ou la corruption physique du matériel informatique ou de commande, mais plutôt l'impact que cela aurait sur la capacité à maintenir la production de façon fiable.

Lors du développement d'un programme de sécurité physique d'actifs, il est important d'inclure tous les systèmes dans le domaine d'application et non de limiter l'effort aux installations informatiques conventionnelles. La CEI/TS 62443-1-1 décrit des critères qui peuvent être utilisés pour déterminer quels actifs physiques il convient de prendre en compte dans le domaine d'application du CSMS.

Les ordinateurs constituant l'IACS sont des outils utilisés pour mettre en œuvre l'installation de façon productive et sûre. Ce sont des moyens et non une fin ainsi que l'actif qu'ils sont censés protéger. Dans certains cas, la sécurité et/ou la productivité est menacée en enfermant un équipement derrière une porte fermée à clé parce que le délai d'accès à l'équipement peut être rallongé.

Il convient de faire preuve de bon sens technique afin d'équilibrer tous les risques lors de la détermination des procédures de sécurité physique pour les actifs à protéger. Bien que la pratique courante consiste à localiser les routeurs et autres équipements de réseau dans des environnements verrouillés, l'extension de cette pratique au-delà de ce cas particulier peut avoir un intérêt limité. Les dispositifs de terrain (c'est-à-dire, les actionneurs de vanne, les démarreurs de moteur et les relais) peuvent généralement être actionnés directement sur le terrain sans signaux de commande sur le réseau IACS. Il peut être prohibitif en termes de coûts de protéger chaque dispositif de terrain individuellement. C'est pourquoi des procédures strictes d'accès au périmètre physique sont généralement nécessaires dans des installations qui présentent un risque élevé.

La liste suivante contient des éléments qu'il convient de prendre en compte lors de la création d'un environnement sécurisé pour la protection d'actifs tangibles contre les dommages physiques dus à une intrusion physique ou aux conditions environnementales.

#### A.3.3.3.2.2 Politique de sécurité

Une politique de sécurité écrite contient des directives qui définissent comment une organisation définit la sécurité, met en pratique son programme de sécurité et examine son programme afin d'apporter des améliorations. Ces politiques écrites permettent au personnel de comprendre clairement leurs rôles et responsabilités dans la sécurisation des actifs de l'organisation. L'organisation doit établir une politique de sécurité physique et environnementale qui est complémentaire de la politique de cyber-sécurité de l'organisation et de sa politique de sécurité physique. L'objectif primaire est de combler les brèches qui peuvent exister entre ces deux politiques. Il convient que la politique de sécurité physique et environnementale soit cohérente et applique les mêmes politiques, comme décrit précédemment, que d'autres politiques de sécurité concernant la sécurité du système de commande. Une évaluation détaillée des risques de sécurité physique est utilisée pour déterminer les procédures de sécurité physique appropriées à mettre en œuvre.

#### A.3.3.3.2.3 Périmètre de sécurité

Il convient de placer les informations ou actifs critiques en lieu sûr protégé par des périmètres de sécurité des commandes d'entrée. Ces commandes de sécurité physique fonctionnent conjointement avec des mesures de cyber-sécurité pour protéger les informations. Il convient d'établir un ou plusieurs périmètres de sécurité physique pour former des barrières contre un accès non autorisé aux installations. Des périmètres multiples peuvent être imbriqués afin de produire des contrôles successifs de plus en plus stricts. Un exemple peut être une armoire verrouillée à l'intérieur d'une salle de commande avec accès par une carte-clé dans une installation avec une clôture de périmètre protégée.

#### A.3.3.3.2.4 Contrôles des entrées

Au niveau de chaque barrière ou limite, il convient de disposer des contrôles d'entrée appropriés. Ces contrôles d'entrée peuvent être des grilles verrouillées, des portes avec des verrous ou des protections appropriés. Il convient que les contrôles d'entrée soient appropriés pour le niveau de sécurité requis dans le secteur sécurisé par les contrôles d'entrée et adaptés au besoin d'accès rapide.

#### A.3.3.3.2.5 Protection contre les dommages environnementaux

Les actifs doivent être protégés contre les dommages environnementaux dus aux menaces telles que les incendies, la fumée, les poussières, les rayonnements et les chocs. Il convient d'apporter une attention particulière aux systèmes de protection contre les incendies utilisés dans les zones affectant les IACS afin de veiller à ce que les systèmes responsables de la protection des installations assurent une protection des dispositifs IACS sans introduire un risque additionnel pour les opérations industrielles.

#### A.3.3.3.2.6 Procédures de sécurité

Il doit être exigé que le personnel suive et applique les procédures de sécurité physique qui ont été établies pour renforcer les contrôles d'entrée et autres contrôles physiques. Il convient que le personnel ne contourne aucun des contrôles d'entrée automatiques et autres contrôles physiques. Un exemple d'employé contournant un contrôle physique consisterait à maintenir une porte de contrôle protégée à l'aide d'une chaise.

#### A.3.3.3.2.7 Points de défaillance unique

Il convient d'éviter les points de défaillance unique dans la mesure du possible. Des systèmes redondants constituent une option plus robuste qui est en mesure d'empêcher des incidents légers d'affecter l'usine ou l'organisation, par exemple, l'utilisation d'une alimentation électrique redondante dans un système critique afin de garantir que si une alimentation électrique est endommagée, le système critique reste fonctionnel.

#### A.3.3.3.2.8 Connexions

Il convient que toutes les connexions (c'est-à-dire, l'alimentation et les communications, comprenant le câblage des commandes E/S, le câblage du bus E/S, les câbles réseau, les câbles de connexion inter-contrôleur, les modems, et autres) sous le contrôle de l'organisation soient protégées de manière appropriée contre les altérations ou les dommages. Cela peut comprendre l'installation des connexions dans des armoires fermées ou dans des enceintes clôturées. Il convient que le niveau de sécurité physique pour ces connexions soit proportionnel au niveau de sécurité pour les systèmes auxquels elles sont reliées. Il convient que, compte tenu de la sécurité physique, les conséquences des dommages environnementaux soient prises en compte. Il convient que ces connexions soient également protégées contre des facteurs naturels tels que la chaleur, les incendies, les poussières, et autres qui peuvent causer des défaillances.

#### A.3.3.3.2.9 Maintenance des équipements

Il convient que tous les équipements comprenant des équipements environnementaux auxiliaires soient correctement maintenus pour assurer un fonctionnement correct. Il convient d'établir des programmes de maintenance et de conduire une maintenance préventive. Il convient que la maintenance des équipements soit suivie et les tendances analysées afin de déterminer s'il convient de modifier les programmes de maintenance.

#### A.3.3.3.2.10 Alarmes

Il convient que des procédures appropriées soient établies pour la surveillance et l'émission d'alarme lorsque la sécurité physique et environnementale est compromise. Il convient que le personnel soit amené à répondre à toutes les alarmes avec les mesures de réponse appropriées. Il convient que toutes les installations, proportionnellement à leur niveau de sécurité, soient équipées d'alarmes en cas d'intrusion physique et environnementale. Celles-ci peuvent comprendre des détecteurs de mouvement, des caméras ou des alarmes de porte pour les intrusions physiques et des alarmes d'incendie, des détecteurs d'eau ou des capteurs de température pour des problèmes environnementaux.

#### A.3.3.3.2.11 Cycle de vie d'équipement

Il convient que des procédures appropriées soient établies et auditées en ce qui concerne l'ajout, le retrait et l'élimination de tout équipement. Le suivi approprié des actifs est une bonne pratique. Ces procédures comprendraient l'élimination du poste de travail, le formatage, le nettoyage de disque, et autres. L'approvisionnement de matériel prendrait en compte la manière dont l'équipement peut être suivi et dont il peut être décontaminé et éliminé lorsqu'il n'est plus nécessaire.

#### A.3.3.3.2.12 Informations physiques

Toutes les informations, exprimées sous une forme physique (c'est-à-dire, des documents écrits ou imprimés, des supports de stockage magnétique et des disques compacts), doivent être protégées de manière appropriée contre les menaces physiques. Cela peut comprendre la mise en place de ces éléments dans des salles ou des armoires verrouillées pour éviter tout accès non autorisé. Il convient de prendre en compte la protection des informations contre les dommages environnementaux tels que des champs magnétiques, une humidité élevée, la chaleur ou l'ensoleillement direct, et autres qui peuvent endommager les informations. Comme pour ces équipements, il convient de mettre en place des procédures pour l'élimination sécurisée des supports physiques lorsqu'ils ne sont plus nécessaires.

#### A.3.3.3.2.13 Utilisation d'actifs à l'extérieur d'environnements contrôlés

Il convient de prendre un soin particulier à l'utilisation d'actifs qui affectent l'IACS à l'extérieur du réseau IACS. Cela comprend le transfert des actifs au niveau des installations d'un intégrateur de système avant installation. De plus, il convient que les actifs tels que des ordinateurs portables ayant accès au réseau IACS utilisés hors site soient manipulés comme une extension du réseau IACS, toutes les procédures physiques et environnementales appropriées étant suivies. Il convient de veiller à utiliser le même niveau de sécurité pour les actifs qui sont temporairement à l'extérieur des limites de sécurité normales. Cela peut nécessiter une planification ou des installations spéciales pour protéger ces actifs contre les accès ou utilisations non autorisés ou contre les dommages environnementaux.

#### A.3.3.3.2.14 Protection intermédiaire des actifs critiques

Pendant et après un événement physique ou environnemental, l'alimentation électrique ou un autre service peut être interrompu pour des systèmes critiques. Il convient de prendre des dispositions pour assurer une protection de ces systèmes critiques. Cela peut comprendre des mesures telles qu'une alimentation électrique de secours, une couverture ou un barrage pour éviter des dégâts des eaux, et autres.

### A.3.3.3.3 Pratiques en support

#### A.3.3.3.3.1 Pratiques de base

Les neuf actions suivantes sont des pratiques de base:

a) Établir des périmètres de sécurité physique pour former des barrières contre un accès non autorisé aux installations. Au niveau de chaque barrière ou limite, des contrôles d'entrée appropriés sont disposés.

b) Protéger les actifs contre les dommages environnementaux dus à des menaces telles que les incendies, l'eau, la fumée, les poussières, les rayonnements et les chocs.

c) Imposer au personnel de suivre et appliquer les procédures de sécurité physique qui ont été établies pour renforcer les contrôles d'entrée et autres contrôles physiques.

d) Exiger des sources d'alimentation redondantes afin d'éviter les points de défaillance unique.

e) Assurer une protection contre les altérations ou dommages par l'intermédiaire de connexions externes.

f) Maintenir tous les équipements, comprenant les équipements environnementaux auxiliaires, de manière à assurer leur fonctionnement correct.

g) Établir des procédures de surveillance et d'alarme lorsque la sécurité physique et/ou environnementale est compromise.

h) Établir et auditer des procédures relatives à l'ajout, au retrait et à l'élimination de tous les actifs.

i) Utiliser des procédures spéciales pour sécuriser les actifs affectant l'IACS à l'extérieur du réseau IACS.

#### A.3.3.3.3.2 Pratiques additionnelles

Les sept actions suivantes sont des pratiques additionnelles:

a) Utiliser des câbles de sécurité, des armoires verrouillées, des entrées protégées au bureau ou à domicile, maintenir l'équipement hors de vue et étiqueter et marquer les actifs.

b) Utiliser des mot de passe pour les commandes de démarrage et de connexion sur les ordinateurs qui ne sont pas dans la salle de commande, un système de fichiers cryptés, des ordinateurs utilisant des techniques de client léger, et autres.

c) Protéger l'équipement informatique hors des salles de commande, tel que les routeurs ou un pare-feu en plaçant ceux-ci dans un environnement verrouillé.

d) Veiller à ce que du personnel soit présent en permanence dans les salles de commande. Cela peut souvent être la première ligne de défense de protection physique. Utiliser les salles de commande pour loger des actifs de types informations et technologiques.

e) Demander au personnel de retourner tout équipement en bon état de fonctionnement lorsqu'il quitte l'organisation.

f) Utiliser un système de suivi des équipements afin de déterminer où un équipement est situé et qui en a la responsabilité.

g) Imposer une protection environnementale pour les actifs comprenant un logement approprié pour un équipement qui est situé à un emplacement où il pourrait être exposé à des poussières, des températures extrêmes, l'humidité, et autres.

#### A.3.3.3.4 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [2], [23], [27], [31].

### A.3.3.4 Élément – Segmentation de réseau

#### A.3.3.4.1 Description de l'élément

La segmentation de réseau implique la séparation des actifs IACS clés dans des zones ayant des niveaux de sécurité communs afin de gérer les risques de sécurité en vue d'obtenir un niveau de sécurité cible souhaité pour la zone. La segmentation de réseau est une contre-mesure de sécurité importante utilisée conjointement avec d'autres couches de défense afin de réduire le risque qui peut être associé à l'IACS.

Les IACS actuels sont connectés et intégrés à des systèmes de gestion dans et entre des entreprises partenaires. Malgré le besoin de connectivité et d'intégration étroite, les IACS ne requièrent pas l'utilisation de la grande majorité des réseaux d'entreprise accédant aux données. L'exposition des dispositifs IACS à l'ensemble de ce trafic augmente la vraisemblance d'un incident de sécurité dans l'IACS. Conformément au principe du droit d'accès minimal et du besoin de connaître, il convient que l'IACS soit structuré de manière à filtrer/éliminer les flots de communication superflus pour leur empêcher d'atteindre les dispositifs IACS. La segmentation de réseau est conçue pour compartimenter les dispositifs en zones de sécurité communes dans lesquelles des pratiques de sécurité identifiées sont utilisées pour obtenir le niveau de sécurité cible souhaité. L'objectif est de réduire au minimum la vraisemblance qu'un incident de sécurité compromette le comportement fonctionnel de l'IACS. L'association de dispositifs en zones ne signifie pas nécessairement qu'ils sont isolés. Des conduits relient les zones de sécurité et permettent le transport des communications nécessaires entre les zones de sécurité segmentées.

L'utilisation de contre-mesures de sécurité doit être proportionnelle au niveau de risque et il convient que ce principe de sécurité l'emporte sur tous les autres. La segmentation de réseau d'un IACS peut ne pas être nécessaire si les risques de sécurité sont faibles. L'élément de gestion des risques et de mise en œuvre fournit des informations additionnelles concernant la gestion des risques. Il convient de l'examiner avant de mettre en œuvre une stratégie de contre-mesure de segmentation de réseau décrite dans cet élément du CSMS.

#### A.3.3.4.2 Segments et zones de réseau

##### A.3.3.4.2.1 Généralités

La CEI/TS 62443-1-1, Article 6 introduit des modèles de référence et donne le contexte pour examiner cette contre-mesure. Des réseaux sont segmentés par l'utilisation d'un type de dispositif de barrière qui a la capacité de contrôler ce qui traverse le dispositif. Sur les réseaux basés sur Ethernet exécutant TCP/IP, les dispositifs de barrière les plus couramment utilisés sont des pare-feu, des routeurs et des commutateurs de niveau 3. Les IACS sont fréquemment constitués de plusieurs réseaux différents utilisant différentes technologies de couche physique et applicative. Ces réseaux non-TCP/IP utilisent également des dispositifs de barrière pour séparer et segmenter des communications. Les dispositifs de barrière peuvent être des passerelles autonomes ou bien intégrés dans le module d'interface de réseau d'un dispositif IACS.

Bien que le placement d'un dispositif de barrière dans le réseau puisse créer un nouveau segment de réseau et une nouvelle zone de sécurité, une zone de sécurité peut également couvrir des segments de réseau multiples. La Figure A.8 ci-dessous illustre une possible architecture segmentée pour un IACS générique. Cette figure tente de décrire comment des niveaux d'équipement fonctionnel peuvent se traduire en réalité physique pour un IACS et en monde logique d'une zone. (La figure est d'un niveau relativement haut et ne comprend pas tous les dispositifs de réseau requis dans une installation réelle.)

Il est important de ne pas confondre les niveaux fonctionnels du modèle de référence avec les niveaux de sécurité associés aux zones de sécurité. Bien qu'il soit généralement vrai que l'équipement de niveau inférieur joue un rôle plus important dans le fonctionnement sûr des systèmes industriels automatisés, il peut ne pas être pratique ou possible d'utiliser une stratégie de segmentation par alignement unàun avec les niveaux d'équipement.

Sur cette figure, la zone de commande contient un équipement ayant un niveau commun de sécurité cible. La figure représente un segment de réseau de commande de processus (*process control network*: PCN) basé sur TCP/IP, un segment de réseau de commande réglementaire (*regulatory control network*: RCN) propriétaire et un segment de réseau de dispositif de terrain (*field device network*: FDN) propriétaire. Ces réseaux relient les équipements de niveau 0, 1, 2 et 3 représentés dans les modèles de référence de la CEI/TS 62443-1-1, 5.2. Les dispositifs de barrière pour chacun de ces segments de réseau régulent les communications entrant et quittant leur segment.

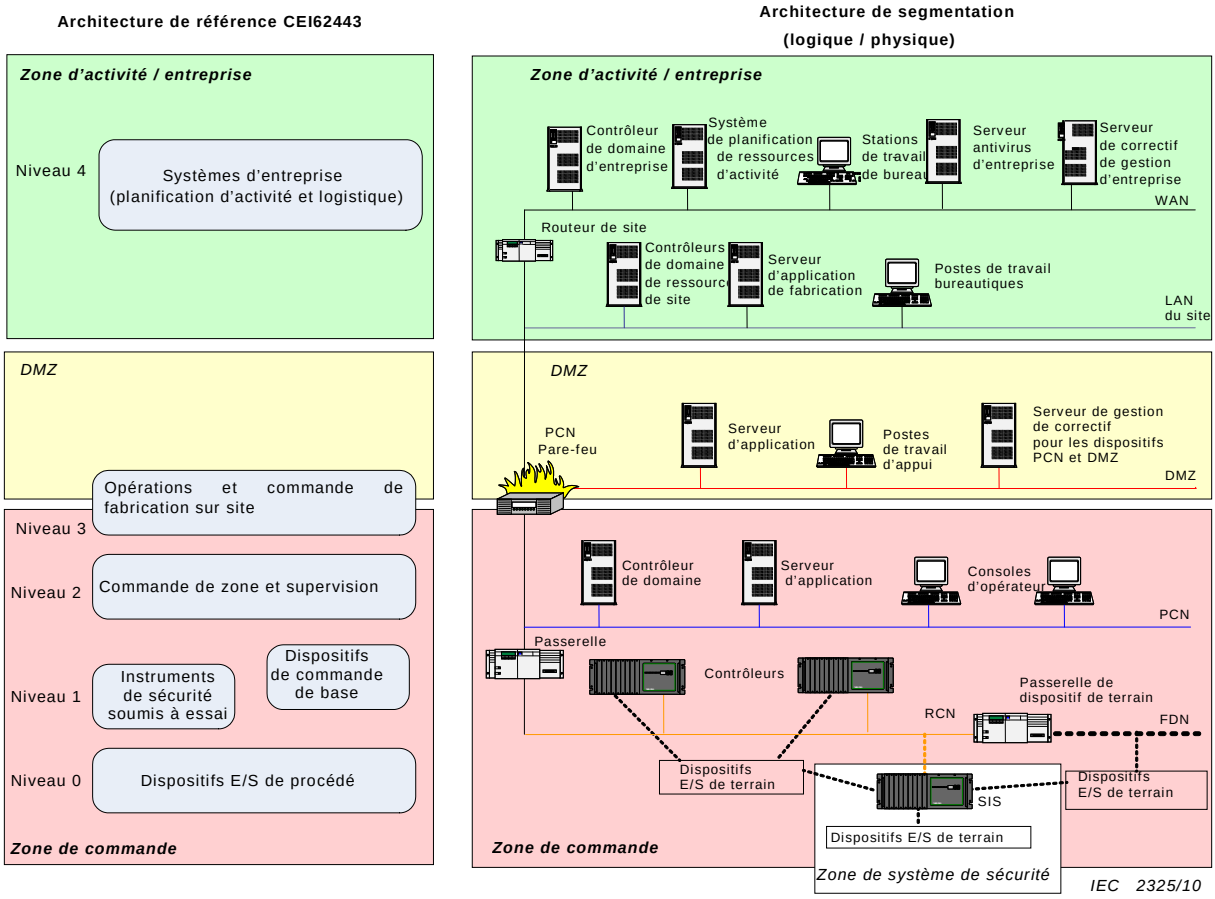



**Figure A.8 – Alignement d'une architecture de référence avec un exemple d'architecture segmentée**

### A.3.3.4.2.2 Zone de commande

Pour un IACS à faible risque, il peut ne pas être nécessaire d'utiliser une segmentation de réseau en tant que contre-mesure, qui nécessiterait la création d'une zone de commande distincte. Cependant, pour un IACS à haut risque, la segmentation de réseau est une contre-mesure produisant une réduction très significative des risques.

La bonne pratique généralement acceptée consiste à utiliser un dispositif de barrière tel qu'un pare-feu pour gérer les communications de part et d'autre du conduit qui relie la zone de commande à la zone d'activité, comme décrit à la Figure A.8.

Des stratégies de filtrage communes au niveau du dispositif de barrière sont décrites ci-dessous:

a) Il convient que la configuration de base du dispositif *rejette toute* communication par défaut et autorise uniquement les communications par exception pour satisfaire à un besoin d'activité critique. Cela s'applique à des communications d'utilisateur interactives, intermittentes de part et d'autre du conduit et des communications continues, de tâche à tâche entre des dispositifs dans ces deux zones. Dans la mesure du possible, il convient de filtrer les communications par ports et services entre des paires IP appairées pour les dispositifs communiquant via le conduit.

b) Il convient de ne pas ouvrir par l'intermédiaire du dispositif de barrière les ports et services fréquemment utilisés en tant que vecteurs d'attaque. Lorsque le service est requis en raison d'une justification économique, il convient d'utiliser des contre-mesures afin de compenser le risque. À titre d'exemple, un http entrant, qui est un vecteur d'attaque commun, peut être nécessaire pour prendre en charge une fonction d'activité

importante. Des contre-mesures de compensation additionnelles telles que des scripts bloquant les entrées et l'utilisation d'un serveur proxy http contribueraient à diminuer le risque d'ouvrir ces ports et services à haut risque.

c) Il est préférable que le nombre de ports et services ouverts par l'intermédiaire du dispositif de barrière soit aussi faible que possible. Il convient d'éviter des technologies de communication qui requièrent l'ouverture d'un grand nombre de ports.

Le dispositif de barrière peut être un bon outil automatisé pour imposer l'application des pratiques de sécurité dans la zone de commande, telles que le rejet des courriers électroniques ou des communications vers/depuis Internet.

#### A.3.3.4.2.3 Zone démilitarisée (DMZ)

Pour un IACS à haut risque, l'utilisation d'une DMZ conjointement avec une zone de commande offre des opportunités additionnelles de réduction des risques entre la zone d'activité à bas niveau de sécurité et la zone de commande à haut niveau de sécurité. Le niveau de sécurité pour la DMZ est plus élevé que la zone d'activité mais plus bas que la zone de commande. La fonction de cette zone est d'éliminer ou fortement réduire toute communication directe entre la zone de commande et la zone d'activité.

Il convient de localiser les dispositifs dans la DMZ qui fonctionne comme un pont ou un tampon entre dispositifs dans la zone d'activité et la zone de commande. La communication est configurée entre un dispositif dans la zone d'activité et la DMZ. Le dispositif dans la DMZ transmet ensuite les informations au dispositif receveur dans la zone de commande. Idéalement, les ports et services utilisés entre le dispositif dans la zone d'activité et la DMZ sont différents des ports et services utilisés entre le dispositif DMZ et le dispositif de zone de commande de destination. Cela réduit la vraisemblance qu'un code malveillant ou un intrus soit en mesure de négocier une communication par l'intermédiaire des conduits combinés reliant la zone d'activité à la zone de commande.

Les stratégies de filtration énumérées ci-dessus pour la zone de commande sont également applicables pour la DMZ. Cependant, certains protocoles à plus haut niveau de risque tels que Telnet peuvent être tolérés pour permettre la gestion de dispositifs dans la DMZ et les zones de commande.

Dans plusieurs cas d'utilisation, une DMZ peut être bénéfique. Ceux-ci ont été présentement inclus afin d'illustrer les concepts de sécurité. Ils ne sont pas destinés à constituer une liste exhaustive ou détaillée de modes de mise en œuvre d'une DMZ:

a) Réduction au minimum des personnes accédant directement à des dispositifs de zone de commande.

   Des serveurs d'historisation sont souvent accédés par des personnes situées sur le réseau local du site dans la zone d'activité. Plutôt que de localiser le serveur d'historisation dans la zone de commande et permettre un accès direct à ce dispositif depuis la zone d'activité par un grand nombre d'utilisateurs, le niveau de sécurité de la zone de commande peut être maintenu à un niveau plus haut si le serveur d'historisation est situé dans la DMZ.

b) Améliorer la sécurité pour les dispositifs IACS importants.

   Dans le cas du serveur d'historisation mentionné ci-dessus, une option consisterait à situer le serveur d'historisation sur le réseau local du site dans lequel la majorité des utilisateurs sont situés. Cela diminuerait le nombre de personnes ayant besoin d'accéder au PCN. Cependant, étant donné que la zone d'activité est une zone à niveau de sécurité faible, le serveur d'historisation serait soumis à un environnement moins sûr. Le risque pour le serveur serait plus important.

c) Compensation des délais de correction de programme.

   La DMZ permet une protection de sécurité additionnelle pour des dispositifs IACS importants qui ne peuvent pas être corrigés rapidement dans l'attente de résultats d'essai de compatibilité de correctif du fournisseur d'application.

d) Amélioration de la sécurité de la zone de commande par migration des dispositifs de gestion à un niveau de sécurité supérieur.

La DMZ est un emplacement approprié pour localiser des dispositifs tels que des serveurs antivirus et des serveurs de gestion de correctifs. Ces dispositifs peuvent être utilisés pour gérer le déploiement de modules de sécurité au niveau des dispositifs de zone de commande et DMZ d'une manière plus contrôlée sans soumettre la zone de commande à haut niveau de sécurité pour diriger la connexion à des serveurs qui peuvent communiquer avec des centaines de dispositifs.

#### A.3.3.4.2.4 Zone de système de sécurité

Certains IACS peuvent utiliser un ensemble de verrous de sécurité qui sont à base de relais ou à base de microprocesseur. Un solveur logique SIS à base de microprocesseur peut nécessiter un ensemble de pratiques de sécurité légèrement différent de celui utilisé dans la zone de commande. Il convient de déterminer le niveau de sécurité cible pour cette zone et de prendre les mesures appropriées pour assurer que des contre-mesures adaptées sont utilisées pour satisfaire au niveau de sécurité cible.

#### A.3.3.4.2.5 IACS isolés

Le risque associé à l'IACS peut être trop élevé pour tolérer une opportunité d'intrusion par un agent externe. Une installation peut choisir de déconnecter tous les conduits entre la zone de commande et une autre zone. Cette stratégie de segmentation de réseau peut être particulièrement adaptée.

Certaines installations adoptant cette approche d'isolation n'éliminent pas automatiquement tous les risques. Il peut rester encore une vulnérabilité importante susceptible d'être exploitée localement. Il convient d'utiliser des couches appropriées de protection de cyber-sécurité et physique pour gérer le risque résiduel après isolation de l'IACS vis-à-vis de la zone d'activité.

### A.3.3.4.3 Architecture de segmentation SCADA

La description ci-dessus concerne une architecture segmentée pour un IACS typique dans une installation à opération unique. La segmentation est une contre-mesure qui a une applicabilité égale pour un IACS de type SCADA. La Figure A.9 illustre une approche de segmentation possible pour ce type d'architecture. Bien que cela ne soit pas décrit en raison de contraintes d'espace, la DMZ et la zone de système de sécurité décrite dans l'IACS d'installation à opération unique peuvent également être utilisées dans une architecture SCADA.

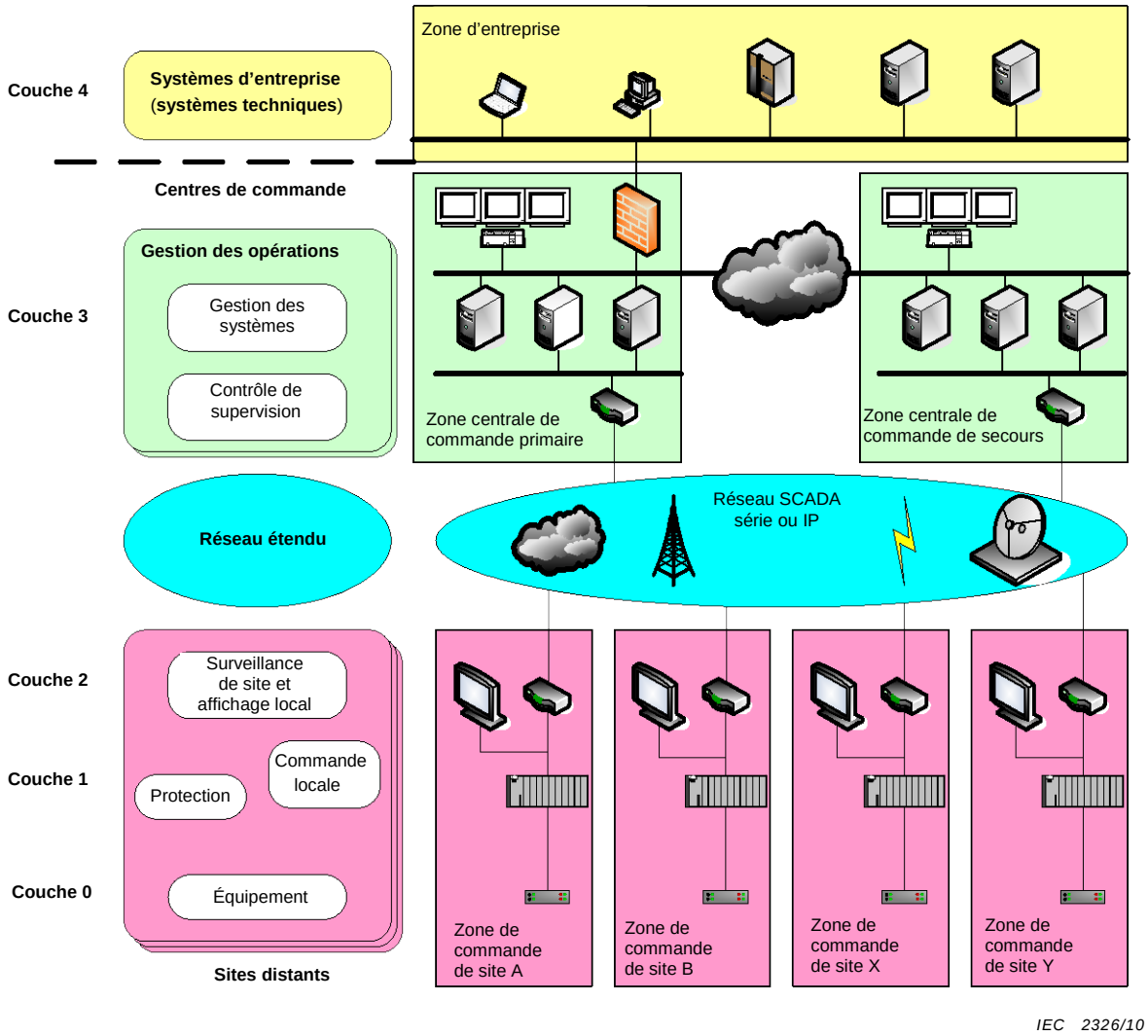



**Figure A.9 – Alignement d'une architecture SCADA de référence avec un exemple d'architecture segmentée**

### A.3.3.4.4 Pratiques suggérées

#### A.3.3.4.4.1 Pratiques de base

Les quatre actions suivantes sont des pratiques de base:

a) Utiliser des dispositifs de barrière tels que des pare-feu pour segmenter des dispositifs IACS à haut risque dans des zones de commande.

b) Utiliser des passerelles ou des dispositifs de barrière internes dans le dispositif IACS pour séparer des réseaux de commande réglementaire du PCN.

c) Utiliser des pratiques robustes de gestion des modifications pour la configuration de dispositif de barrière.

d) Déconnecter l'IACS à haut risque de la zone d'activité.

#### A.3.3.4.4.2 Pratiques additionnelles

Les quatre actions suivantes sont des pratiques additionnelles:

a) Utiliser des dispositifs de barrière complémentaires additionnels dans la zone de commande afin de segmenter plus avant le réseau.

b) Utiliser un profil de sécurité commun et à gestion centralisée pour tous les dispositifs de barrière de zone de commande.

c) Utiliser une architecture de segmentation de DMZ.

d) Effectuer des essais d'évaluation automatisés pour vérifier que la configuration de dispositif de barrière a été correctement mise en œuvre conformément à la spécification de conception.

#### A.3.3.4.5 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans la référence suivante, qui est répertoriée dans la Bibliographie: [1].

### A.3.3.5 Élément: Contrôle d'accès: Administration des comptes

#### A.3.3.5.1 Description générale de contrôle d'accès

Le contrôle d'accès est la méthode permettant de contrôler qui ou quelles ressources peuvent accéder aux locaux et aux systèmes et quel type d'accès est accordé. Une mauvaise utilisation des données et des systèmes peut avoir des conséquences graves, telles qu'un danger pour la vie humaine, des dommages dans l'environnement, des pertes financières et une dégradation de la réputation de l'entreprise. Ces risques augmentent si le personnel a des droits d'accès indus aux données et aux systèmes. Il est très important que la politique de sécurité qui définit les règles de contrôle d'accès et procédures soit clairement documentée et communiquée à l'ensemble du personnel (c'est-à-dire, les employés, les coentreprises, les sous-traitants et les employés temporaires).

Un des éléments de sécurité les plus importants pour un système informatique quelconque est un ensemble cohérent et approprié de procédures de contrôle d'accès. Il existe trois aspects clés associés au contrôle d'accès: l'administration des comptes, l'authentification et l'autorisation.

Chacun de ceux-ci est décrit séparément dans le paragraphe d'élément correspondant de la présente norme. Cependant, les trois aspects doivent être mis en œuvre conjointement pour établir une stratégie de contrôle d'accès cohérente et fiable.

Dans chacun des trois aspects de contrôle d'accès, il convient d'établir des règles pour confirmer que l'accès d'un utilisateur à des systèmes et des données est contrôlé. Il convient que les règles soient généralement appliquées à des rôles ou des groupes d'utilisateurs. Il convient que les utilisateurs aient accès aux systèmes et données qui sont requis pour satisfaire aux exigences de l'activité mais n'aient pas un tel accès si celui-ci n'a pas d'utilité définie pour celle-ci.

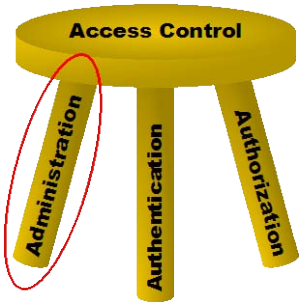
Certaines règles sont appliquées de façon administrative et d'autres sont appliquées automatiquement par utilisation de la technologie. Les deux types de règles doivent être gérés comme faisant partie de la stratégie globale de contrôle d'accès. Un exemple de règle administrative qu'une organisation peut mettre en œuvre est la suppression de comptes d'employés ou de sous-traitant après avoir quitté l'organisation. Un exemple de règle imposée par la technologie consiste à exiger que des utilisateurs distants se connectent au réseau d'entreprise pour utiliser un VPN.

En plus des règles, des procédures de sécurité physique et des procédures de cyber-sécurité sont mises en œuvre conjointement pour établir le cadre de sécurité global pour le système. Les procédures de sécurité physique comprennent des mesures telles que le verrouillage des locaux dans lesquels l'équipement d'interface utilisateur est situé. La présente norme présente une description de base des domaines de la sécurité physique qui concernent la cyber-sécurité dans A.3.3.3.

Le contrôle d'accès comporte un aspect en temps réel et un aspect hors connexion. Très souvent, une attention insuffisante est accordée aux activités hors connexion du contrôle

d'accès pour l'IACS. L'activité hors connexion, présentement décrite dans Administration des comptes, est la première étape dans le processus et comprend la définition des droits d'utilisateur et des besoins de ressources pour l'utilisateur. Ceux-ci sont basés sur le rôle de l'utilisateur et la tâche à effectuer. Le processus hors connexion comprend en outre une étape d'approbation par une partie responsable avant que le compte d'accès soit configuré pour permettre l'accès approprié.

#### A.3.3.5.2 Description de l'élément




**Légende**

| Anglais | Français |
|---|---|
| Access control | Contrôle d'accès |
| Administration | Administration |
| Authentication | Authentification |
| Authorization | Autorisation |

**Figure A.10 – Contrôle d'accès: Administration des comptes**

L'administration des comptes, un des trois piliers du contrôle des accès comme décrit sur la Figure A.10, est la méthode utilisée dans la configuration initiale des autorisations et des droits pour accéder à des ressources spécifiques sur le réseau ou système et pour examiner ces autorisations et droits d'accès sur une base périodique. Elle peut être liée d'une certaine façon à l'accès physique aux ressources. L'administration des comptes dans l'environnement IACS dépasse la définition IT conventionnelle de l'accès à un compte de système d'exploitation pour un utilisateur particulier. Dans l'environnement IACS, les comptes d'accès sont plus à base de rôle pour les fonctions qu'ils peuvent effectuer sur une machine particulière que pour les données auxquelles ils peuvent accéder. Un rôle d'utilisateur peut changer au cours du temps dans une organisation. C'est pourquoi le processus d'administration peut être utilisé plus fréquemment sur des comptes IACS. Les droits d'accès comprennent souvent l'accès à des répertoires de fichiers, des heures d'accès et une quantité d'espace de stockage allouée. Le rôle attribué au niveau application pour le compte d'accès doit être identifié et compris au cours de la phase d'administration. Plusieurs étapes sont impliquées, comprenant l'identification des ressources nécessaires pour remplir la fonction de la personne, l'approbation indépendante par une personne de confiance et la configuration du compte informatique qui assigne automatiquement les ressources à la demande.

En plus de la tâche de création de comptes d'accès et l'assignation d'utilisateurs à des rôles au niveau du système d'exploitation, de nombreuses applications de fabrication requièrent des attributions de rôles additionnels. Les administrateurs système pour un IACS doivent être formés et aptes à remplir ces fonctions d'administration de compte sur des applications de commande d'équipement en temps réel. Il convient que le processus de gestion des changements pour effectuer ces modifications de compte spécifie clairement les contraintes temporelles qui doivent être respectées en raison des risques de sécurité au cours de certaines séquences de l'opération de commande.

#### A.3.3.5.3 Considérations relatives à l'administration des comptes

##### A.3.3.5.3.1 Généralités

Lors du développement d'un programme pour l'administration des comptes, il est important d'inclure tous les systèmes dans le domaine d'application et de ne pas limiter l'effort aux seules installations conventionnelles de salle informatique.

##### A.3.3.5.3.2 Règles de contrôle de l'accès d'un utilisateur à des systèmes, des données et des fonctions spécifiques

Il convient que chaque organisation établisse des règles pour contrôler l'accès d'un utilisateur aux systèmes, données et fonctions. Il convient que ces règles soient basées sur le risque pour le système et la valeur des informations. Il convient de communiquer ces règles à l'ensemble du personnel.

##### A.3.3.5.3.3 Processus d'administration normalisé

Il convient d'appliquer un processus d'administration normalisé pour la création de comptes d'accès. Bien qu'il puisse être plus économique pour une organisation individuelle de gérer la fonction d'administration des comptes pour l'ensemble des systèmes informatiques dans une entreprise, les fonctions administratives de contrôle de la création de compte et du processus de maintenance peuvent être remplies par des groupes de personnes différents pour les systèmes IACS et IT. Cela est souvent dû au fait que les ensembles de risques associés à ces systèmes sont différents. Les approbations de compte peuvent également nécessiter une approbation par un superviseur familiarisé avec les tâches et opérations IACS.

##### A.3.3.5.3.4 Comptes d'accès à base de rôle

Il convient d'appliquer un processus d'administration normalisé pour la création de comptes d'accès. Il convient que les comptes soient à base de rôle et accordent à l'utilisateur uniquement les privilèges et droits d'accès aux ressources qui sont nécessaires pour remplir leur fonction particulière dans leur poste.

##### A.3.3.5.3.5 Droits minimaux

Il convient d'attribuer aux utilisateurs les droits et autorisations minimaux qui sont nécessaires pour effectuer leurs tâches. Il convient d'accorder les droits sur la base des besoins pour soutenir les fonctions d'un poste particulier. Il convient que les droits à base de rôle tiennent compte des exigences spéciales pour installer des logiciels, des exigences pour configurer des services, des besoins de partage de fichiers et des besoins d'accès à distance.

##### A.3.3.5.3.6 Séparation des fonctions

Le processus d'administration des comptes comprend les principes de séparation des fonctions avec des approbateurs et des implémenteurs distincts pour la configuration des comptes. Ce principe ajoute une couche de protection additionnelle afin qu'une personne seule ne puisse pas altérer un système.

##### A.3.3.5.3.7 Identification des personnes

Il convient que chaque utilisateur soit identifiable avec des comptes d'accès séparés sauf si des risques HSE sont associés à de tels comptes. Dans de tels cas, il convient d'utiliser d'autres contrôles de sécurité physique pour limiter les accès. L'accès doit être contrôlé par une méthode d'authentification appropriée (c'est-à-dire, un ID utilisateur et un mot de passe, des numéros d'identification personnelle (PIN) ou des jetons). Il convient de ne pas partager ces identifiants personnels sauf dans certaines situations spécifiques. Un cas particulier est une salle de commande dans laquelle les opérateurs travaillent en équipe. Dans cette situation, chaque membre de l'équipe de travail peut utiliser les mêmes identifiants (ce sujet est détaillé plus avant au A.3.3.6). Il convient qu'un autre processus d'identification existe en cas d'oubli d'un mot de passe.

#### A.3.3.5.3.8 Autorisation

Il convient d'accorder des accès sous l'autorité d'un responsable approprié (de l'entreprise responsable ou d'une organisation partenaire). Il convient que les approbations soient effectuées par des superviseurs familiarisés avec les tâches de fabrication/opérations et la formation spécifique qu'une personne a reçue pour le rôle.

#### A.3.3.5.3.9 Comptes d'accès non nécessaires

Les comptes d'accès sont les moyens de contrôler les accès au système, par conséquent, il est important que ces comptes soient désactivés, suspendus ou supprimés et les autorisations d'accès révoquées dès qu'ils ne sont plus nécessaires (par exemple, changement de poste, départ de l'employé, et autres). Il convient que le responsable approprié prenne cette mesure dès que possible une fois que le compte d'accès n'est plus nécessaire.

#### A.3.3.5.3.10 Examen des autorisations des comptes d'accès

La nécessité d'accéder à des systèmes critiques doit être explicitement reconfirmée périodiquement. Il convient d'examiner périodiquement tous les comptes d'accès créés afin de vérifier que les comptes sont encore utilisés, si leurs rôles et besoins d'accès sont encore corrects, que l'utilisateur est toujours autorisé et a uniquement les droits minimaux requis. Il convient de supprimer les comptes inactifs ou non nécessaires. Si un compte d'accès reste inutilisé pendant une durée prolongée, la nécessité de le conserver est explicitement confirmée par le propriétaire et le responsable du compte.

#### A.3.3.5.3.11 Enregistrement des comptes d'accès

Une des fonctions primaires de l'administration des comptes est l'enregistrement des comptes d'accès individuels. Il convient de maintenir à jour des enregistrements de tous les comptes d'accès, comprenant des détails sur la personne, ses autorisations et le responsable ayant accordé les droits.

#### A.3.3.5.3.12 Gestion des changements

Il convient que le processus de gestion des changements pour l'administration des comptes identifie clairement les contraintes temporelles qui doivent être respectées à cause des risques de sécurité que représentent des changements effectués pendant certaines séquences d'opérations industrielles. Ces changements sont traités avec autant d'importance que les changements de procédé, de logiciel et d'équipement. Il convient d'intégrer le processus d'administration des comptes d'accès aux procédures normalisées de gestion de la sécurité des procédés (PSM) et d'inclure des étapes d'approbation et de documentation. Les approbateurs de comptes d'accès pour les fonctions de fabrication/opérations peuvent être un ensemble de personnes différent des personnes qui approuvent les utilisateurs pour les systèmes IT. Il convient que des approbations soient effectuées par des superviseurs familiarisés avec les tâches de fabrication/opérations et la formation spécifique qu'une personne a reçue pour ce rôle.

#### A.3.3.5.3.13 Mots de passe par défaut

De nombreux systèmes de contrôle sont fournis avec des mots de passe par défaut qui sont utilisés pour installer initialement le système. Ces mots de passe de compte d'accès sont souvent largement connus ou facilement déterminés à partir de la littérature publiée ou d'autres sources. Il convient de les modifier immédiatement après la configuration et avant la connexion au système.

#### A.3.3.5.3.14 Audit de l'administration des comptes

Il convient de conduire des examens périodiques de la conformité des informations d'administration de compte d'accès. Cela garantit que les propriétaires des informations ou

documents sont conformes aux politiques, normes ou autres exigences appropriées définies par l'organisation.

#### A.3.3.5.4 Pratiques en support

##### A.3.3.5.4.1 Pratiques de base

Les neuf actions suivantes sont des pratiques de base:

a) Assigner les droits et autorisations minimaux aux utilisateurs appropriés pour effectuer leurs tâches. Il convient d'accorder des droits sur la base des besoins liés à une fonction particulière du poste.

b) Contrôler l'identification et l'accès pour chaque utilisateur individuel par une méthode d'authentification appropriée (par exemple, un ID utilisateur et un mot de passe). Ces identifiants personnels (c'est-à-dire, les mots de passe, les PIN et/ou les jetons) ne sont pas partagés sauf dans certaines situations spéciales.

c) Établir un autre processus d'identification en cas de perte des identifiants ou d'oubli d'un mot de passe.

d) Accorder, modifier ou supprimer l'accès sous l'autorité d'un responsable approprié (de l'organisation, l'organisation sous-traitante ou un tiers). Un enregistrement de l'ensemble des comptes d'accès est conservé, comprenant des détails concernant la personne, les autorisations, et le responsable ayant accordé les autorisations.

e) Suspendre ou supprimer tous les comptes d'accès et révoquer les autorisations dès qu'ils ne sont plus nécessaires (par exemple, un changement de poste).

f) Examiner tous les comptes d'accès établis de façon périodique afin de vérifier qu'ils sont encore utilisés et requièrent toujours l'accès à des systèmes critiques.

g) Reconfirmer le besoin des comptes d'accès avec le responsable approprié si les comptes sont inutilisés pendant une durée prolongée.

h) Exiger que les mots de passe par défaut soient immédiatement modifiés.

i) Exiger que l'ensemble du personnel (c'est-à-dire, les employés, les coentreprises, les sous-traitants, et les employés temporaires) s'engagent par écrit à se conformer à la politique de sécurité, comprenant les politiques de contrôle d'accès.

##### A.3.3.5.4.2 Pratiques additionnelles

Les cinq actions suivantes sont des pratiques additionnelles:

a) Utiliser des outils (c'est-à-dire, la configuration et la gestion d'identité) pour gérer le processus de création, suspension, et suppression des comptes d'accès. Un système de configuration gère également le flux d'approbation selon lequel le détenteur de l'activité approuve les accès, y compris les connexions. Il peut également automatiser le processus de création/suspension de compte sur les systèmes cibles.

b) Lier le processus d'administration des comptes au processus de ressources humaines de sorte que les changements des employés déclenchent des examens et des mises à jour des comptes d'accès.

c) Définir et documenter les rôles/droits d'utilisateur d'application (c'est-à-dire, les fonctions des postes correspondants aux rôles d'application et aux droits d'accès pour chaque rôle) par le propriétaire des informations de l'application ou son délégué.

d) Apporter une attention particulière aux utilisateurs ayant un accès privilégié (c'est-à-dire, des examens et des vérifications générales plus fréquents).

e) Permettre aux utilisateurs d'avoir plusieurs comptes d'accès, sur la base de leur poste-rôle particulier à un moment particulier. Une personne utiliserait un compte d'administrateur système pour effectuer une mise à jour d'application sur une machine particulière mais nécessiterait un compte d'accès d'opérateur pour exécuter et soumettre à essai l'application.

#### A.3.3.5.5 Ressources utilisées

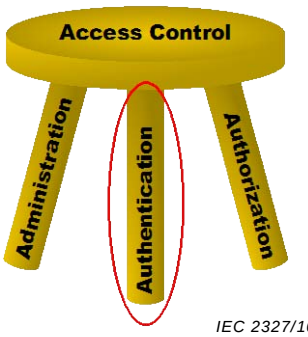
Cet élément est en partie basé sur le matériel décrit dans la référence suivante, qui est répertoriée dans la Bibliographie: [6].

### A.3.3.6 Élément: Contrôle d'accès: Authentification

#### A.3.3.6.1 Description de l'élément

NOTE Pour plus d'informations sur le sujet général du Contrôle d'accès, voir la section d'introduction au A.3.3.5.1.

L'authentification, un autre des trois piliers du contrôle d'accès comme décrit sur la Figure A.11, est la méthode d'identification formelle des utilisateurs du réseau, des hôtes, des applications, des services et des ressources pour toute transaction informatisée, de sorte que ceux-ci puissent disposer des droits et responsabilités autorisés appropriés. La méthode utilise une combinaison de facteurs d'identification ou identifiants. L'authentification est la condition préalable pour autoriser l'accès aux ressources dans un système.




IEC 2327/10

**Légende**

| Anglais | Français |
|---|---|
| Access control | Contrôle d'accès |
| Administration | Administration |
| Authentication | Authentification |
| Authorization | Autorisation |

**Figure A.11 – Contrôle d'accès: Authentification**

L'authentification dans l'environnement IACS comporte plusieurs défis qui ne sont généralement pas présents dans des situations IT normales. Les technologies d'authentification IT actuelles présentent plusieurs limitations qui ne sont pas adaptées à l'environnement IACS et pourraient en fait conduire à des risques HSE accrus au détriment d'une diminution des risques de cyber-sécurité.

Dans l'environnement IACS, il est important de veiller à ce que les personnes appropriées aient accès aux informations et aux systèmes adéquats et ne soient pas empêchées de remplir leurs fonctions par l'authentification. L'impossibilité d'authentifier un utilisateur valide peut avoir des implications HSE si l'utilisateur n'est pas en mesure d'effectuer des tâches dans une situation critique. Dans l'environnement IACS, l'accent est mis sur la combinaison des mesures d'authentification physiques avec des pratiques d'authentification électronique.

L'emplacement physique de l'utilisateur peut avoir un impact significatif sur le niveau de risque de l'accès. Par exemple, un utilisateur se connectant à un système depuis l'intérieur d'un bâtiment qui utilise un système de garde et de lecteur de badge à la porte présente un risque moins élevé de connexion que depuis une autre région du monde. La stratégie

d'authentification combine les contrôles de sécurité physique et de cyber-sécurité pour gérer le risque de contrôle global. La stratégie définit clairement les exigences d'authentification pour des situations spéciales.

Il existe plusieurs types de stratégies d'authentification, chacune étant plus ou moins forte. Les méthodes d'authentification fortes sont celles qui sont très précises dans l'identification formelle de l'utilisateur. Les méthodes d'authentification faibles sont celles qui peuvent être facilement contournées et permettre ainsi un accès indésirable à l'information.

L'emplacement physique de l'utilisateur peut avoir un impact significatif sur le risque d'accès à l'IACS. L'authentification pour ces cas est abordée dans les paragraphes suivants.

#### A.3.3.6.2 Authentification pour des utilisateurs locaux

Il est très important que seules des ressources formées et désignées puissent intervenir sur les stations IHM de commande industrielle, telles que les stations de commande d'opérateur. De nombreuses industries commandent leurs équipements depuis des salles de commande dans lesquelles plusieurs opérateurs sont postés. Ces opérateurs travaillent fréquemment en équipe et effectuent des actions sur des stations IHM multiples dans le cadre de leurs fonctions normales. Des comptes d'accès communs, partagés par l'équipe d'opérateurs sont fréquemment utilisés. Si les stations IHM n'intègrent pas des schémas d'authentification forts, robuste et économiques, la pratique recommandée est d'utiliser des contrôles physiques pour assurer que seuls des individus désignés effectuent des actions sur des stations IHM de salle de commande. Il convient de gérer l'accès aux salles de commande par des combinaisons appropriées de technologies de contrôle des entrées et de procédures administratives. Les implications HSE sont prises en compte dans le développement de procédures de contrôle d'accès.

#### A.3.3.6.3 Authentification pour des utilisateurs distants

Un utilisateur distant est toute personne qui est à l'extérieur du périmètre de la zone de sécurité concernée.

EXEMPLE Un utilisateur distant peut être une personne située dans un bureau du même bâtiment, une personne se connectant sur le réseau étendu (WAN) de l'entreprise et une personne se connectant sur des réseaux publics.

Les contrôles physiques et administratifs qui reposent sur une authentification visuelle ne fonctionnent pas pour les utilisateurs interactifs distants. Cependant, de nombreux schémas d'authentification basés sur des technologies peuvent être utilisés. Il est important d'utiliser un schéma d'authentification d'un niveau de force approprié pour identifier formellement l'utilisateur interactif distant. Les opérations industrielles ayant peu de chances de créer des incidents HSE et qui ont un faible impact financier peuvent être protégées en utilisant des méthodes d'authentification faibles telles que de simples ID utilisateur et mot de passe. Cependant, il convient de protéger les opérations industrielles à fort enjeu financier ou HSE à l'aide de technologies d'authentification forte. Pour ces types d'opérations, il est recommandé que le système soit conçu de telle manière que l'utilisateur distant ne soit pas autorisé à effectuer des fonctions de commande, mais uniquement des fonctions de surveillance.

#### A.3.3.6.4 Authentification pour la communication de tâche à tâche

La discussion ci-dessus concerne plus particulièrement les utilisateurs interactifs. Il est tout aussi important d'utiliser des schémas d'authentification appropriés pour la communication de tâche à tâche entre des serveurs d'application ou entre des serveurs et des dispositifs contrôlés. Il convient que l'interface de communication utilise des méthodes permettant de vérifier que le dispositif demandeur est bien le dispositif correct pour effectuer la tâche. Certaines méthodes utilisées par les interfaces critiques pour authentifier les communications de tâche à tâche entre des dispositifs vérifient l'adresse IP (Internet Protocol) et l'adresse MAC (Media Access Control), en utilisant un code secret ou en utilisant une clé de chiffrement afin de vérifier que la demande provient du dispositif prévu. Des interfaces à faible risque peuvent utiliser des méthodes d'authentification moins sécurisées. Un exemple de communications non sécurisées est un protocole de transfert de fichiers anonyme (FTP)

pour les transfert/téléchargement/comparaison de programmes entre une IHM de commande et un dépôt de données.

#### A.3.3.6.5 Considérations relatives à l'authentification

##### A.3.3.6.5.1 Généralités

Lors du développement d'un programme de contrôle d'accès, il est important d'inclure la totalité des systèmes dans le domaine d'application et de ne pas limiter l'effort aux installations d'une salle informatique traditionnelle.

a) Définir une stratégie d'authentification

   Il convient que les entreprises aient une stratégie d'authentification ou une approche pour définir la ou les méthodes d'authentification à utiliser.

b) Authentifier tous les utilisateurs avant l'utilisation du système

   Il convient que tous les utilisateurs soient authentifiés avant d'utiliser l'application demandée. Cette authentification peut être une combinaison de pratiques d'authentification physiques et informatiques.

c) Demander des comptes fortement sécurisés pour l'administration du système et/ou la configuration d'application

   Il convient d'utiliser des ID utilisateur et mot de passe robustes sur tous les comptes d'accès d'administration système et de configuration d'application. L'administrateur système ne requiert généralement pas l'accès à des tâches de niveau système sur les ordinateurs. Il est plus important d'empêcher des utilisateurs non formés d'utiliser des fonctions de niveau système que de permettre un accès rapide.

d) Exiger une administration locale

   Sur les systèmes très sensibles, une bonne pratique consiste à exécuter toutes les fonctions d'administration système ou de configuration d'appareil localement au niveau du dispositif afin de réduire le risque qu'une interruption du réseau cause un problème de commande de l'équipement. Il convient que l'administrateur système ou le gestionnaire d'applications coordonne tous les changements avec l'opérateur de la zone afin de ne pas affecter la production lors d'un changement de configuration.

##### A.3.3.6.5.2 Authentification pour des utilisateurs locaux

Si une pratique introduit un risque de retarder la capacité d'un opérateur à effectuer une action correctrice rapide au niveau des opérations industrielles depuis la station de commande IHM, les pratiques d'authentification IT normales peuvent être inadaptées. Afin d'assurer la sécurité dans le fonctionnement d'un système de commande tout en permettant une réponse rapide, il a été observé qu'une combinaison de contrôles physiques et informatiques donnent les meilleurs résultats. Certains de ces contrôles comprennent, mais ne sont pas limités à:

- des verrouillages manuels (par exemple, une clé et un code) sur les portes d'accès aux locaux ou armoires contenant des composants du système de commande;
- des verrouillages automatiques (par exemple, des lecteurs de badge et de carte);
- la présence permanente de personnel dans les salles de commande;
- la responsabilité individuelle du personnel de la salle de commande de maintenir un accès limité au personnel désigné et assurer que seul du personnel formé effectue des actions sur les stations de commande d'opérateur.

Certains exemples de pratiques IT courantes qui peuvent ne *pas* être applicables dans un environnement IACS sont:

a) ID utilisateur et mots de passe individuels pour chaque opérateur pour les environnements de travail posté

De nombreuses industries contrôlent leurs opérations depuis des salles de commande dans lesquelles sont postés plusieurs opérateurs. Ces opérateurs travaillent fréquemment en équipe et effectuent des actions sur des stations IHM multiples dans le cadre de leurs fonctions normales. Exiger que chaque opérateur se connecte et soit authentifié chaque fois qu'il utilise une nouvelle IHM pourrait compromettre la rapidité de réponse à un événement opérationnel.

b) Accès à des contrôleurs de domaine et des serveurs de répertoire actifs non locaux pour l'authentification des comptes d'accès

Dans cette architecture, des problèmes de réseau peuvent interférer avec une connexion en temps opportun.

c) Verrouillage automatique des comptes d'accès après un certain nombre de tentatives de connexion infructueuses

Dans certaines conditions nécessitant une réponse rapide d'un opérateur, l'opérateur peut être perturbé et entrer un mot de passe erroné. Si le compte de l'opérateur est bloqué, cela peut compromettre sa capacité à résoudre la situation.

d) Mots de passe longs et robustes contenant un mélange de caractères alphanumériques, numériques et spéciaux

Bien que des mots de passe robustes augmentent la sécurité, dans l'environnement de salle de commande, l'exigence d'entrer de tels mots de passe pourrait ralentir le temps de réponse d'un opérateur. Un niveau de sécurité similaire pourrait être obtenu par des moyens physiques tels que des portes verrouillées ou la présence constante de personnel dans la salle de commande qui connaît les opérateurs autorisés.

e) Changements de mot de passe après un nombre de jours spécifié

L'impact du changement régulier de mot de passe est très similaire à celui de mots de passe robustes. Il peut également ralentir la réponse à une situation nécessitant une réaction rapide. Il convient de modifier les mots de passe lors d'un changement de personnel, mais la modification du mot de passe après un nombre de jours défini peut être improductive.

f) Économiseurs d'écran avec protection par mot de passe

De nombreuses stations IHM sont conçues pour les rapports par exception. L'opérateur peut n'avoir aucune action à effectuer jusqu'à ce qu'une alerte soit générée. Les économiseurs d'écran risquent d'interférer avec l'action de l'opérateur en bloquant l'affichage de l'opération sous contrôle et retarder la réponse à une situation d'urgence.

#### A.3.3.6.5.3 Authentification pour des utilisateurs distants

Les utilisateurs distants n'ont normalement pas besoin de répondre rapidement à des situations communes aux opérateurs. De plus, pour les utilisateurs distants, la responsabilité devient plus importante que la disponibilité. Par conséquent, certaines pratiques communes pour la sécurité IT sont également bénéfiques pour les utilisateurs distants. Celles-ci comprennent:

a) Authentifier tous les utilisateurs distants au niveau approprié

Il convient que l'organisation utilise un schéma d'authentification avec un niveau de force approprié pour identifier formellement un utilisateur interactif distant.

b) Consigner et examiner toutes les tentatives d'accès aux systèmes critiques

Il convient que le système journalise toutes les tentatives d'accès aux systèmes critiques et que l'organisation examine ces tentatives lorsqu'elles échouent ou sont infructueuses.

c) Désactiver le compte d'accès après un certain nombre de tentatives de connexion infructueuses de la part d'un utilisateur *distant*

Après un certain nombre de tentatives de connexion infructueuses de la part d'un utilisateur *distant*, il convient que le système désactive le compte d'accès de l'utilisateur pendant un certain temps. Cela contribue à contrer les attaques brutales de violation de mot de passe sur le système. Bien que les utilisateurs distants n'aient normalement pas besoin de répondre rapidement à des situations opérationnelles, il peut y avoir des cas,

par exemple des salles de commande sans personnel ou des installations distantes (par exemple, des systèmes SCADA contrôlant un système de distribution électrique), un accès rapide depuis un emplacement distant peut être nécessaire. Dans ces cas, la désactivation du compte d'accès peut être inappropriée. Il convient que chaque organisation gère l'authentification des utilisateurs distants de manière appropriée pour leur situation et la tolérance des risques.

d) Exiger une nouvelle authentification après une certaine durée d'inactivité de l'utilisateur *distant* sur le système

Après une période d'inactivité définie, il convient que l'utilisateur s'authentifie à nouveau avant de pouvoir accéder à nouveau au système. Cela permet d'assurer que le compte d'accès n'est pas laissé ouvert et accessible depuis le dispositif distant. Bien que les utilisateurs distants n'aient normalement pas besoin de se connecter au système de commande pendant de longues périodes, il peut y avoir des cas, par exemple les salles de commande sans personnel ou les installations distantes (par exemple, des systèmes SCADA sur un système de distribution électrique), un opérateur distant peut devoir surveiller le système pendant une durée prolongée. Dans ces cas, il peut être inapproprié de demander une nouvelle authentification. Il convient que chaque organisation gère l'authentification des utilisateurs distants de manière appropriée pour leur situation et la tolérance des risques.

Pour les utilisateurs distants, il convient que le niveau d'authentification requis soit proportionnel au risque d'accès non autorisé au système. Une authentification faible peut être appropriée si le système n'a pas de contrôle sur les opérations avec un risque HSE élevé. Pour les systèmes avec des risques HSE, une authentification forte peut être plus appropriée.

Des exemples d'authentification faible comprennent:

- la connexion de modems directement à des dispositifs ou réseaux de commande d'opérations industrielles qui utilisent une authentification simple par ID utilisateur et mot de passe;
- la connexion de dispositifs ou réseaux de commande d'opérations industrielles depuis le réseau local ou étendu de l'entreprise utilisant une authentification simple par ID utilisateur et mot de passe;
- l'utilisation d'une authentification par ID utilisateur et mot de passe Microsoft Windows® au niveau applicatif sur des dispositifs de commande d'opérations industrielles.

Des exemples d'authentification forte comprennent:

- l'utilisation d'une authentification à deux facteurs par jeton physique ou carte à puce qui requiert à la fois la possession d'un dispositif physique et une connaissance (par exemple, un numéro d'identification personnel (PIN)) de la part de l'utilisateur;

NOTE La sécurité est améliorée par l'entrée d'un code PIN sécurisé, par exemple, lorsque le code PIN est entré en utilisant un lecteur sécurisé pour éviter le piratage de code.

- authentification à l'aide de cartes à puce et de biométrie;
- authentification des utilisateurs basée sur leur emplacement;
- connexion de modems à des dispositifs ou réseaux de commande d'opérations industrielles qui utilisent une fonctionnalité de rappel à un numéro de téléphone prédéfini;
- connexion de dispositifs ou réseaux de commande d'opérations industrielles au réseau local ou étendu de l'entreprise et utilisation d'authentification par carte à puce ou biométrie;
- connexion d'ordinateurs à domicile à des dispositifs ou réseaux de commande d'opérations industrielles à l'aide d'une connexion VPN et d'une authentification à deux facteurs à l'aide d'un jeton et d'un code PIN.

#### A.3.3.6.5.4 Authentification pour la communication de tâche à tâche

Les communications de tâche à tâche ne sont normalement pas surveillées directement comme des sessions interactives d'utilisateur. L'authentification de communications de tâche à tâche se produira typiquement au démarrage d'une opération industrielle et à intervalles réguliers par la suite. Il convient que les systèmes utilisent une solution technique pour authentifier chaque dispositif ou réseau.

NOTE CEI/TR 62443-3-1 [6] contient une description de ces technologies, entre autres. Ce document décrit leurs forces et faiblesses ainsi que leur applicabilité à l'environnement IACS.

#### A.3.3.6.6 Pratiques en support

#### A.3.3.6.6.1 Pratiques de base

Les cinq actions suivantes sont des pratiques de base:

a) Établir une stratégie ou une approche qui définit la méthode d'authentification à utiliser. La méthode peut varier suivant les risques, les conséquences associées au processus d'activité et la sensibilité des données.

b) Utiliser différentes stratégies pour des utilisateurs se connectant depuis différents emplacements géographiques (y compris, des installations distantes) ou pour des dispositifs ayant des exigences de sécurité spécifiques. Ce problème tient compte des caractéristiques de sécurité physique qui interagissent avec les caractéristiques de cyber-sécurité pour établir le niveau de sécurité global pour l'utilisateur.

c) Authentifier tous les utilisateurs avant qu'ils soient autorisés à utiliser une application particulière. Cette exigence peut être abandonnée s'il existe des contrôles physiques de compensation.

d) Exiger au moins la saisie manuelle d'un ID utilisateur et un mot de passe au niveau minimal d'authentification électronique.

e) Authentifier les communications de tâche à tâche en connaissant l'adresse MAC et/ou IP pour le dispositif, une clé électronique spécifique, le nom du dispositif, et autres.

#### A.3.3.6.6.2 Pratiques additionnelles

L'action suivante est une pratique additionnelle:

a) Autoriser les utilisateurs à l'intérieur d'une installation verrouillée qui utilise des barrières et des lecteurs de badge à accéder aux systèmes ayant un niveau de risque plus élevé que celui auquel un utilisateur distant serait autorisé.

#### A.3.3.6.7 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [6], [23].

### A.3.3.7 ÉLÉMENT – Contrôle d'accès: Autorisation

Pour plus d'informations sur le sujet général du contrôle des accès, voir la section d'introduction en A.3.3.5.1.


IEC 2328/10

**Légende**

| Anglais | Français |
|---|---|
| Access control | Contrôle d'accès |
| Administration | Administration |
| Authentication | Authentification |
| Authorization | Autorisation |

**Figure A.12 – Contrôle d'accès: Autorisation**

L'Autorisation, le troisième pilier du contrôle des accès est représenté à la Figure A.12, est la procédure automatisée effectuée par le système informatique pour accorder les droits d'accès aux ressources en cas d'authentification réussie de l'utilisateur et d'identification de son compte d'accès associé. Les droits accordés sont déterminés dans la procédure par la détermination de la configuration du compte effectuée pendant l'étape d'administration des comptes.

Certaines procédures d'autorisation normalisées utilisées dans l'espace général de travail IT peuvent être inappropriées ou inadéquates pour les IACS. Par exemple, les comptes d'accès dans un système IT typique sont principalement basés sur les utilisateurs avec un nombre limité de rôles assignés (c'est-à-dire, un utilisateur lambda ou un administrateur système). Généralement, un seul rôle est assigné à chaque utilisateur. Les comptes d'accès dans un système IACS type sont principalement à base de rôle avec une plus grande granularité des rôles (c'est-à-dire, opérateur, ingénieur, spécialiste application, fournisseur et administrateur système). On peut assigner plusieurs rôles à un utilisateur sur la base d'une fonction particulière du poste qu'il doit remplir à un moment particulier. L'utilisateur peut devoir se connecter à un dispositif particulier et par ailleurs dans une application devoir être autorisé à apporter des modifications à des variables de commande et d'automatisation industrielle. Sinon, un utilisateur peut devoir se connecter à un système et se reconnecter pour effectuer des tâches d'administration système sur le même dispositif.

Ce paragraphe explore les contrôles destinés à protéger les informations et les actifs de toute destruction, modification ou divulgation délibérée ou accidentelle. Il est spécifiquement focalisé sur les mesures visant à permettre que les agents authentifiés (c'est-à-dire, le personnel, les applications, les services et les dispositifs) aient accès aux actifs de type information requis.

Les informations sensibles à toute divulgation doivent être protégées de manière appropriée afin de maintenir un avantage compétitif et protéger la confidentialité des employés.

Les règles d'autorisation souhaitées par une organisation détermineront comment celle-ci attribue des rôles à des utilisateurs ou groupes d'utilisateurs spécifiques et comment les droits pour ces comptes d'accès sont configurés. La capacité à mettre en œuvre une politique d'autorisation souhaitée dépend des fonctionnalités dans les systèmes sous-jacents pour distinguer les fonctions et les données requises pour différentes tâches. Par conséquent, la définition d'une politique d'autorisation est une procédure itérative dans laquelle l'organisation définit une politique idéale et détermine ensuite comment elle peut être fidèlement mise en œuvre en utilisant les fonctionnalités de leurs systèmes et de leur réseau. Lors de la mise en service d'un nouveau système, la prise en charge d'une politique d'autorisation souhaitée

peut être un élément de la spécification de mise en service. Lors de la conception d'une nouvelle configuration de réseau, des technologies telles que des pare-feu pour les utilisateurs distants peuvent être ajoutées pour créer une couche additionnelle d'autorisation pour les dispositifs critiques, comme décrit dans les alinéas suivants.

#### A.3.3.7.1 Considérations relatives à l'autorisation

##### A.3.3.7.1.1 Généralités

Lors du développement d'un programme de contrôle d'accès, il est important d'inclure la totalité des systèmes dans le domaine d'application et de ne pas limiter l'effort aux installations d'une salle informatique traditionnelle.

a) Politique de sécurité d'autorisation

   Les règles qui définissent les droits autorisés dans les comptes d'accès pour le personnel dans différentes fonctions doivent être définies dans une politique de sécurité d'autorisation qui est clairement documentée et appliquée à l'ensemble du personnel après authentification.

b) Méthodes d'autorisation logiques et physiques pour accéder aux dispositifs IACS.

   Il convient que la permission d'accéder aux dispositifs IACS soit logique (règles accordant ou refusant l'accès à des utilisateurs connus en fonction de leur rôle), physique (verrous, caméras et autres dispositifs de contrôle qui limitent l'accès à une console informatique active), ou les deux.

c) Accès aux informations ou aux systèmes au moyen de comptes d'accès à base de rôle

   Il convient que les comptes d'accès soient basés sur les rôles, ce qui permet de donner l'accès à des informations ou systèmes appropriés pour le rôle de cet utilisateur. Les implications de sécurité sont une composante critique de la définition de rôle.

##### A.3.3.7.1.2 Autorisation pour des utilisateurs locaux

De nombreuses industries de fabrication contrôlent leurs opérations depuis des salles de commande dans lesquelles sont postés plusieurs opérateurs. Ces opérateurs travaillent fréquemment en équipe et effectuent des opérations sur des stations IHM multiples dans le cadre de leurs fonctions normales. L'autorisation d'effectuer les fonctions d'une tâche spécifique est fournie par l'application. L'utilisateur local est autorisé à accéder à certains dispositifs ou opérations sur la base d'un compte d'accès à base de rôle. L'ID utilisateur et mot de passe de connexion effectifs sont typiquement communs à tous les utilisateurs dans le rôle. Cette approche de travail en équipe pour le fonctionnement d'une salle de commande peut être en conflit avec la politique et la pratique d'autorisation IT normalisée.

Les implications de sécurité doivent être prises en compte lors du développement de la stratégie d'autorisation. Pour des opérations industrielles à vulnérabilité élevée, il convient de définir les droits d'autorisation au niveau du dispositif de commande de procédé local et de ne pas demander l'accès aux dispositifs au niveau du réseau local ou étendu pour assigner des droits. Cela renforce le principe de contrôle de base de la réduction au minimum des points de défaillance potentiels.

Il convient de configurer les comptes d'accès de manière à accorder les privilèges minimaux requis pour le rôle. La formation doit être utilisée pour établir des niveaux communs de compétences pour chacun des rôles. Il convient d'éviter de personnaliser les comptes d'accès individuels conformément aux niveaux de compétence du personnel. Il convient que tous les utilisateurs ayant le même poste utilisent des comptes d'accès configurés pour le même rôle.

##### A.3.3.7.1.3 Autorisation pour des utilisateurs distants

Le processus d'autorisation présentement décrit jusqu'ici situe la fonction d'autorisation au nœud terminal du dispositif et au niveau de l'application. Dans les environnements de commande critiques, il convient d'utiliser une stratégie d'autorisation de destination additionnelle au niveau d'un dispositif de barrière (pare-feu ou routeur) pour le réseau IACS.

Une fois qu'un utilisateur est authentifié au niveau du dispositif de barrière, il convient d'attribuer des droits d'accès de destination à base de rôle à l'utilisateur de sorte que celui-ci puisse tenter uniquement de se connecter à des dispositifs pré-assignés sur le réseau IACS. Il convient que la connexion au nœud terminal établisse les droits finaux de l'utilisateur pour exécuter les fonctions sur le dispositif. Il convient que les installations à vulnérabilité élevée utilisent ce niveau additionnel d'autorisation de destination.

Il convient que les comptes d'accès à base de rôle prennent en compte l'emplacement géographique. Une personne peut utiliser un compte d'accès lorsqu'elle travaille sur site et un autre lorsqu'elle se connecte à distance depuis son domicile en appui au personnel local. Il convient que cette pratique soit clairement définie dans les procédures administratives. Il convient que le respect des procédures administratives soit basé sur la responsabilité individuelle.

#### A.3.3.7.2 Pratiques en support

##### A.3.3.7.2.1 Pratiques de base

Les deux actions suivantes sont des pratiques de base:

a) Autoriser l'accès à des dispositifs IACS avec des contrôles logiques (règles accordant ou refusant l'accès à des utilisateurs connus en fonction de leur rôle), physiques (verrous, caméras et autres dispositifs de contrôle qui limitent l'accès à une console informatique active), ou les deux.

b) Journaliser et examiner toutes les tentatives d'accès aux systèmes informatiques critiques, qu'elles aboutissent ou échouent.

##### A.3.3.7.2.2 Pratiques additionnelles

Les six actions suivantes sont des pratiques additionnelles:

a) Protéger les connexions réseau entre l'organisation et d'autres organisations par utilisation d'un pare-feu géré.

b) Utiliser un serveur proxy d'authentification pour tous les accès Internet sortants.

c) Accorder l'accès à un utilisateur distant en activant un modem sur un dispositif de commande d'opérations industrielles uniquement en cas de besoin.

d) Utiliser un accès audité lorsque des tâches à risque élevé sont effectuées (par exemple, des opérations industrielles qui ont des conséquences HSE ou qui représentent des risques critiques pour l'activité).

e) Distinguer les données à sensibilité et/ou conséquence pour l'activité importantes des autres informations internes de sorte que les contrôles d'autorisation existants puissent restreindre l'accès à ces informations.

f) Séparer le réseau d'activité du réseau IACS avec un dispositif de contrôle d'accès et limiter l'accès des utilisateurs aux actifs critiques des deux côtés.

#### A.3.3.7.3 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [6], [23], [27], [30], [43].

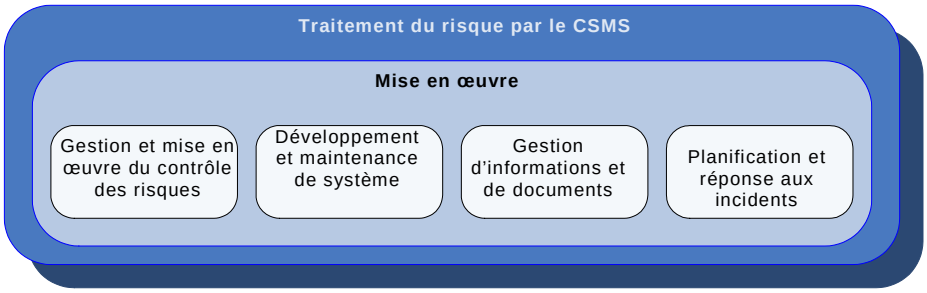
### A.3.4 Groupe d'éléments: Mise en œuvre

#### A.3.4.1 Description du groupe d'éléments

Le troisième groupe d'éléments dans cette catégorie est Mise en œuvre. Cet élément dans ce groupe décrit les différents aspects liés à la mise en œuvre du CSMS. La Figure A.13 est une représentation graphique des quatre éléments dans le groupe d'éléments:

- Gestion et mise en œuvre du contrôle des risques,

- Développement et maintenance de système,
- Gestion des informations et des documents et
- Planification et réponse aux incidents




.

**Figure A.13 – Vue graphique du groupe d'éléments: Mise en œuvre**

### A.3.4.2 Élément: Gestion et mise en œuvre du contrôle des risques

#### A.3.4.2.1 Description de l'élément

Le fondement de tout CSMS ou programme de sécurité est de maintenir les risques à un niveau acceptable. La Gestion et mise en œuvre du contrôle des risques concerne le choix, le développement et la mise en œuvre de mesures de sécurité qui sont adaptées aux risques. Les mesures de sécurité peuvent prendre en compte une conception des opérations industrielles intrinsèquement plus sûre, l'utilisation de produits avec de fortes caractéristiques de sécurité intrinsèques, des contre-mesures de sécurité manuelles et procédurales, et des contre-mesures à base de technologie pour prévenir ou réduire les incidents de sécurité.

Bien que le risque ne soit jamais totalement éliminé, il peut être contrôlé. Ce paragraphe décrit un cadre pour mesurer les risques et gérer ceux-ci par la mise en œuvre de différentes contre-mesures de sécurité pour réduire la vraisemblance qu'un incident se produise ou réduire les conséquences de l'événement résultant.

Dans la plupart des cas, le risque est mesuré en termes de coût ou de conscience sociale. Bien qu'il puisse être aisé de chiffrer le coût d'une interruption de production due à un incident de cyber-sécurité, il n'est pas possible d'attribuer un coût à un événement conduisant à la blessure ou au décès d'une personne. Les entreprises doivent déterminer leur tolérance des risques pour certains types d'événements et doivent utiliser celle-ci pour définir leur stratégie de gestion des risques.

#### A.3.4.2.2 Construction d'un cadre de gestion et de mise en œuvre du contrôle des risques

Étant donné que l'élimination totale des risques est généralement irréaliste ou impossible, il convient que les organisations se focalisent sur les applications et infrastructures critiques afin de réduire le risque à un niveau acceptable. Le choix des contre-mesures de cyber-sécurité à mettre en œuvre est déterminé par un équilibre entre les risques et les coûts. Il convient que les décisions soient basées sur une évaluation des risques et soient documentées de manière à servir de base pour les planifications et actions futures.

Il convient que les organisations analysent l'évaluation des risques détaillée, identifient le coût de réduction de chaque risque, comparent le coût au risque d'événement et choisissent les contre-mesures pour lesquelles le coût est inférieur au risque potentiel. Étant donné qu'il peut être irréaliste ou impossible d'éliminer tous les risques, il faut se concentrer sur les applications et infrastructures les plus critiques dans un premier temps. Les mêmes risques sont souvent observés à plusieurs emplacements. Il est raisonnable d'envisager le choix d'un ensemble normalisé de contre-mesures qui peuvent être applicables dans plusieurs cas et ensuite de définir à quel moment les utiliser. Cette approche permettra à l'organisation de

mettre en œuvre des solutions communes et de réduire les coûts de conception et de mise en œuvre pour améliorer la gestion de la sécurité par l'organisation. Une façon possible d'approcher cela est de développer un cadre global pour la mise en œuvre qui incorpore l'évaluation des risques, la tolérance des risques de l'organisation, l'évaluation et le choix des contre-mesures et la stratégie pour mettre en œuvre des activités de réduction des risques.

Chaque organisation aura probablement une tolérance des risques différente qui sera influencée par les réglementations, les moteurs de l'activité et les valeurs clés. La tolérance des risques de l'organisation aux incidents IACS détermine le degré d'effort qu'une organisation est prête à consacrer à la réduction du niveau de risque à un niveau acceptable. Si l'organisation a une faible tolérance des risques, elle peut souhaiter consacrer une grande quantité de ressources financières et/ou en personnel à la tâche d'amélioration du niveau de sécurité de l'IACS.

Le Tableau A.2 identifie la sensibilité de l'organisation à différents types de risque et groupe les différentes conséquences en niveau élevé, moyen ou faible. Lorsque ces catégories de conséquences sont combinées avec la vraisemblance qu'un incident se produise, comme décrit dans le Tableau A.1, le résultat est une matrice de catégories de conséquences en fonction de la vraisemblance. En l'absence d'une méthode analytique pour mesurer de façon quantitative la vraisemblance et les conséquences, il peut être pratique d'attribuer simplement des niveaux de risque qualitatifs faible, moyen et élevé aux points d'intersection dans la matrice. Ces niveaux de risque reflètent la sensibilité de l'organisation aux risques, comme décrit dans le Tableau A.3. Ces niveaux de risque impliquent des seuils de tolérance qui régissent la stratégie de mise en œuvre de réduction des risques. Il s'agit d'une méthode claire pour communiquer la position de l'organisation sur les risques.

La stratégie de réduction des risques peut utiliser différentes contre-mesures, pratiques d'architecture, sélection de dispositif IACS et les décisions concernant quand et où utiliser celles-ci sur la base du niveau de risque indiqué dans le Tableau A.3. Des systèmes à risque élevé requièrent l'utilisation de contre-mesures plus strictes pour obtenir un niveau de sécurité plus élevé.

Une méthode d'enregistrement des décisions de l'organisation concernant le choix de contre-mesures consiste à développer une table énumérant des contre-mesures spécifiques à utiliser pour des dispositifs IACS sur la base du niveau de risque de l'IACS. Un exemple de table de contre-mesures possibles est présenté dans le Tableau A.4.

Le tableau définit l'ensemble des solutions communes de contre-mesures à utiliser pour tenter d'atteindre le niveau de sécurité cible. Ces contre-mesures doivent être utilisées sauf en cas de contrainte unique qui rend cette solution indésirable pour un IACS donné. La stratégie de réduction des risques de l'organisation peut également utiliser les notations de niveau de risque pour définir des priorités et le délai pour mettre en œuvre les contre-mesures identifiées présentées dans le Tableau A.4. Il conviendra probablement qu'un IACS ayant des évaluations de risque élevées soit géré avec une plus grande urgence qu'un IACS à niveau de risque plus faible.

Les contre-mesures pour contrôler un risque spécifique peuvent être différentes pour différents types de systèmes. Par exemple, des contrôles d'authentification d'utilisateur pour un serveur de commande d'application avancé associé à un DCS peuvent être différents des contrôles d'authentification pour l'IHM sur la ligne d'emballage. La documentation et la communication des contre-mesures choisies, avec les instructions d'application pour utilisation des contre-mesures, est une bonne stratégie à suivre.

**Tableau A.4 – Exemples de contre-mesures et pratiques basées sur des niveaux de risque d'IACS**

| Contre-mesure et pratiques d'architecture | IACS à risque élevé | IACS à risque moyen | IACS à faible risque |
|---|---|---|---|
| Authentification à deux facteurs pour contrôler l'accès au dispositif | Requis | Requis | Optionnel |
| Renforcement du système d'exploitation | Requis | Recommandé | Optionnel |
| Utilisation de la segmentation de réseau | Requis | Requis | Optionnel |
| Utilisation d'une application antivirus | Requis | Requis | Requis |
| Utilisation de réseau étendu | Non autorisée | Peut être autorisée | Autorisée |
| Authentification forte par mot de passe au niveau application | Requis | Recommandé | Recommandé |
| Autres contre-mesures | … | … | … |

Il existe plusieurs contre-mesures de réduction des risques différentes pour des technologies des informations qui peuvent et doivent être appliquées à des dispositifs IACS. Des directives sur des contre-mesures spécifiques sont décrites dans d'autres parties de la série CEI 62443 qui sont encore en développement, telles que la CEI 62443-3-2 [7] et CEI 62443-3-3 [8], qui décrivent de manière approfondie différentes contre-mesures et leur application à l'environnement IACS.

La plupart des organisations disposent de ressources financières et en personnel limitées pour les consacrer aux activités CSMS. En conséquence, il est important d'utiliser ces ressources d'une manière la plus efficace possible. Un cadre de gestion des risques commence par la connaissance des vulnérabilités qui existent à l'intérieur de l'IACS et des conséquences potentielles qui peuvent survenir si cette vulnérabilité était exploitée. Une fois que les risques sont connus, l'entreprise doit développer un cadre de mise en œuvre pour réduire les risques de manière à les maintenir à un niveau acceptable. Plusieurs des modèles de sécurité décrits dans CEI/TS 62443-1-1 seront utilisés dans la création du cadre de mise en œuvre. Les modèles comprennent le modèle de niveau de sécurité avec le modèle de zone et de conduit.

NOTE Ce paragraphe décrit une manière possible d'approcher cet élément clé du CSMS à l'aide des modèles de sécurité de la CEI/TS 62443-1-1. Il n'existe pas d'approche appropriée unique pour cet élément. D'autres approches peuvent conduire à un cadre très fonctionnel pour gérer les risques.

La description détaillée et l'exemple qui suivent sur le sujet de la gestion des risques et de la mise en œuvre décrit le processus cadre tel qu'il est appliqué pour réduire les risques de cyber-sécurité pour un système existant dans un secteur d'opération industrielle unique. Le cadre est également applicable à de nombreux nouveaux IACS à des emplacements multiples autour du monde.

Quelle que soit l'approche de gestion et mise en œuvre du contrôle des risques détaillée utilisée, un cadre de qualité approprié doit comporter quatre ensembles principaux de tâches au cours du cycle de vie d'un IACS:

- Évaluation des risques de l'IACS;
- Développement et mise en œuvre des contre-mesures;
- Documentation des contre-mesures et des risques résiduels;
- Gestion des risques résiduels au cours du cycle de vie de l'IACS.

Ces tâches sont couvertes de manière détaillée dans A.3.4.2.3 à A.3.4.2.5 et sont représentées graphiquement dans les modèles de cycle de vie de sécurité décrits dans CEI/TS 62443-1-1, 5.11.

#### A.3.4.2.3 Évaluation des risques de l'IACS pour déterminer le niveau de risque de cyber-sécurité de l'IACS

##### A.3.4.2.3.1 Généralités

Le modèle de zone et de conduit, le modèle de cycle de vie de niveau de sécurité, et le modèle de référence sont décrits de manière détaillée dans CEI/TS 62443-1-1. L'utilisation et l'intégration de ces modèles sera décrite dans ce paragraphe.

A.2.3 contient des instructions sur une procédure à suivre afin d'analyser le risque de l'IACS. Il s'agit d'une des premières activités dans la phase d'évaluation du modèle de cycle de vie de niveau de sécurité. Une organisation doit développer et documenter un processus d'analyse des risques de sorte qu'il puisse être utilisé sur des IACS multiples sur différents emplacements au sein de l'organisation avec des résultats répétables.

Ce paragraphe explique comment la phase d'évaluation s'intègre dans la stratégie globale de gestion des risques. Cela est illustré en suivant le scénario d'examen d'un IACS existant et en améliorant la position de cyber-sécurité de ce système afin de réduire les risques. La Figure A.14 représente la phase d'évaluation du modèle du cycle de vie du niveau de sécurité.

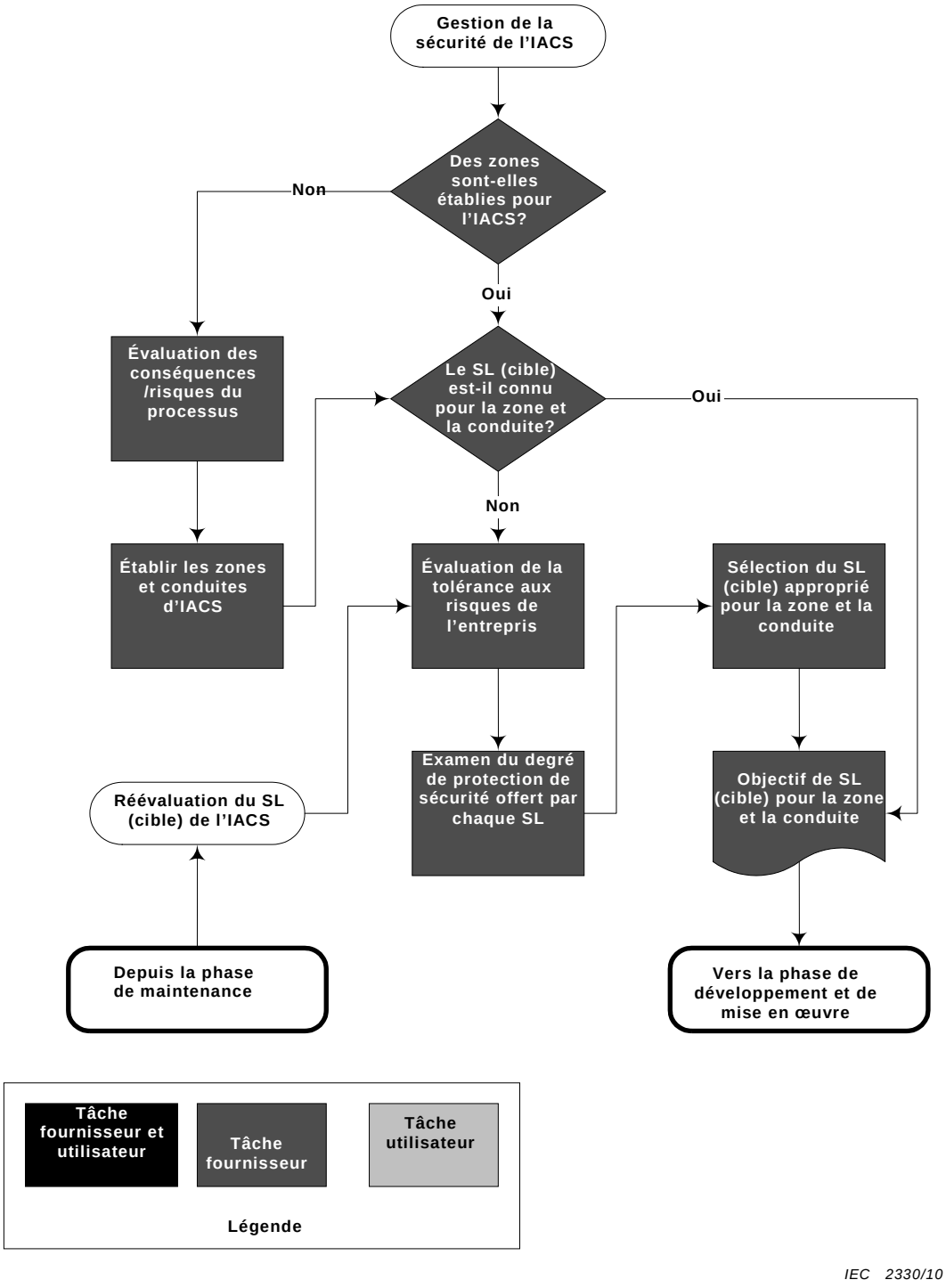



**Figure A.14 – Modèle de cycle de vie du niveau de sécurité: Phase d'évaluation**

Pour un IACS existant qui n'a jamais subi une évaluation des risques et n'a jamais utilisé le modèle de zone, l'activité commence par le cadre intitulé "Évaluation de conséquence/risques du processus".

L'objectif de l'évaluation est de comprendre l'impact des risques sur l'activité dans le cas où l'IACS subit un incident informatique et n'est pas en mesure de remplir ses fonctions de commande prévues ou exécute des fonctions inappropriées. Une fois que le risque associé à l'IACS a été documenté, il convient d'exécuter les activités associées à la gestion et la réduction des risques.

Le résultat de l'analyse des risques sera un tableau qui énumère l'évaluation des conséquences et l'évaluation de vraisemblance pour chaque actif ou collection d'actifs IACS. Le Tableau A.5 est un exemple de résultat d'une évaluation détaillée des risques et résulte de la combinaison du Tableau A.1, du Tableau A.2 et du Tableau A.3 de la présente norme. L'évaluation de vraisemblance est définie sur la base de l'évaluation détaillée de vulnérabilité de chacun des actifs énumérés, et de la vraisemblance d'occurrence des menaces.

**Tableau A.5 – Exemple de tableau des actifs IACS avec les résultats d'évaluation**

| Actif de dispositif IACS | Évaluation de conséquence | Évaluation de vraisemblance |
|---|---|---|
| Console d'opérateur de salle de commande | A | Moyenne |
| Console d'opérateur distant | C | Haute |
| Station de configuration technique | A | Haute |
| Serveur d'historisation | B | Moyenne |
| Contrôleur | A | Moyenne |
| Passerelle | B | Moyenne |
| Autres dispositifs | C | Basse |

#### A.3.4.2.3.2 Détermination du niveau de risque de l'IACS

Le Tableau A.3 est un modèle d'exemple simplifié pour traduire la sensibilité d'une entreprise aux risques, en niveaux de risque qualitatifs pour l'IACS. Il convient qu'il soit généré par la direction de l'organisation avant que l'analyse des risques soit conduite.

L'intersection des évaluations de conséquence et de vraisemblance produit le niveau de risque.

EXEMPLE Un dispositif IACS avec une évaluation de conséquence B et une vraisemblance Haute représenterait un dispositif à haut risque.

Les classements de risque dans le Tableau A.3 peuvent être appliqués aux actifs des dispositifs IACS dans le Tableau A.5 résultant en une évaluation globale pour l'IACS telle que décrite dans le Tableau A.6. Ce tableau présente un classement par priorité pour des vulnérabilités particulières.

Chaque dispositif est associé à un niveau de risque de cyber-sécurité. Dans un IACS étroitement intégré, les fonctions de commande remplies par chaque dispositif sont fortement dépendantes de l'intégrité des autres dispositifs de l'IACS. L'intégrité fonctionnelle du système de commande sera affectée par l'intégrité du dispositif le plus vulnérable.

Une hypothèse de sécurité simplifiée est que le dispositif ayant le plus haut niveau de risque de l'IACS définit le niveau de risque inhérent pour l'ensemble de l'IACS. Dans l'exemple d'IACS présenté dans le Tableau A.6, le niveau de risque inhérent pour l'IACS est un risque élevé parce que plusieurs des dispositifs de l'IACS ont un niveau de risque identifié comme Haut.

**Tableau A.6 – Exemple de tableau des actifs IACS avec les résultats d'évaluation et les niveaux de risque**

| Actif de dispositif IACS | Évaluation de conséquence | Évaluation de vraisemblance | Évaluation de conséquence |
|---|---|---|---|
| Console d'opérateur de salle de commande | A | Moyenne | Risque haut |
| Console d'opérateur distant | C | Haute | Risque moyen |
| Station de configuration technique | A | Haute | Risque haut |
| Serveur d'historisation | B | Moyenne | Risque moyen |
| Contrôleur | A | Moyenne | Risque haut |
| Passerelle | B | Moyenne | Risque moyen |
| Autres dispositifs | C | Basse | Risque faible |

La compréhension de ce niveau de risque de base inhérent est essentielle pour exécuter un plan de gestion des risques. Celui-ci établit le niveau de sécurité cible à atteindre pour réduire les risques. Cela établit la justification pour mettre en œuvre un plan de réduction et de gestion des risques, si l'IACS n'est déjà pas opérationnel à ce niveau cible. Différentes contre-mesures de sécurité seront utilisées pour ramener les risques pour l'IACS à un niveau tolérable. Cependant, si ces contre-mesures ne parviennent pas à réduire le risque, cela peut conduire à un incident, ayant pour conséquence l'amplitude identifiée lors de la tâche d'analyse des risques.

#### A.3.4.2.3.3 Établir des zones de sécurité et associer des dispositifs IACS aux zones

Le modèle de référence décrit dans la CEI/TS 62443-1-1 identifie plusieurs niveaux opérationnels ou plusieurs équipements différents pour un IACS. Bien qu'il puisse exister différents niveaux opérationnels dans un IACS, les exigences de cyber-sécurité peuvent être similaires pour plusieurs de ces niveaux opérationnels ou équipements. Il peut être possible d'incorporer plusieurs niveaux opérationnels/équipement dans une seule zone de sécurité logique.

Le modèle de niveau de sécurité introduit le concept d'utilisation de zones assignées à l'un de trois niveaux de sécurité ou plus. À titre d'illustration dans cet exemple, supposons qu'il y ait trois niveaux de sécurité qualitativement décrits par Bas, Moyen et Haut. La tâche à effectuer consiste à examiner les besoins de sécurité des différents actifs des dispositifs de l'IACS et assigner ceux-ci à ces différentes zones.

Le Tableau A.6 énumère le niveau de risque de cyber-sécurité de l'IACS pour chacun des actifs. Les actifs ayant un niveau de risque Haut partagent un besoin d'un haut niveau de cyber-protection afin de réduire les risques. Il convient que ces actifs soient assignés à une zone de sécurité commune. Il convient que les actifs ayant des niveaux de risque plus faibles soient assignés à une zone de sécurité plus faible. À ce stade dans le processus de gestion des risques, il est approprié de superposer les zones de sécurité identifiées sur le schéma du réseau physique du système développé pour conduire l'analyse des risques.

Compte tenu des technologies de contre-mesure de sécurité actuelles, les zones de sécurité seront typiquement alignées avec les segments de réseau physique. Un dispositif IACS peut ne pas être situé actuellement sur le segment de réseau approprié sur la base des résultats de l'analyse des risques pour ce dispositif. Si c'est le cas, il peut être nécessaire de transférer le dispositif dans un segment de réseau différent. Un actif avec un niveau de risque Bas peut être affecté à une zone de sécurité de risque plus élevé, mais il convient que les actifs avec un niveau de risque Haut ne soient pas placés dans une zone de sécurité de risque plus faible. Cela augmenterait le risque d'une conséquence inacceptable en cas d'incident de cyber-sécurité.

Au cours de la phase de mise en œuvre du modèle de cycle de vie de niveau de sécurité, il convient que les dispositifs ayant des besoins de sécurité ne correspondant pas à la zone

dans laquelle les dispositifs sont physiquement situés soient relocalisés dans les segments de réseau appropriés afin de satisfaire aux exigences de sécurité.

Une organisation peut choisir d'établir une approche commune des zones de sécurité en vue d'améliorer l'efficacité de la gestion des risques. Une façon d'effectuer cela consiste à adopter une architecture de modèle d'entreprise incorporant des stratégies de segmentation de réseau et des zones de sécurité pour les différents types et systèmes utilisés dans l'entreprise. La Figure A.15 présente un exemple d'une architecture de modèle de zone de sécurité pour une organisation. La Figure A.16 décrit comment les actifs IACS dans l'exemple sont mis en correspondance avec les zones dans l'architecture de modèle utilisant une approche de zone à trois niveaux.

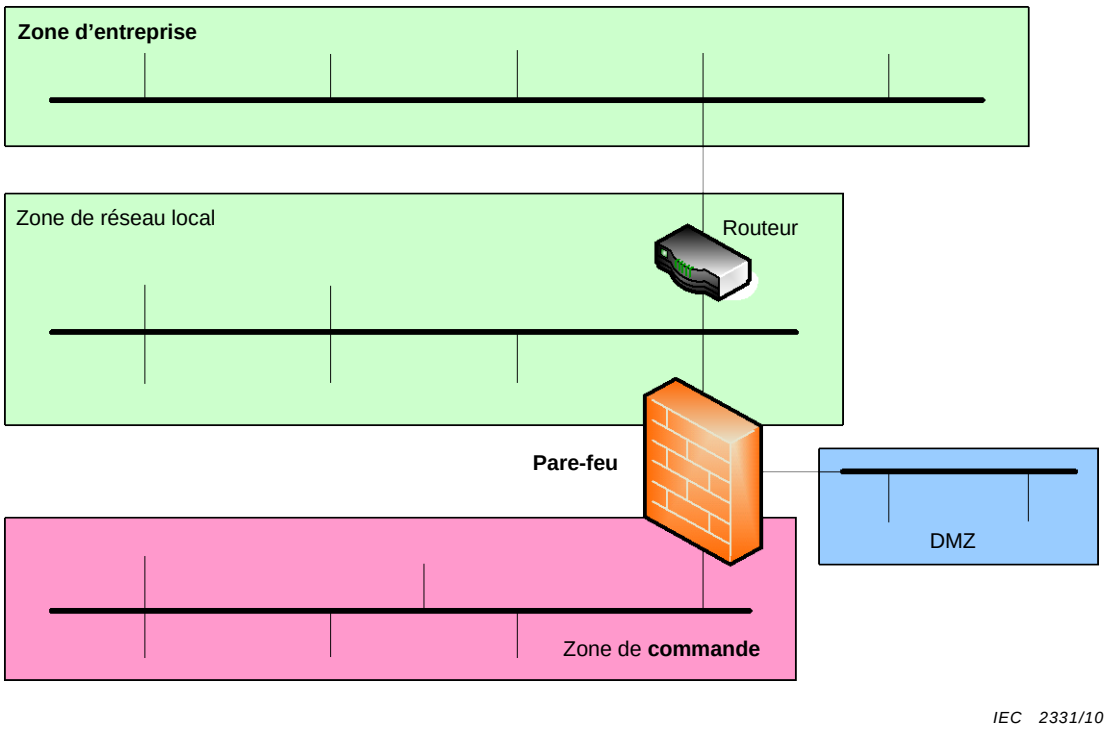



**Figure A.15 – Modèle d'architecture de zone de sécurité pour l'entreprise**

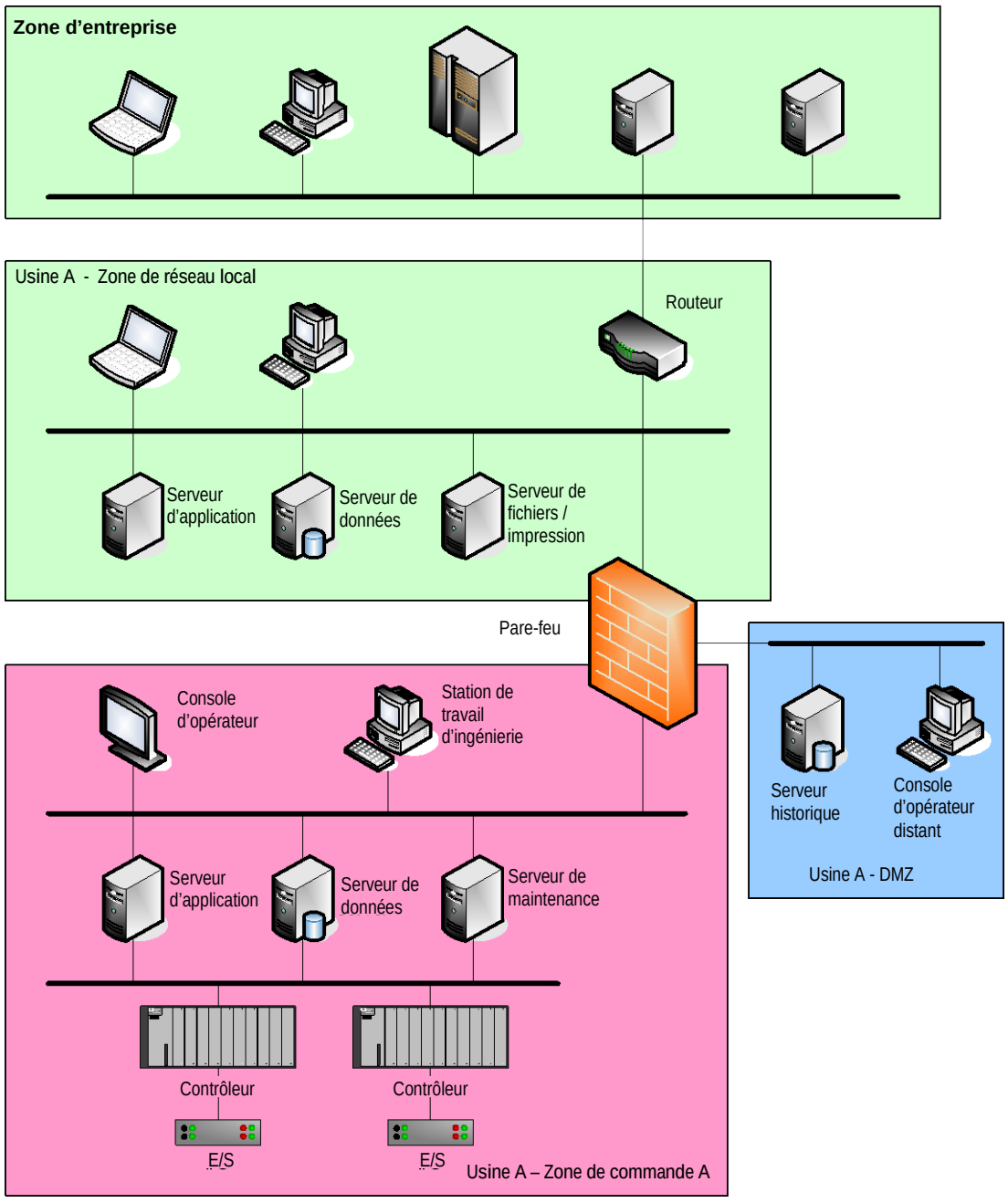



**Figure A.16 – Zones de sécurité pour un exemple d'IACS**

#### A.3.4.2.3.4 Détermination du niveau de sécurité cible

Le modèle de niveau de sécurité introduit le concept d'assignation d'un niveau de sécurité à la zone. Dans l'exemple décrit à la Figure A.16 ci-dessus, le niveau de risque inhérent de l'IACS a été déterminé comme étant un risque Haut sur la base de l'évaluation détaillée des risques de chaque dispositif IACS. Les contre-mesures de sécurité supplémentaires doivent être utilisées pour protéger les dispositifs situés dans la zone de commande de l'Usine A. En utilisant les niveaux de sécurité énumérés dans CEI/TS 62443-1-1, Tableau 8, il est approprié d'assigner un niveau de sécurité cible à chacune des zones, comme décrit dans le Tableau A.7.

**Tableau A.7 – Niveaux de sécurité cibles pour un exemple d'IACS**

| Zone | Niveau de sécurité cible = SL(cible) |
|---|---|
| Zone de commande Usine A | Haut |
| DMZ Usine A | Moyen |
| Zone de réseau local Usine A | Bas |
| Zone d'entreprise | Bas |

#### A.3.4.2.3.5 Sélection des dispositifs et conception de système basée sur SL (capacité)

La capacité de niveau de sécurité de chaque dispositif doit être examinée pour comprendre les forces de sécurité et les vulnérabilités qu'il introduit dans la zone. Bien que le SL(capacité) ne puisse pas être mesuré quantitativement à ce stade, il existe des moyens plus qualitatifs pour évaluer le SL(capacité) relatif des dispositifs constituant l'IACS. Ces éléments d'évaluation sont typiquement couverts comme faisant partie d'une évaluation de vulnérabilité détaillée. Par exemple:

- Si le dispositif est un serveur Web, exécution d'un outil d'évaluation pour identifier les faiblesses d'applications de serveur Web et détermination si les faiblesses peuvent être corrigées.
- Exécution d'un outil d'évaluation pour identifier le nombre de services et de ports requis pour que l'application fonctionne sur le dispositif.
- Examen des ports et des services requis pour déterminer si ceux-ci ont été historiquement utilisés par des attaquants afin d'exploiter les vulnérabilités du système.
- Examen du système d'exploitation du dispositif et détermination si les correctifs et les mises à niveau de sécurité sont toujours fournis pour la version utilisée.
- Exécution d'un outil d'évaluation pour soumettre l'application à des entrées inhabituelles afin de déterminer si le dispositif et l'application continueront de fonctionner avec des flux de communication anormaux.
- Examen de l'historique d'exploitation des technologies sous-jacentes utilisées dans le dispositif pour déterminer la vraisemblance d'exploitations futures.

Il convient que l'organisation ait des critères d'acceptation pour un dispositif destiné à être utilisé dans un niveau de sécurité cible particulier sur la base des résultats de ces outils d'évaluation et des faiblesses identifiées. Si le SL(capacité) du dispositif est simplement trop faible pour atteindre le SL(cible) pour la zone, il peut être nécessaire de sélectionner un autre dispositif. Pour un IACS existant constitué de dispositifs d'ancienne génération, il peut être nécessaire de remplacer le dispositif par un dispositif de nouvelle génération ayant un SL(capacité). Un exemple pourrait être une station de commande d'opérateur basée sur PC fonctionnant sous Microsoft Windows® NT sous la forme de son système d'exploitation. Les résultats d'évaluation détaillée de vulnérabilité pour ce dispositif et cette application peuvent présenter des vulnérabilités significatives. Les caractéristiques de sécurité intégrées dans ce système d'exploitation plus ancien sont inférieures à la plupart des systèmes d'exploitation de nouvelles générations. De plus, des correctifs de sécurité pour gérer ces vulnérabilités ne sont plus fournis par le fournisseur. Cela laisse le dispositif dans une position relativement faible en ce qui concerne son SL(capacité) améliorée.

Il convient que le SL(capacité) de chaque nouveau dispositif IACS soit examiné afin de s'assurer qu'il prend en charge l'objectif de SL(cible) pour la zone. Bien que des mesures quantitatives de SL(capacité) puissent ne pas être disponibles et/ou publiées, les fournisseurs peuvent être en mesure de fournir des mesures plus qualitatives basées sur des évaluations qu'eux-mêmes ou des tiers ont conduites en utilisant des outils de sécurité normalisés et des essais de terrain. Il convient de prendre en compte ces résultats d'évaluation de vulnérabilité détaillés pour le choix de dispositifs IACS.

La conception préliminaire identifiant les dispositifs IACS et les assignations de zone doit être transformée en une conception plus détaillée identifiant tous les équipements et segments de réseau à utiliser dans l'IACS. C'est le stade auquel les dispositifs dont les besoins en termes de risque de sécurité ne correspondent pas au SL(cible) pour la zone doivent être relocalisés. Il convient que le résultat de cette étape soit un schéma de réseau détaillé localisant tous les dispositifs IACS et réseau qui feront partie de l'IACS global.

#### A.3.4.2.4 Développement et mise en œuvre des contre-mesures sélectionnées pour chaque zone

##### A.3.4.2.4.1 Généralités

La phase de développement et de mise en œuvre du modèle de cycle de vie de niveau de sécurité concerne les étapes et tâches visant à réduire les risques. Le concept global de cette phase est l'utilisation de contre-mesures pour qu'un IACS atteigne le niveau de sécurité cible pour la zone établie pendant la phase d'évaluation. La Figure A.17 envisage plusieurs points de départ différents. Elle s'applique à la mise en œuvre d'un nouvel IACS, des modifications d'un IACS existant sous la forme d'un nouvel équipement, et l'amélioration de la sécurité d'un IACS existant. La Figure A.17 est un cadre de référence pour guider la réflexion plutôt qu'un organigramme détaillé ou une liste de contrôle d'étapes qui doivent être suivies.

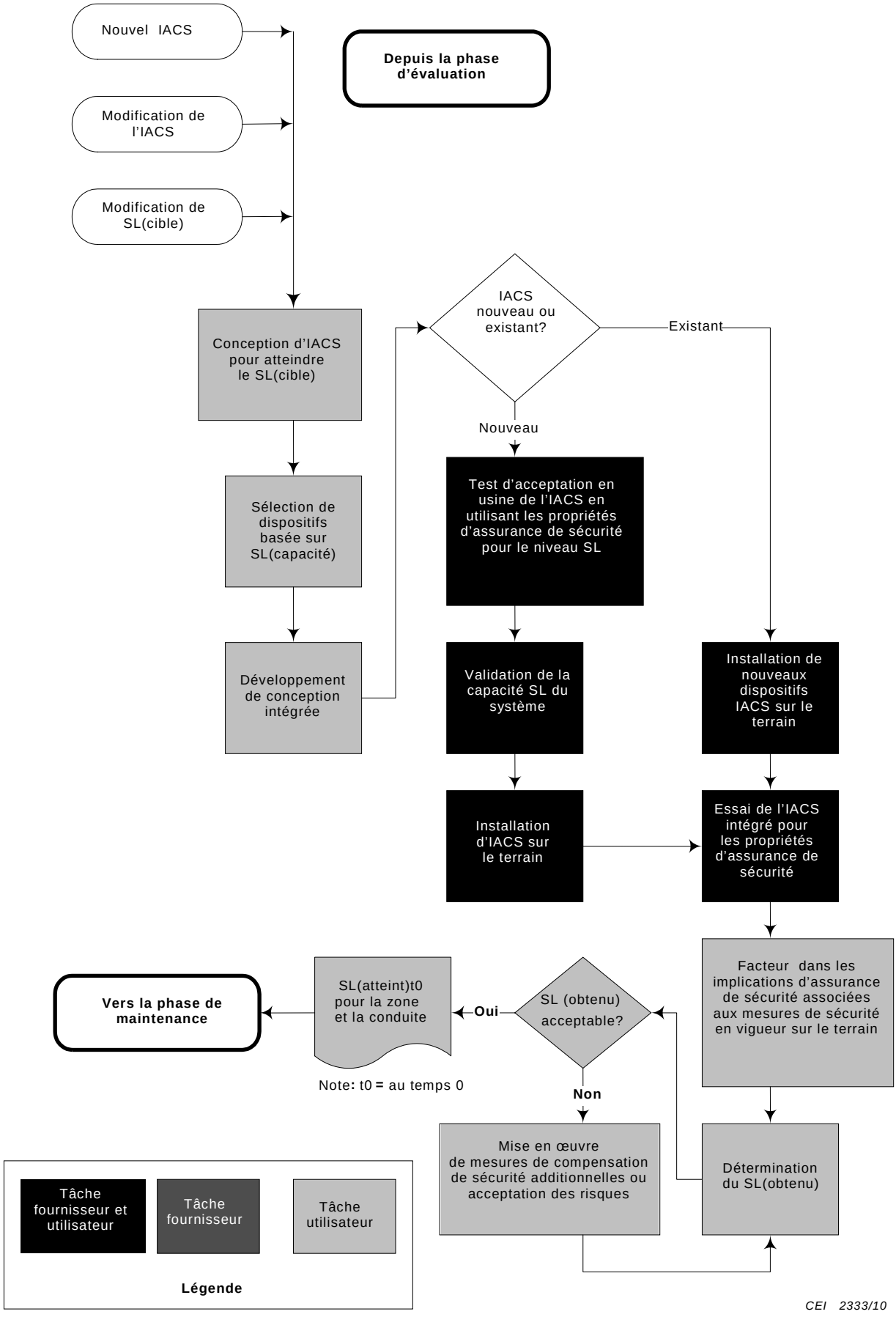



**Figure A.17 – Modèle de cycle de vie du niveau de sécurité: Phase de développement et de mise en œuvre**

Le point de départ de cette phase est l'objectif de sécurité à atteindre. Celui-ci est exprimé comme étant le niveau de sécurité cible pour chaque zone de l'IACS. Dans la phase d'évaluation, ces cibles ont été établies et des assignations de zone préliminaires ont été effectuées pour chacun des dispositifs IACS. La tâche à effectuer est de suivre cette approche préliminaire et de créer une conception détaillée pour mise en œuvre.

#### A.3.4.2.4.2 Essai de sécurité hors ligne

Tout comme l'essai fonctionnel d'un IACS est essentiel pour mettre en œuvre un IACS afin qu'il satisfasse aux besoins des installations opérationnelles, l'essai de sécurité des dispositifs est également important pour veiller à ce que l'intégrité opérationnelle et la robustesse soient assurées. La section A.3.4.3 contient des informations plus détaillées sur la conduite des essais de sécurité.

Si l'IACS est un nouveau système, il convient de réaliser les essais de sécurité lorsque le système est dans un environnement hors ligne. Il peut s'agir d'un essai d'acceptation sur le site d'un fournisseur ou d'une étape d'installation hors ligne à l'emplacement final sur le terrain. L'emplacement n'est pas aussi important que de s'assurer que les étapes d'essai de sécurité sont effectuées. Bien qu'il soit très utile de soumettre à essai la sécurité de l'ensemble des dispositifs et contre-mesures utilisés dans l'état final installé, cela peut n'être ni abordable, ni pratique. Par conséquent, il convient que la conception des essais soit axée sur la SL(capacité) des dispositifs IACS et les contre-mesures qui ne sont pas spécifiques à l'emplacement d'installation sur le terrain.

Le paragraphe précédent mentionne plusieurs outils et éléments à prendre en considération pour l'essai de SL(capacité). Ces éléments sont typiquement couverts comme faisant partie d'une évaluation détaillée de vulnérabilité. Il convient que les essais de sécurité comprennent non seulement des essais pour évaluer la capacité à résister à des menaces de sécurité typiques rencontrées dans des conditions opérationnelles, mais qu'ils comprennent les mesures qui feront partie du support continu de sécurité du système. Celles-ci comprennent mais ne sont pas limitées à:

- l'essai du processus de correction pour les correctifs et mises à niveau du système d'exploitation;
- l'essai du processus de correction et de mise à niveau pour les mises à jour de fournisseur d'IACS;
- l'essai de l'environnement de développement de système hors ligne;
- l'essai du déploiement de logiciel antivirus et les mises à jour des signatures de programmes malveillants.

L'objectif global des activités d'essai de sécurité décrites au centre de la Figure A.17 est de valider que le SL(capacité) des dispositifs est aligné avec la base de conception.

#### A.3.4.2.4.3 Essais de sécurité de terrain

Les éléments représentés sur la droite de la Figure A.17 ci-dessus identifient les activités d'essais associées à l'environnement de destination final. C'est le point auquel les contre-mesures utilisées sont soumises à essai et/ou examinées pour déterminer si le niveau de sécurité atteint est égal ou supérieur au niveau de sécurité cible de la conception de base pour la zone.

Dans le cas d'un nouvel IACS installé, il est probablement possible de réaliser ces essais avant que l'IACS soit mis en ligne. Si l'activité consiste à rattraper et remplacer un dispositif IACS existant ou mettre en œuvre de nouvelles contre-mesures de sécurité pour l'IACS, il peut ne pas être possible d'obtenir une fenêtre d'opportunité pour effectuer des essais de sécurité de terrain complets. Le défi est plus souvent de mettre en œuvre le nouveau dispositif ou la nouvelle contre-mesure et de réaliser un essai de terrain pour vérifier que la fonction opérationnelle de base de l'IACS n'a pas été affectée de façon inacceptable par les mesures de sécurité.

Il est important de garder à l'esprit qu'il convient que les essais de performance du système comprennent la réponse du système à des événements de type opération industrielle normaux et anormaux ainsi que des événements de type sécurité normaux et anormaux. Ceux-ci sont combinés pour obtenir une mesure globale de la robustesse et de l'intégrité du système.

Étant donné que chaque opération industrielle est légèrement différente, il n'est pas possible d'identifier une procédure de type recette de cuisine pour cet essai. Des efforts de conception considérables seront nécessaires pour déterminer le meilleur moyen de soumettre à essai l'assurance que les fonctions de sécurité satisfont aux objectifs de sécurité pour atteindre le niveau de sécurité cible.

#### A.3.4.2.4.4 Obtention du niveau de sécurité cible

L'obtention du niveau de sécurité cible sur le terrain peut nécessiter un certain degré d'itération. Le terrain n'est pas un monde parfait. Il est généralement approprié de tenter d'appliquer un ensemble commun de contre-mesures à l'ensemble des dispositifs dans la zone pour obtenir le niveau de sécurité souhaité. Une contre-mesure sélectionnée identifiée pour mise en œuvre sur tous les dispositifs peut ne pas être utilisable sur un dispositif particulier en raison d'une contrainte opérationnelle ou physique initialement reconnue au cours de la conception de sécurité du système. Par conséquent, il est important de noter que les situations concrètes peuvent nécessiter l'élimination ainsi que l'ajout de contre-mesures pour des dispositifs individuels dans une zone pour obtenir l'équilibre correct entre le bénéfice en termes de sécurité et le risque de sorte que toutes les parties impliquées dans le processus de décision soient satisfaites.

#### A.3.4.2.4.5 Illustration du processus de conception en utilisant l'exemple d'IACS

Les paragraphes précédents concernent les principes de mise en œuvre de contre-mesures de sécurité pour atteindre le SL(cible) pour la zone. Ce paragraphe décrit le processus de conception d'application de ces principes sur un exemple concret.

Le Tableau A.6 identifie un serveur d'historisation avec un niveau de risque de dispositif Moyen. En utilisant le modèle d'architecture de sécurité d'entreprise, il a été déterminé que ce dispositif devait être situé dans une zone de sécurité ayant un SL(cible) moyen ou élevé. La DMZ de l'Usine A a été identifiée comme étant la zone appropriée pour ce dispositif, bien que le dispositif soit actuellement situé dans la zone réseau local de l'Usine A.

Dans la préparation pour la mise en œuvre physique de la DMZ de l'Usine A, le SL(capacité) du serveur d'historisation est examiné afin de déterminer s'il satisfait au SL(cible). L'examen des vulnérabilités à l'aide d'une évaluation détaillée de vulnérabilité met en évidence que:

- Le système d'exploitation pour le serveur est Microsoft Windows® NT, pour lequel aucune mise à jour de sécurité n'est disponible.
- Aucune application antivirus n'est exécutée sur le serveur. Le fournisseur de l'application historique n'a pas encore qualifié de produits logiciels antivirus comme étant compatibles avec l'application historique.
- La majorité des utilisateurs de l'application historique sont situés dans des zones de bureau avec des connexions PC à la zone réseau local de l'Usine A de plus basse sécurité.
- Des efforts pour renforcer le serveur en désactivant les tâches non requises n'ont pas abouti avec succès parce que le fournisseur de l'application historique ne certifie pas que l'application fonctionnerait correctement si les services étaient interrompus.

La conclusion est que le SL(capacité) inhérent du serveur d'historisation est incohérent avec le SL(cible) pour la DMZ de l'Usine A.

Étant donné que le SL(capacité) inhérent est trop bas, l'utilisation de contre-mesures additionnelles a été examinée pour déterminer si elles pouvaient réduire avec succès le

risque de satisfaire au SL(cible). Des contre-mesures additionnelles telles que l'élimination de l'accès Internet, l'élimination du courrier électronique, la désactivation des ports de média sur le serveur, l'utilisation de mots de passe forts ont été examinées. Bien qu'elles puissent contribuer à la réduction des risques, il est estimé que l'utilisation de ces pratiques de sécurité additionnelles ne compenserait pas le faible SL(capacité) inhérent du serveur d'historisation.

Étant donné que le serveur d'historisation est directement interfacé avec la passerelle de l'IACS du réseau de commande réglementaire, les faiblesses de sécurité de ce dispositif diminuent également le SL(obtenu) de la zone de commande de l'Usine A. La conclusion est que le meilleur moyen de gérer ces états de SL(obtenu) inacceptable pour la DMZ de l'Usine A et la zone de commande de l'Usine A consiste à remplacer le serveur d'historisation actuel par une application logicielle historique plus récente exécutée sur un système d'exploitation actuellement pris en charge. Après avoir examiné le SL(capacité) du serveur et de l'application historique récents afin de vérifier qu'il correspond au SL(cible), le serveur et l'application sont soumis à essai et mis en œuvre dans la DMZ de l'Usine A au cours d'un arrêt des opérations industrielles.

Il convient de souligner plusieurs points importants en ce qui concerne cet exemple. Le SL(obtenu) d'une zone dépend du SL(capacité) des dispositifs dans la zone mais également de la connectivité dans et entre les zones. Une analyse de vulnérabilité pour un dispositif prend en compte non seulement les propriétés inhérentes du dispositif concerné en isolement, mais également la connectivité de ce dispositif sur le réseau. Ceci est important parce qu'un IACS qui utilise uniquement des dispositifs qui ont un SL(capacité) Haut lorsqu'ils sont considérés en isolement, peuvent ne pas nécessairement atteindre le SL(cible) Haut pour une zone lorsqu'ils sont considérés dans leur ensemble. Par exemple, un nouveau dispositif IACS utilisant un nouveau système d'exploitation, même avec tous les correctifs en exécutant un logiciel antivirus, a un SL(obtenu) plus faible lorsqu'il est directement connecté au réseau IT de l'entreprise. Inversement, si on limite l'accès physique et la connectivité réseau à une zone, des dispositifs de plus faible SL(capacité) peuvent atteindre conjointement un SL(obtenu) plus élevé pour la zone.

La sécurité du conduit entre des zones peut également avoir un effet sur le SL(obtenu) de la zone. Par exemple, un conduit utilisant une liaison de communication sans fil plutôt qu'un câble physique peut avoir un SL(obtenu) différent pour le conduit et avoir un impact sur le SL(obtenu) des zones reliées par le conduit.

De manière similaire, le SL(obtenu) de la zone en question peut être influencé par le niveau de sécurité de la zone se connectant à la zone en question. Dans l'exemple, les utilisateurs de l'application historique sont dans une zone ayant un niveau de sécurité plus faible que le serveur d'historisation. Même si le SL(obtenu) du conduit entre ces zones est Haut, le SL(obtenu) plus faible de la zone de réseau local de l'Usine A peut potentiellement avoir un effet négatif sur le SL(obtenu) de la DMZ de l'Usine A.

#### A.3.4.2.5 Maintien des niveaux de sécurité pour chaque zone

##### A.3.4.2.5.1 Généralités

Le niveau de sécurité d'un dispositif subit une érosion constante. De nouvelles vulnérabilités à la sécurité sont découvertes presque chaque semaine. Au cours de la période durant laquelle les exploitations de vulnérabilité sont connues et non traitées, l'IACS peut être menacé et le SL(obtenu) de la zone est potentiellement plus faible que le SL(cible). Cette situation concrète doit être gérée avec un plan pour maintenir le niveau de sécurité de la zone à un niveau de sécurité acceptable.

La phase de maintien du modèle de cycle de vie de la sécurité, représentée sur la Figure A.18 ci-dessous, décrit l'ensemble cyclique des activités qui sont essentielles pour maintenir la sécurité de la zone. Les événements déclenchant une réévaluation des risques comprennent, mais ne sont pas limités à:

- un changement des opérations industrielles physiques ou des changements de l'IACS susceptibles d'introduire de nouveaux risques;
- une nouvelle vulnérabilité découverte dans un module logiciel dans l'IACS;
- une nouvelle version du système d'exploitation ou un correctif d'application qui déclenche le déploiement d'un code d'exploitation sur Internet;
- des audits et analyses de sécurité périodique programmés.

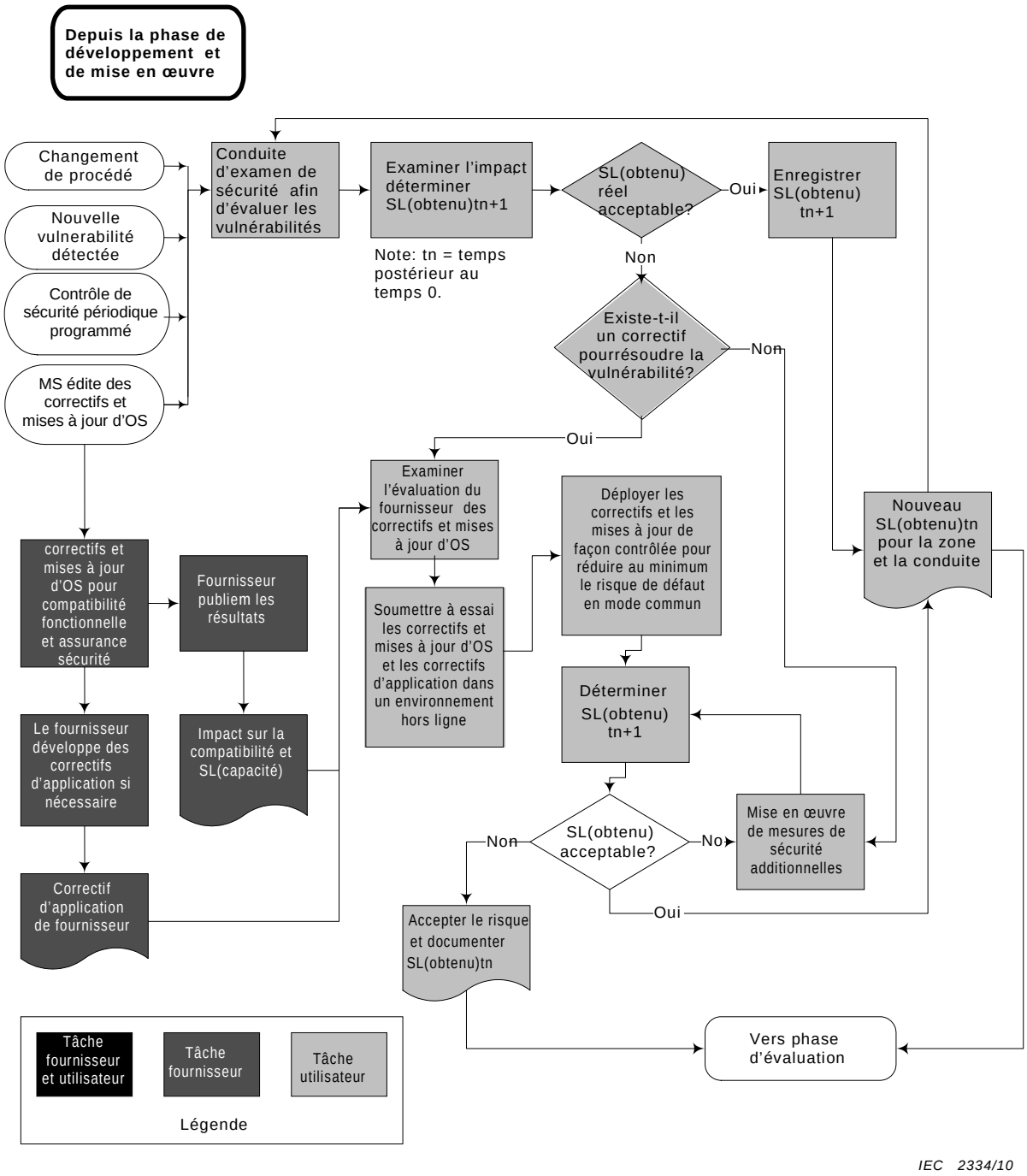



**Figure A.18 – Modèle de cycle de vie du niveau de sécurité: Phase de maintien**

### A.3.4.2.5.2 Correction de dispositifs IACS

La Figure A.18 ci-dessus présente une vue d'ensemble générale de l'intégration des correctifs dans la phase de maintien du modèle de cycle de vie du niveau de sécurité. Ce paragraphe n'est pas destiné à présenter une description complète de tous les aspects associés aux correctifs. L'objectif est de décrire l'aspect itératif de l'examen de l'état du SL(obtenu) de la zone et de la nécessité de prendre des décisions énergiques sur les correctifs à appliquer et quand les appliquer.

Les fournisseurs de dispositifs IACS et d'applications partagent avec les utilisateurs la responsabilité de contrôler les risques de sécurité. Les utilisateurs comptent sur les

fournisseurs pour comprendre le fonctionnement interne de leurs applications IACS, afin de déterminer l'applicabilité d'un correctif et d'effectuer un essai de régression automatisé pour la compatibilité de l'application IACS avec les correctifs et les révisions majeures du système d'exploitation. Étant donné que l'installation de correctifs est susceptible d'interférer avec le fonctionnement normal de l'application logicielle IACS, les utilisateurs doivent être aussi sûrs que possible que l'installation du logiciel révisé ne conduit pas à une défaillance du dispositif de commande.

Comme indiqué à la Figure A.18, l'essai de compatibilité de fournisseur est la première étape dans un plan d'essai multi-phases avant qu'une correction généralisée soit effectuée sur l'IACS en fonctionnement. Il convient que des essais additionnels soient conduits dans l'environnement cible du dispositif. Idéalement, il faudrait exécuter cela sur un dispositif en ligne identique à l'IACS actif. Si cela n'est pas possible, il convient d'envisager d'autres approches qui peuvent comprendre des essais dans un environnement virtuel ou dans un déploiement strictement contrôlé dans l'IACS actif.

À l'aide des informations de vulnérabilité du fournisseur du système d'exploitation, des informations d'applicabilité de correctif du fournisseur d'IACS, des informations de compatibilité du fournisseur d'IACS, de la connaissance de l'utilisation du dispositif IACS et finalement des essais utilisateurs, l'utilisateur doit prendre une décision sur le déploiement du correctif sur le terrain.

#### A.3.4.2.5.3 Utilisation de contre-mesures additionnelles

Il peut être nécessaire d'utiliser des contre-mesures additionnelles afin de contrôler les vulnérabilités non résolues par les correctifs ou les vulnérabilités introduites par des changements des opérations industrielles. Ceci est déterminé en évaluant le SL(obtenu) et en comparant celui-ci au SL(cible) pour la zone. Comme indiqué précédemment, cela est plus subjectif que réellement quantitativement mesuré.

Dans certains cas, le risque pour l'activité de prendre des mesures pour augmenter le SL(obtenu) peut avoir un coût prohibitif à court ou à long terme. Dans ce cas, il convient que les preneurs de décision technique documentent:

- les risques;
- les contre-mesures utilisées;
- les contre-mesures envisagées, rejetées et les raisons correspondantes;
- la recommandation pour les dirigeants d'entreprise d'accepter le risque pendant un certain temps jusqu'à ce qu'une contre-mesure ou qu'une solution de sécurité plus acceptable puisse être identifiée, soumise à essai et mise en œuvre.

Il convient que les dirigeants d'entreprise signent formellement l'acceptation documentée de cette stratégie.

#### A.3.4.2.5.4 Examens de sécurité programmés

Il convient qu'un CSMS complet comprenne un élément de conformité comprenant une évaluation périodique visant à vérifier que les pratiques et les contre-mesures de sécurité telles qu'identifiées dans la politique de sécurité d'entreprise et les normes sont utilisées dans la réduction des risques pour atteindre le niveau SL(cible). Cela est un autre déclencheur de la phase de maintien du modèle de cycle de vie de niveau de sécurité.

Un audit de sécurité peut mesurer le degré de conformité aux politiques et normes définies et conduit à des mesures qui sont utiles pour assurer la sécurité. Cependant, en plus de la vérification de l'alignement avec les pratiques requises, il convient qu'une organisation évalue périodiquement (et sur la base des déclencheurs comme décrit sur la Figure A.18), si le SL(obtenu) satisfait ou dépasse le SL(cible) dans ses zones IACS.

#### A.3.4.2.6 Pratiques en support

##### A.3.4.2.6.1 Pratiques de base

Les huit actions suivantes sont des pratiques de base:

a) Définir et valider les politiques de sécurité. Les énoncés de politiques de sécurité détaillés définissent l'engagement au niveau opérationnel à réduire chacun des risques de sécurité au cours de l'évaluation des risques.

b) Développer des procédures qui présentent des détails, telles que des actions pour prévenir, détecter et répondre aux menaces.

c) Adapter les normes des organisations internationales dans le domaine de la cyber-sécurité pour utilisation dans l'environnement IACS de l'organisation.

d) Développer des services tels que des images d'OS sécurisées et des applications communes pour une utilisation d'IACS sécurisée.

e) Identifier les outils et produits de sécurité pour mettre en œuvre des parties de la politique de sécurité. Bien que des outils et produits de sécurité, tels que des pare-feu et des VPN, puissent être utilisés dans les environnements IT et IACS, les ensembles de règles et d'applications de ces types d'outils et produits peuvent être significativement différents en raison des différents risques associés aux environnements.

f) Établir une méthodologie formelle pour accepter les risques, comprenant l'approbation du niveau de direction approprié en fonction du domaine d'application et de la documentation.

g) Mettre en œuvre des politiques, des procédures, des outils, et autres d'une manière qui réduit au minimum la surcharge administrative au niveau utilisateur sans compromettre l'efficacité. Des commandes bien conçues génèrent souvent des données de traçabilité qui peuvent être utilisées pour une vérification ultérieure.

h) Documenter les raisons de sélectionner ou ne pas sélectionner certaines contre-mesures de sécurité et les risques qu'elles contrôlent dans une déclaration d'applicabilité (SoA). Une bonne documentation sur les mesures d'amélioration de la sécurité contribue au processus de prise de décision, facilite la communication des décisions, constitue une base pour la formation des personnes afin de répondre aux incidents et aux menaces et pour les auto-évaluations ou les audits de conformité aux contre-mesures.

##### A.3.4.2.6.2 Pratiques additionnelles

NOTE 1 Les CEI/TR 62443-3-1 [6] et CEI/TR 62443-3-3 [8] aborderont les pratiques associées lorsqu'elles seront terminées.

NOTE 2 Les auteurs de la présente norme sont conscients qu'il existe de nombreux types différents de contre-mesures disponibles. Ils sont également conscients qu'inclure présentement une liste des différents types de contre-mesures donnerait au lecteur trop d'informations à assimiler ou pas assez de détails pour que le lecteur puisse appliquer correctement les contrôles à l'IACS. Par conséquent, les auteurs ont choisi de transférer la description de pratiques de sécurité IACS additionnelles dans d'autres documents, qui pourront donner au lecteur une vue plus approfondie des différent types de contre-mesures disponibles et comment les appliquer correctement à l'environnement IACS.

#### A.3.4.2.7 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [23], [24], [27], [28], [29], [30], [31], [33].

### A.3.4.3 Élément: Développement et maintenance du système

#### A.3.4.3.1 Description de l'élément

Cet élément concerne les méthodes de support nécessaires pour développer et maintenir les systèmes de technologie d'information IACS qui affectent et sont affectés par le CSMS. Il concerne les aspects de cyber-sécurité suivants: documentation des exigences, conception, approvisionnement, essais, gestion des changements, gestion des correctifs et processus de sauvegarde et de reprise.

Le point clé de cet élément est de décrire ces méthodes dans le contexte de la cyber-sécurité. L'objectif de cette approche n'est pas de reproduire une documentation décrivant les aspects fondamentaux de ces méthodes, mais plutôt pourquoi les problèmes de sécurité sont inhérents aux processus de développement et de maintenance des systèmes. Les problèmes de sécurité doivent être gérés tout au long des processus normaux de développement et de maintenance des systèmes.

#### A.3.4.3.2 Documentation des exigences

A.3.4.2 introduit le concept de niveau de sécurité cible. Le terme "exigences" fait référence aux capacités et/ou caractéristiques d'un système ou dispositif donné. Les exigences peuvent faire référence à de nombreuses caractéristiques dans de nombreux contextes: exigences relatives au système ou à un logiciel, des produits ou des opérations industrielles, fonctionnelles ou non fonctionnelles. Cependant, dans le contexte de cet élément, les "exigences système" sont définies comme étant les attributs du niveau de sécurité cible et les "exigences dispositif" sont définies comme étant les caractéristiques des contre-mesures requises pour les dispositifs dans la zone pour atteindre le niveau de sécurité cible souhaité. Étant donné que les exigences système définissent le niveau de sécurité cible, elles doivent être déterminées dans la phase de Gestion et de mise en œuvre du contrôle des risques. Ces exigences système sont souvent appelées exigences de haut niveau. Les exigences des dispositifs peuvent varier suivant les résultats de la phase de conception.

Par exemple, une exigence système pour la zone de commande pourrait limiter l'ensemble du trafic sur le réseau au trafic de contrôle et d'automatisation authentifié. Une exigence dispositif pour une console de commande d'opérateur pourrait désactiver tous les protocoles de réseau et de communication inutilisés. Dans ce cas, cette exigence dispositif pourrait remplir seulement partiellement l'exigence au niveau système. Plusieurs exigences dispositif peuvent être nécessaires pour satisfaire aux exigences système.

L'ensemble détaillé, vérifiable, d'exigences système et dispositif est à la base des méthodes d'essai et du schéma de vérification et de validation, de l'approvisionnement, et des processus de gestion des modifications et de gestion des correctifs. Il est extrêmement difficile de déterminer si la conception, l'approvisionnement, les modifications système, ou les correctifs sont non conformes au niveau de sécurité cible si les fonctionnalités spécifiques nécessaires pour atteindre ce niveau ne sont pas définies.

#### A.3.4.3.3 Conception

Il convient que la cyber-sécurité soit intégrée dans l'IACS au cours du processus de conception. Il convient que cet objectif soit pris en compte au cours des phases de développement et d'approvisionnement ainsi que pendant la maintenance du système. De nombreux documents décrivent ces processus logiques de conception de système. La présente norme n'a pas pour objectif de couvrir ce sujet. Mais il est utile de souligner qu'un aspect critique du processus de conception est qu'il convient de mettre en correspondance des contre-mesures spécifiques avec chaque exigence système afin de vérifier que les dispositifs et le système dans son ensemble satisfont au niveau de sécurité cible.

Le processus de conception couvre non seulement la préparation des spécifications du projet, mais également l'approche de vérification des plans et la vérification que le projet satisfait aux exigences définies. La vérification initiale peut être effectuée à l'aide d'une analyse sur papier. La vérification finale est effectuée en soumettant à essai le système.

Il est important de noter que de nouveaux projets sont continuellement initiés et exécutés. Afin d'éviter de devoir retravailler sur ces projets une fois qu'ils sont installés et en production, les équipes d'opérations et d'ingénierie responsables de l'exécution des projets doivent être informées des normes relatives à la cyber-sécurité applicables et spécifiques à l'industrie et des politiques d'entreprise et procédures relatives à la cyber-sécurité.

#### A.3.4.3.4 Approvisionnement

Le processus d'approvisionnement est particulièrement important pour atteindre le niveau de sécurité cible souhaité. Lors de la spécification d'un équipement nouveau ou une mise à jour destinée à un fournisseur, il est important d'inclure des exigences relatives à la cyber-sécurité. S'il existe des exigences dispositif spécifiques qui sont requises pour satisfaire aux exigences systèmes, celles-ci doivent être explicitement spécifiées dans le processus d'approvisionnement de ces dispositifs. Il peut être également nécessaire de spécifier toute exigence dispositif pour des éléments qu'il convient que le fournisseur ou l'intégrateur n'inclue pas. Certaines pratiques courantes que les fournisseurs ou intégrateurs utilisent sur leurs dispositifs peuvent conduire à des brèches indésirables de sécurité qui empêcheraient le système d'atteindre le niveau de sécurité cible. Par exemple, historiquement, les fournisseurs ont toujours placé des portes arrière sur leurs produits afin de faciliter le dépannage et améliorer les temps de réponse du service d'assistance. Ces portes arrière représentent une vulnérabilité qu'un intrus pourrait exploiter. Un agent commercial peut même ne pas être informé de l'existence de ces portes arrière et il convient d'exclure de tels points de dépannage sauf s'ils sont explicitement inclus dans les exigences d'approvisionnement.

Pour ce qui concerne la cyber-sécurité le sujet relatif au langage est trop vaste pour la présente norme. D'autres groupes ont développé ce sujet du langage et peuvent donner plus d'informations (par exemple, voir [58]).

#### A.3.4.3.5 Essais

##### A.3.4.3.5.1 Généralités

L'objectif d'un programme d'essai est de s'assurer que le système satisfait aux exigences énoncées pour le projet. Il convient qu'un système soit conçu pour satisfaire à la fois aux exigences opérationnelles et aux exigences de sécurité. Une des décisions initiales à prendre lors du développement d'un programme d'essai est de déterminer le niveau d'assurance requis par l'organisation de la part de ses fournisseurs et intégrateurs en ce qui concerne la cyber-sécurité des dispositifs ou des systèmes. Le niveau d'assurance requis pour un dispositif ou système particulier déterminera le type d'essai requis. Un fournisseur peut avoir une stratégie d'essai recommandée pour un dispositif ou un système particulier, mais l'utilisateur devra déterminer si cette stratégie d'essai est suffisante pour valider ses exigences de sécurité.

Idéalement, un système devrait être soumis à essai dans tous les états possibles afin de s'assurer que chaque condition de sécurité est satisfaite ou au moins de sorte que le risque résiduel soit connu. Bien qu'un système d'essai complet soit théoriquement possible, il ne peut pas être obtenu pour la plupart des spécifications en raison des contraintes financières et de personnel. Par conséquent, le défi est de déterminer un niveau de risque acceptable et ensuite de conduire un niveau d'essai suffisant compte tenu du risque acceptable.

Après la planification d'essai initiale, il convient de rédiger des plans et des procédures d'essai écrits pour chaque stade d'essai. Il convient que ceux-ci définissent les essais à effectuer et les résultats attendus. Il convient qu'ils comprennent la configuration du système, les entrées et sorties du système et les marges d'erreur tolérables. Lors des essais, il est important d'effectuer au moins un contrôle superficiel des résultats afin de vérifier qu'ils sont tels que prévus ou de déterminer si l'action corrective doit être effectuée. Après chaque étape des essais, il convient d'évaluer les résultats. Après les essais de validation du système, il convient qu'un rapport final soit préparé pour examiner les résultats de l'ensemble des essais et résumer les conclusions.

##### A.3.4.3.5.2 Types d'essais

Les essais de cyber-sécurité, comme les autres essais dans d'autres domaines, comprennent des essais de vérification et de validation. Selon le modèle de maturité de capacité [39]: "*La vérification confirme que les produits reflètent les exigences spécifiées pour ceux-ci. En d'autres termes, la vérification garantit qu'ils sont correctement conçus. La validation confirme que le produit, tel que fourni, est conforme à son utilisation prévue. En d'autres termes, la*

*validation assure que 'vous avez bien conçu le produit'".* Pour résumer cela, la vérification détermine si la mise en œuvre satisfait à la spécification, tandis que la validation détermine si la spécification satisfait à l'exigence.

Les essais spécifiques effectués dépendront du niveau d'essai requis, du composant ou du système soumis à essai et du type d'essai requis pour le système ou le composant. Les essais de cyber-sécurité sont généralement réalisés en trois étapes: essais de composant, essais d'intégration, et essais du système. Des essais de vérification doivent être mis en œuvre au cours des stades d'essai du composant et de son intégration, bien que des essais de validation puissent également être utiles. Des essais de vérification et de validation doivent être mis en œuvre au stade des essais système.

#### A.3.4.3.5.3 Essais de composant

Il convient que les essais de composant soient effectués par le fournisseur et vérifiés par le propriétaire du système. Le composant peut être un logiciel, un matériel, un micro logiciel ou une combinaison de ceux-ci. Le composant doit être soumis à essai pour vérifier qu'il satisfait aux exigences opérationnelles et de sécurité spécifiques. Les essais de composant sont normalement des essais de performance et sont nécessaires pour assurer que, lorsque les composants sont combinés dans un système, chaque composant individuel fonctionne correctement comme prévu.

#### A.3.4.3.5.4 Essais d'intégration

Il convient que des essais d'intégration soient effectués par l'intégrateur et vérifiés par le propriétaire du système. De tels essais mettent en œuvre des essais opérationnels et des essais de sécurité des différents composants pouvant provenir de différents fournisseurs, qui sont mutuellement connectés sur un dispositif d'essais de performance ou un banc d'essai afin de déterminer si tous les composants fonctionnent correctement ensemble avant d'être placés dans l'environnement IACS. Les essais d'intégration peuvent mettre en œuvre l'utilisation d'outils d'essai additionnels, tels que des outils de gestion et d'administration réseau, qui ne sont pas nécessaires au cours de la phase d'essai composant.

Un dispositif d'essais de performance doit avoir la configuration exacte du système de commande existant dans les installations opérationnelles. Il est fréquent qu'un système simplifié ou répliqué, dans une configuration de développement ou de laboratoire, soit le plus adapté pour les phases d'essai de composant et d'intégration. Il convient que les essais d'intégration soient basés sur cette installation d'essais de performance. Il convient de veiller à noter les différences entre la configuration des essais d'intégration et l'environnement IACS ainsi que les outils additionnels nécessaires de sorte que des éléments qui n'ont pas pu être vérifiés au cours des essais d'intégration soient soumis à essai au cours des essais système. Pour cette raison, il peut être utile, en particulier au cours de la phase d'essai d'intégration, de localiser le système simplifié ou sa copie à proximité du site d'un système opérationnel.

Dans certains cas, il est possible d'effectuer un essai d'intégration hors production afin de déterminer comment les contre-mesures de sécurité fonctionnent conjointement et comment elles s'interfacent avec les caractéristiques opérationnelles. Par exemple, des contre-mesures de sécurité qui sont appliquées à un matériel/logiciel discret peuvent être reliées via un réseau d'essais de performance de laboratoire. Dans d'autres cas, cette intégration peut être impossible. Il convient que le plan d'essai d'intégration tire profit d'un schéma d'essais de performance quelconques qui peut être configuré pour soumettre à essai des combinaisons de conditions opératoires qui peuvent être présentes dans le système opérationnel.

#### A.3.4.3.5.5 Essais système

Il convient que les essais système soient vérifiés et validés par le propriétaire. L'objectif des essais de validation est de démontrer, à l'aide de techniques, procédures et affinements de procédures (si nécessaire) appropriés, que les contre-mesures de gestion, opérationnelles et techniques pour l'IACS sont correctement mises en œuvre, sont efficaces dans leur

application, et d'assurer que les nouvelles contre-mesures de sécurité, telles que fournies et installées, satisfont aux exigences.

Les essais système peuvent comprendre des essais de pénétration du système afin d'assurer que les composants de sécurité sont capables de protéger le système contre différentes menaces comme requis pour satisfaire au niveau de sécurité de chaque zone. Dans un essai de pénétration, une personne connue tente de pénétrer les défenses de sécurité dans un système, en recherchant les faiblesses et vulnérabilités qui peuvent être exploitées pour accéder ou prendre le contrôle du système. De nombreuses entreprises sont spécialisées dans les essais de pénétration de systèmes IT conventionnels. Il peut être plus difficile de trouver une équipe qui comprenne les exigences spéciales des IACS.

Différents outils d'essai tels que des scripts d'essai, des bases de données de variables, des configurations de base avec un état initial supposé, des mesures et des outils d'étalonnage sont disponibles pour faciliter les essais réels. Il existe également des outils commercialisés et gratuits qui sont préconfigurés pour effectuer des diagnostics de routine et simuler des passerelles et des dispositifs connectés.

Si des essais de pénétration sont effectués, les performances du système pendant les essais doivent être notées en plus des résultats de l'essai de pénétration. Il est probable qu'une dégradation des performances du système ou des composants soit observée en raison de l'essai de pénétration. Il convient de noter ces dégradations de performances pour une utilisation future.

Il est important de souligner que les contre-mesures de sécurité peuvent également impliquer des personnes agissant dans le cadre de politiques et de procédures, ainsi que des vérifications manuelles de sécurité. Par exemple, une contre-mesure peut être l'installation par un ingénieur de contrôle d'un correctif de sécurité pour un matériel ou un logiciel. Le plan d'essai peut suivre la séquence d'un essai général de l'installation de correctif, en notant d'autres facteurs que celui-ci peut affecter.

#### A.3.4.3.5.6 Séparation des environnements de développement et d'essai

Les activités de développement et d'essai peuvent causer de graves problèmes, tels qu'une modification indésirable de fichiers ou de l'environnement du système ou même une défaillance du système. Pour cette raison, il est important de conduire des essais de cyber-sécurité sur des systèmes qui ne sont pas opérationnels, afin de réduire le risque de modification accidentelle ou d'accès non autorisé aux logiciels opérationnels et aux données d'activité par l'intermédiaire d'un accès inapproprié des développeurs. Si le personnel de développement et d'essai a accès au système opérationnel et aux informations qu'il contient, il peut être en mesure d'introduire du code non autorisé et non soumis à essai ou modifier les données opérationnelles. Les développeurs et les investigateurs sont également une menace pour la confidentialité des informations opérationnelles. Les activités de développement et d'essai peuvent causer des changements non prévus des logiciels et des informations si elles partagent le même environnement informatique.

La méthode préférée pour éliminer ces problèmes est l'utilisation d'un système qui est séparé du système opérationnel pour effectuer le développement et les essais initiaux. Si cela n'est pas possible, on doit veiller à ce que le système utilise un système de gestion des modifications pour documenter les modifications qui sont apportées au système et permettre d'annuler ces modifications.

### A.3.4.3.6 Gestion des modifications

Des systèmes de gestion des modifications pour SIS sont utilisés dans certaines industries sur la base d'exigences réglementaires. Pour un CSMS complet, il convient d'utiliser des systèmes de gestion des modifications pour tous les IACS. Il convient que le processus de gestion des modifications respecte les principes de séparation des fonctions afin d'éviter des conflits d'intérêt. Cela signifie que le même individu ne peut pas approuver une modification et mettre en œuvre la modification. Il convient qu'une personne techniquement qualifiée

examine les modifications proposés pour l'IACS afin d'évaluer leur impact potentiel sur les risques HSE et les risques de cyber-sécurité sur la base de politiques clairement définies. Si une des politiques est violée par le changement, il peut être nécessaire que le changement proposé soit examiné par une autre personne qualifiée afin de vérifier qu'il est valide ou rejeter le changement.

Pour que la gestion des modifications soit efficace, il convient de tenir à jour un enregistrement détaillé de ce qui est installé et de baser les propositions de changement sur ce dernier. Le système de gestion des modifications doit être associé à une procédure de sauvegarde et de restauration documentée et approuvée. Il est essentiel que l'ensemble des mises à niveau, correctifs et changements de politique du système soit mis en œuvre conformément aux procédures du système de gestion des modifications.

#### A.3.4.3.7 Gestion des correctifs

L'installation de correctifs, mises à niveau, et changements de politique, qui peut sembler inoffensive de façon isolée, peut avoir de graves implications en ce qui concerne la cyber-sécurité. Leur non installation peut également représenter un grave danger. Une méthode doit être développée pour déterminer la pertinence et la nature critique des vulnérabilités que de nouveaux correctifs sont destinés à réduire. Une telle méthode doit déterminer l'impact sur la capacité à maintenir le niveau de sécurité cible si le correctif est appliqué *et* s'il n'est pas appliqué.

NOTE La CEI/TR 62443-2-3 [5] est un rapport technique planifié sur la gestion des correctifs.

#### A.3.4.3.8 Sauvegarde et reprise

Il convient de veiller à vérifier que les processus de sauvegarde et de reprise sont compatibles avec le niveau de sécurité cible pour le système. Généralement, il convient que le processus de sauvegarde et de reprise garantisse que les copies de sauvegarde soient protégées au même degré que les originaux. Cela peut nécessiter des procédures spéciales afin de vérifier que les sauvegardes n'ont pas été corrompues et que les mécanismes de signalisation d'une sauvegarde ou une restauration réussie n'ont pas été altérés. Il convient de vérifier périodiquement la stabilité des sauvegardes afin de vérifier que le support contenant les fichiers n'a pas été dégradé et également que les données contenues sur ce support peuvent toujours être lues et utilisées. Il peut être nécessaire de conserver les anciens équipements dans des cas où d'anciennes sauvegardes ne peuvent pas être lues par un équipement plus récent.

#### A.3.4.3.9 Pratiques en support

##### A.3.4.3.9.1 Pratiques de base

Les six actions suivantes sont des pratiques de base:

a) Documenter les exigences de sécurité (menaces/contre-mesures/plans d'essai).

b) Mettre en correspondance les contre-mesures de sécurité avec les exigences de sécurité.

c) Définir un comportement attendu de réponse en cas d'échec.

d) Définir, développer et soumettre à essai la fonctionnalité des composants de sorte que le système entier satisfasse au niveau de sécurité cible.

e) Vérifier et valider la cyber-sécurité au cours des essais des composants, de l'intégration et du système.

f) Inclure une chaîne d'autorisation, un système de sauvegarde et de restauration, un système de gestion des correctifs et une procédure relative aux antivirus/programmes malveillants dans le système de gestion des modifications.

##### A.3.4.3.9.2 Pratiques additionnelles

Les cinq actions suivantes sont des pratiques additionnelles:

a) Mettre en œuvre des environnements de développement, d'essai et opérationnel séparés.

b) Utiliser des procédures indépendantes de vérification et de validation des composants.

c) Utiliser des procédures indépendantes d'intégration, de vérification et de validation.

d) Utiliser des procédures indépendantes de vérification et de validation du système.

e) Intégrer des procédures de gestion des modifications de l'IACS avec les procédures PSM existantes.

#### A.3.4.3.10 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [23], [38], [39].

### A.3.4.4 Élément: Gestion des informations et des documents

#### A.3.4.4.1 Description de l'élément

La Gestion des informations et des documents est le processus de classement des données, de protection des informations, de gestion des documents et de mise à disposition de façon appropriée des informations associées à l'IACS et au CSMS. La gestion des documents IACS peut être incluse dans le système général de conservation des enregistrements et de gestion des documents de l'organisation. La Gestion des informations et des documents assure que les données sont disponibles pendant la durée requise conformément aux exigences internes (par exemple, les politiques de l'organisation et la maintenance des dispositifs) ou externes (par exemple, légales, réglementaires et politiques).

#### A.3.4.4.2 Considérations relatives à la gestion des informations et des documents

Les informations associées au CSMS d'une organisation sont importantes, souvent sensibles et doivent être contrôlées et gérées de manière appropriée. Par conséquent, il convient que les organisations utilisent des politiques de gestion des informations et des documents complètes pour leur CSMS. Les informations associées au développement et à l'exécution d'un CSMS, des analyses des risques, des études d'impact sur l'activité, des profils de tolérance des risques, et autres peuvent être sensibles pour l'organisation et peuvent devoir être protégées, comme le sont les contre-mesures, la philosophie et les stratégies de mise en œuvre. De plus, les conditions d'activité sont changeantes et requièrent des analyses et des études mises à jour. Il convient de veiller à protéger ces informations et vérifier que les versions appropriées sont conservées. Cela implique la présence d'un système de classement des informations qui permet que les actifs de type informations bénéficient d'un niveau de protection approprié.

Une des premières étapes de la création d'un système de gestion des informations et des documents IACS est la définition de niveaux de classification des informations. Il convient que les informations (par exemple, confidentielles, restreintes et publiques) soient définies pour gérer l'accès et le contrôle des actifs d'informations. Il convient que les niveaux et pratiques associées assurent le partage, la copie, la transmission et la distribution d'actifs d'informations appropriés pour le niveau de protection requis.

Une fois que les niveaux de base ont été définis, les informations associées à l'IACS (par exemple, des informations de conception de système de commande, des évaluations de vulnérabilité, des schémas de réseau et des programmes de commande d'opérations industrielles) doivent être classées afin d'indiquer le niveau de protection requis. Il convient que ce niveau de protection soit déterminé sur la base de la sensibilité des informations et des conséquences potentielles en cas de diffusion des informations. Il convient que le niveau de classification indique le besoin et la priorité des informations, ainsi que la sensibilité des informations. Les politiques et procédures pour accéder aux informations ou documents doivent être liées aux procédures de contrôle d'accès telles que définies dans A.3.3.5, A.3.3.6 et A.3.3.7.

Il convient de développer et maintenir un processus de gestion des documents du cycle de vie à cette fin. Il convient que ce processus confirme la sécurité, la disponibilité et la convivialité de la configuration du système de commande. Cela comprend la logique utilisée dans le développement, la configuration ou la programmation pendant le cycle de vie de l'IACS. Il convient que ce processus comprenne en outre un mécanisme pour les mises à jour lorsque des changements se produisent.

Il convient de développer des politiques et procédures détaillant, la rétention, la protection, la destruction et l'élimination des informations de l'entreprise comprenant des enregistrements écrits et électroniques, des équipements et d'autres supports contenant des informations, en tenant compte des exigences légales ou réglementaires. Il convient que les politiques et les procédures développées pour le système de gestion des informations et des documents IACS soient cohérentes entre elles et entrées dans un éventuel système de gestion des informations et des documents de l'entreprise. Il convient d'effectuer des vérifications juridiques des politiques de rétention afin d'assurer la conformité aux éventuelles lois ou réglementations. Il convient d'identifier les documents nécessitant une rétention et de documenter une période de rétention.

Il est également nécessaire d'assurer que des mesures appropriées soient utilisées pour assurer que des enregistrements à long terme puissent être extraits (c'est-à-dire, convertir les données dans un nouveau format, conserver les anciens équipements qui peuvent lire les données). Il convient de développer des méthodes et des procédures pour prévenir la corruption des données de sauvegarde. Il convient d'effectuer des copies de sauvegarde à intervalles réguliers. Il convient de soumettre à essai ces sauvegardes afin de vérifier qu'elles sont encore fiables. Il convient que les procédures de restauration soient également vérifiées et soumises à essai périodiquement.

Il convient de conduire des examens périodiques des niveaux de classification des informations et des documents. La nécessité de traiter certaines informations ou certains documents avec un contrôle ou une manipulation spéciale doit être évaluée au cours de ces examens. Une méthode pour augmenter ou diminuer le niveau de classification d'une information ou un document particulier devra également être développée.

Il convient de conduire également un contrôle périodique du système de gestion des informations et des documents dans son ensemble. Cela garantit que les propriétaires des informations ou des documents se conforment aux politiques, normes ou autres exigences appropriées définies par l'organisation.

#### A.3.4.4.3 Pratiques en support

##### A.3.4.4.3.1 Pratiques de base

Les six actions suivantes sont des pratiques de base:

a) Définir des niveaux de classification des informations (c'est-à-dire, confidentielles, restreintes et publiques) pour accès et contrôle comprenant le partage, la copie, la transmission et la distribution appropriés pour le niveau de protection requis.

b) Classer toutes les informations (par exemple, les informations de conception de système de commande, les résultats d'évaluation de vulnérabilité, les schémas de réseau et les programmes de commande d'opérations industrielles) pour indiquer le besoin, la priorité et le niveau de protection requis conformément à leurs sensibilité et conséquences.

c) Examiner les informations qui requièrent un contrôle ou une manipulation spéciale de façon périodique afin de valider si une manipulation spéciale est encore nécessaire.

d) Développer et inclure des politiques et des procédures détaillant l'enregistrement, la mise à jour, la rétention, la destruction et l'élimination des informations comprenant les enregistrements écrits et électroniques, les équipements et autres supports contenant des informations. Il convient que les exigences légales ou réglementaires soient prises en compte lors du développement de ces politiques et ces procédures.

e) Développer et utiliser des méthodes pour éviter la corruption des données associées aux processus et à la journalisation des sauvegardes.

f) Confirmer la sécurité, la disponibilité et la convivialité de la configuration du système de commande. Cela comprend la logique utilisée dans le développement, la configuration ou la programmation pendant le cycle de vie de l'IACS.

#### A.3.4.4.3.2 Pratiques additionnelles

Les quatre actions suivantes sont des pratiques additionnelles:

a) Utiliser les mesures appropriées pour assurer l'enregistrement à long terme des informations qui peuvent être extraites (c'est-à-dire, convertir les données dans un nouveau format, conserver les anciens équipements qui peuvent lire les données).

EXEMPLE Des données d'émission enregistrées il y a dix ans sur un système qui n'existe plus ou sont dans un format propriétaire.

b) Effectuer des examens périodiques de la conformité à la politique de gestion des informations et des documents.

c) Effectuer des examens légaux des politiques de rétention afin d'assurer la conformité aux éventuelles lois et règlementations.

d) Chiffrer toutes les communications sur Internet contenant des informations confidentielles à l'aide d'une couche SSL (*Secure Socket Layer*) ou d'un chiffrement de force équivalente.

#### A.3.4.4.4 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la bibliographie: [6], [23], [24], [26].

### A.3.4.5 Élément: Planification et réponse aux incidents

#### A.3.4.5.1 Description de l'élément

La planification et la réponse aux incidents répond au besoin de vigilance dans les efforts visant à détecter les incidents de cyber-sécurité et d'identifier et répondre rapidement à ces incidents. Quel que soit le soin apporté à la protection d'un système, il est toujours possible que des intrusions indésirables compromettent l'intégrité du système. Les vulnérabilités de technologie continuent d'exister et les menaces externes augmentent en termes de nombre et de sophistication, de manière à nécessiter une stratégie robuste pour déterminer la planification et la réponse appropriée. La planification et la réponse aux incidents permet à une organisation de prédéfinir comment elle détecte et réagit aux incidents de cyber-sécurité. Cela permet à l'organisation d'être proactive plutôt que réactive avec son programme de cyber-sécurité.

La planification et la réponse aux incidents permet à l'organisation de planifier son comportement en cas d'incidents de sécurité et répondre ensuite conformément aux pratiques établies. Les objectifs de planification et de réponse aux incidents sont très similaires à ceux de la planification de continuité d'activité, mais concernent généralement des incidents à plus petite échelle et éventuellement ce qui concerne le temps réel. Il convient qu'une partie du plan de réponse aux incidents comprenne des procédures décrivant comment l'organisation doit répondre aux incidents, comprenant des processus de notification, des processus de documentation, et des pratiques d'investigation et de suivi ultérieur. En réponse aux urgences, assurer la sécurité du personnel et remettre les systèmes en ligne fait partie de la réponse à un incident. L'identification précoce d'un incident et une réponse appropriée peuvent limiter les dommages/conséquences de l'événement.

La planification et la réponse aux incidents est un élément clé du système de gestion pour un type quelconque de risque pour une organisation, comprenant les risques de cyber-sécurité. Des pratiques cohérentes de gestion des informations prennent en compte la nécessité de la mise en place d'un système formel de planification et réponse aux incidents.

Trois phases principales font partie de l'activité de planification et de réponse aux incidents: planification, réponse et reprise. La phase de planification comprend le développement du programme du système initial et les efforts de planification d'événements spécifiques. La phase de réponse implique la capacité à répondre aux incidents réels. La phase de reprise restaure les IACS dans leurs états opérationnels précédents.

#### A.3.4.5.2 Phase de planification

Il convient d'établir un programme pour identifier et répondre aux incidents dans l'environnement IACS. Ce programme doit comprendre un plan écrit, documentant les types d'incidents qui seront gérés et la réponse prévue pour chacun de ces incidents.

Il convient que le plan d'incident comprenne les types d'incidents qui peuvent se produire et la réponse prévue à ces incidents. Il convient d'identifier les différents types d'incidents qu'une intrusion dans un système peut causer et de les classer en fonction de leurs effets et leur vraisemblance, afin qu'une réponse appropriée puisse être formulée pour chaque incident potentiel. Il convient que ce plan comprenne des actions étape par étape qu'il convient que les différentes organisations exécutent. S'il existe des exigences d'établissement de rapport, il convient de noter celles-ci, ainsi que le lieu où il convient que le rapport soit rédigé et les numéros de téléphone afin d'éviter toute confusion dans l'établissement du rapport. Au cours de la préparation du plan de réponse aux incidents, il convient d'obtenir l'apport des différentes parties prenantes comprenant les opérations, la direction, les services juridiques et la sécurité. Il convient que ces parties prenantes signent et approuvent le plan.

Il convient que le plan d'incident comprenne des plans d'intervention couvrant la gamme complète de conséquences qui peuvent survenir en cas de défaillances dans le programme de cyber-sécurité de l'IACS. Il convient que ces plans d'intervention comprennent des procédures pour séparer l'IACS de tous les conduits non essentiels qui peuvent constituer des vecteurs d'attaque, protéger les conduits essentiels contre d'autres attaques et restaurer l'IACS dans l'état précédemment connu en cas d'incident. Il convient de les soumettre à essai périodiquement afin d'assurer qu'ils continuent de satisfaire à leurs objectifs.

Une autre information importante qui doit être incluse dans le plan d'incident est l'information du contact pour l'ensemble du personnel responsable de répondre aux incidents au sein de l'organisation. Il peut être difficile de localiser cette information lorsqu'un incident se produit.

Une fois que le plan d'incident est complet, l'organisation doit distribuer des copies à l'ensemble des groupes de personnel appropriés dans l'organisation, ainsi qu'aux organisations appropriées à l'extérieur de celle-ci. L'ensemble du personnel et des organisations associés doit être informé de ses responsabilités avant, pendant et après un incident.

En plus de la simple distribution du plan à l'ensemble des organisations appropriées, il convient que le plan soit périodiquement soumis à essai afin de garantir qu'il est toujours pertinent. Il convient que l'organisation conduise des exercices du plan de réponse aux incidents et analyse les résultats de ces exercices. Il convient que les problèmes rencontrés pendant les exercices soient gérés et que le plan soit mis à jour.

#### A.3.4.5.3 Phase de réponse

Plusieurs mesures peuvent être prises en réponse à un incident de sécurité. Celles-ci peuvent aller de l'absence d'action à une interruption totale du système. La réponse particulière dépendra du type d'incident et de son effet sur le système. Il convient de rédiger un plan écrit au cours de la phase de planification qui documente clairement les types d'incidents qui peuvent se produire et la réponse prévue à ces incidents. Celui-ci servira de guide dans des périodes de confusion ou de stress dus à l'incident.

L'organisation doit disposer de procédures en place pour identifier et signaler des incidents. Il convient que ces procédures établissent des lignes directrices pour déterminer ce qui peut constituer un incident et comment il convient que les incidents potentiels soient signalés et classés. Il convient que ces lignes directrices comprennent des informations sur la reconnaissance et le signalement d'événements inhabituels qui peuvent en fait être des incidents de cyber-sécurité. Il convient que les procédures comprennent en outre des responsabilités spéciales (par exemple, des méthodes d'identification, des exigences d'établissement de rapport et des actions spécifiques) dont le personnel doit être informé en cas d'incident de cyber-sécurité.

Si un incident est détecté, il convient que les détails de cet incident soient documentés pour enregistrer l'incident lui-même, la/les mesure(s) de réponse prises, les leçons tirées de l'incident et les mesures à prendre pour modifier le CSMS compte tenu de cet incident. Les détails de l'incident doivent être communiqués à tous les groupes appropriés dans l'organisation (par exemple, direction, IT, sécurité des procédés, automatisation et automatique et fabrication) et éventuellement aux organisations extérieures affectées par l'incident. Il est important que ces détails soient communiqués de manière opportune pour aider l'organisation à prévenir les incidents ultérieurs.

Étant donné que chaque incident peut ne pas être initialement reconnu ou détecté, il convient que l'organisation dispose de procédures en place afin d'identifier les succès et échecs de violations de cyber-sécurité. Suivant l'amplitude des dommages dus à un incident particulier, il peut être nécessaire de faire appel à des spécialistes d'investigation pour la cyber-sécurité afin d'évaluer l'efficacité de la/les réponse(s) et, en cas de perte intentionnelle, préserver la chaîne de preuves pour soutenir les efforts de recherche du coupable. Si l'incident se produit sur un système IACS critique, conduisant à une interruption de continuité d'activité, l'objectif sera probablement de rétablir le fonctionnement des installations aussi rapidement que possible. Cela peut impliquer le reformatage de disques durs et une réinstallation complète du système d'exploitation et des applications qui effacera probablement toutes les preuves. Il est important d'établir des priorités de réponse aux incidents et des pratiques avant un incident pour que chacun comprenne les objectifs et les méthodes.

#### A.3.4.5.4 Phase de reprise

Les conséquences de l'incident peuvent être mineures ou peuvent causer de nombreux problèmes dans le système. Il convient de documenter des actions de reprise étape par étape afin que le fonctionnement normal du système puisse être rétabli aussi rapidement et sûrement que possible.

Un composant important de la phase de reprise est la restauration des systèmes et des informations (c'est-à-dire, les données, les programmes et les procédures) dans leur état opérationnel. Cela requiert un système de sauvegarde et de reprise adéquat pour gérer l'ensemble de l'IACS. Celui-ci peut être constitué d'un ou plusieurs dispositifs physiques de sauvegarde et de reprise, mais il convient que ceux-ci fonctionnent conjointement pour faciliter la reprise de l'IACS.

Il convient que l'organisation dispose d'un processus d'analyse des incidents afin de gérer les problèmes qui sont découverts et assurer que ceux-ci soient corrigés. Les résultats du processus d'examen doivent être incorporés dans les politiques et procédures de cyber-sécurité appropriées, les contre-mesures techniques et les plans de réponse aux incidents. Les incidents liés à la cyber-sécurité peuvent être répartis en trois catégories:

- programmes malveillants tels que les virus, les vers, les bots, les rootkits et les chevaux de Troie;
- perte accidentelle de disponibilité, d'intégrité ou de confidentialité (comprenant la disponibilité de production);
- intrusion non autorisée s'étendant aux actifs physiques.

Les incidents dans les deux premières catégories sont typiquement gérés dans le processus de réponse aux incidents de sécurité IT. La troisième catégorie serait typiquement gérée en collaboration avec des spécialistes HSE et la direction du site.

#### A.3.4.5.5 Pratiques en support

##### A.3.4.5.5.1 Pratiques de base

Les neuf actions suivantes sont des pratiques de base:

a) Établir des procédures pour l'ensemble de l'organisation pour reconnaître et signaler des événements inhabituels qui peuvent être des incidents de cyber-sécurité.

b) Établir des procédures de planification et de réponse aux incidents comprenant:

- la désignation de la personne responsable de l'exécution du plan en cas de besoin;
- la constitution d'une équipe de réponse aux incidents qui peut être appelée, comprenant des participants des services IT, sécurité et IACS et du personnel additionnel;
- l'établissement de la responsabilité de la coordination de la défense et de la réponse à un incident;
- la gestion de l'incident depuis l'initialisation jusqu'à l'analyse finale;
- la création de procédures pour identifier, classer et hiérarchiser les incidents;
- la création de procédures pour différents types d'incidents telles que des attaques DoS, le piratage du système, les programmes malveillants, les accès non autorisés et une utilisation inappropriée.

c) Identifier des mesures proactives pour identifier automatiquement les incidents à un stade précoce.

d) Pré-planifier des scénarios de réponses aux menaces identifiées à partir des évaluations de vulnérabilité et de risque.

e) Communiquer les incidents IACS à l'ensemble des organisations appropriées (direction, IT, sécurité des procédés, automatisation et contrôle et fabrication) et aux organisations opérationnelles pour renforcer la sensibilisation.

f) Communiquer les indices et les incidents à la direction générale.

g) Conduire des analyses périodiques des incidents passés afin d'améliorer le CSMS.

h) Documenter les détails de l'incident, les leçons tirées et les éventuelles mesures à prendre pour modifier le CSMS à la lumière de cet incident.

i) Conduire des exercices afin de soumettre à essai le plan. Tenir des réunions à la suite des exercices afin d'identifier les points à améliorer.

##### A.3.4.5.5.2 Pratiques additionnelles

Les treize actions suivantes sont des pratiques additionnelles:

a) Développer des capacités d'enquête internes ou externes pour les systèmes IACS.

b) Développer un procédé pour signaler immédiatement les incidents de cyber-sécurité. Assurer que le processus a des liens avec l'équipe de gestion de crise de l'organisation. Former le personnel à l'aide d'exemples d'incidents à signaler afin qu'il puisse mieux satisfaire aux exigences de signalement.

c) Comprendre les liens potentiels entre l'IT, la sécurité et l'IACS et incorporer cette compréhension dans les procédures.de réponse associées aux incidents de sécurité

d) Développer, soumettre à essai, déployer et documenter le processus d'investigation d'incident.

e) Développer des politiques d'entreprise pour signaler les incidents de cyber-sécurité et le partage des informations d'incident avec des groupes au sein de l'industrie et des agences réglementaires lorsque les politiques d'entreprise le permettent.

f) Spécifier les rôles et les responsabilités en ce qui concerne le respect des réglementations locales et/ou d'autres parties prenantes critiques dans un programme d'investigation d'incident interne et partagé.

g) Étendre l'investigation des incidents sur la base des conséquences potentielles qui auraient pu se produire à la place des conséquences réelles, en reconnaissant que l'incident informatique peut avoir une origine malveillante. Il peut être nécessaire d'élever le niveau d'investigation d'un incident suivant la gravité potentielle de l'incident.

h) Développer des méthodologies et des mécanismes afin de garantir que les actions correctives identifiées à la suite d'un incident de cyber-sécurité ou d'un exercice ont été intégralement mises en œuvre.

i) Dispenser une formation de réponse aux incidents de sécurité aux équipes de formation inter-fonctionnelles de l'organisation.

j) Examiner les résultats finaux d'investigation d'incident avec l'ensemble du personnel dont les tâches sont concernées par les observations. Analyser l'incident en tenant compte des tendances et enregistrer celui-ci afin qu'il puisse être utilisé pour des analyses de tendance ultérieures.

k) Favoriser des activités d'assistance mutuelle au sein d'une industrie et entre industries afin de tirer des enseignements des expériences d'autres personnes concernant l'évaluation, la réponse, l'investigation, la communication et la correction des incidents de cyber-sécurité.

l) Identifier les conséquences précédemment imprévues, en particulier celles qui peuvent affecter l'application future du plan. Les incidents peuvent comprendre des événements à risque, des quasi-incidents et des dysfonctionnements. Cela concerne également les faiblesses observées ou suspectées dans le système ou les risques qui peuvent ne pas avoir été précédemment reconnus.

m) Incorporer une planification de réponse en cas d'urgence en planification de réponse aux incidents.

#### A.3.4.5.6 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [26], [36].

## A.4 Catégorie: Surveillance et amélioration du CSMS

### A.4.1 Description de la catégorie

Un CSMS comprend toutes les mesures nécessaires pour créer et maintenir un programme de cyber-sécurité. Le domaine d'application et le niveau de cet effort dépendent des objectifs, de la tolérance des risques et de la maturité du programme de cyber-sécurité de l'organisation. Il convient que ce système de gestion prenne en compte les exigences, méthodes, dispositifs, interfaces et personnel nécessaires pour mettre en œuvre le programme de cyber-sécurité.

La surveillance et l'amélioration du CSMS met en œuvre l'assurance que le CSMS est utilisé et l'examen du CSMS lui-même afin de déterminer son efficacité. La Figure A.19 représente les deux éléments qui font partie de la catégorie:

- La conformité et
- l'examen, l'amélioration et la maintenance du CSMS.

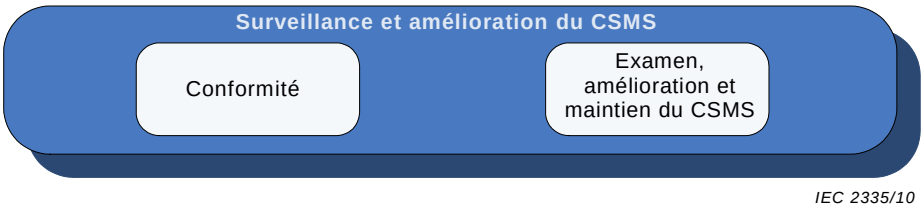



**Figure A.19 – Vue graphique de la catégorie: Surveillance et amélioration du CSMS**

### A.4.2 Élément: Conformité

#### A.4.2.1 Description de l'élément

La conformité est le processus consistant à valider que l'organisation applique le programme de cyber-sécurité qui a été développé. Le CSMS n'est satisfaisant que dans la mesure où une organisation est en mesure de l'appliquer. L'organisation doit être tenue responsable des politiques et procédures définies comme faisant partie du CSMS ou bien le système de gestion sera inefficace. En validant sa conformité au CSMS, l'organisation peut utiliser les processus intégrés du CSMS pour améliorer le système global dans le futur.

La validation de la conformité au CSMS comporte des activités planifiées ou non. Des examens périodiques du CSMS sont considérés comme des activités planifiées, mais une réponse à un incident de cyber-sécurité est considérée comme une activité non planifiée.

Établir des indicateurs de performances clés (KPI: *key performance indicators*) constitue un moyen pour l'organisation de mesurer les performances du CSMS. L'utilisation de KPI qui sont compatibles avec les principales solutions des groupes industriels ou d'autres organisations permettra d'évaluer les performances du CSMS.

#### A.4.2.2 Activités planifiées et non planifiées

De nombreux paragraphes du CSMS contiennent le concept d'examens périodiques d'un aspect particulier afin de suivre ou améliorer le CSMS au cours du temps. Ces examens font tous partie du modèle de maturité d'un programme de sécurité comme décrit dans la CEI/TS 62443-1-1. Les examens conduits dans le cadre habituel d'un CSMS évitent que le système se dégrade au cours du temps en raison de nouvelles menaces, vulnérabilités ou situations qui n'existaient pas lorsque le système a été initialement développé.

Des menaces, vulnérabilités ou situations critiques peuvent également survenir qui doivent être traitées avant l'examen périodique suivant. Celles-ci constitueraient des activités non planifiées et peuvent nécessiter une réévaluation du CSMS afin d'assurer son efficacité.

Des examens et audits périodiques du CSMS déterminent si les politiques, procédures et contre-mesures souhaitées ont été correctement mises en œuvre et qu'elles sont conduites comme prévu. Dans l'environnement IACS, les auditeurs doivent pleinement comprendre les politiques et procédures de cyber-sécurité de l'entreprise et les risques HSE spécifiques associés à une installation et/ou des opérations industrielles particulières. On doit veiller à ce que les audits n'interfèrent pas avec les fonctions de commande de l'équipement IACS. Il peut être nécessaire de mettre un système hors ligne avant que l'audit puisse être conduit. Il convient que l'audit vérifie que:

- les politiques, procédures et contre-mesures présentes au cours des essais de validation du système sont encore installées et fonctionnent correctement dans le système opérationnel;
- le système opérationnel est exempt de failles de sécurité;

NOTE En cas d'incident, il est attendu que des journaux et enregistrements soient générés, afin d'enregistrer la nature et le degré de l'incident.

- le programme de gestion des modifications est rigoureusement suivi par une trace d'audit des examens et approbation de toutes les modifications.

Une activité particulière non planifiée qui peut déclencher un examen du CSMS peut être l'ajout ou le retrait d'actifs de l'IACS. Une pratique courante pendant la maintenance ou une intervention technique sur le système peut être l'ajout, la mise à niveau ou le retrait d'équipement ou de logiciel de l'IACS. Un processus de gestion des modifications bien défini et appliqué permet de détecter ce type d'événement, qui peut déclencher un examen ou audit du CSMS. Cet examen ou audit garantirait que le changement n'a pas d'effet indésirable sur la cyber-sécurité de l'IACS. Un autre exemple d'activité non planifiée serait une réponse à une attaque virale sur une installation. Après que le système CSMS a été utilisé pour répondre et traiter l'incident, il convient de conduire un examen ou audit du CSMS afin de déterminer quelle défaillance a permis au virus de se propager.

Des examens ou audits de cyber-sécurité (internes ou externes) fournira à l'organisation des données utiles afin d'améliorer le CSMS. Il convient que les résultats de ces examens ou audits comprennent des informations aussi détaillées que nécessaire afin d'assurer que les exigences légales ou réglementaires éventuelles soient satisfaites et que toute modification indiquée par l'examen ou l'audit puisse être effectuée. Il convient que les résultats soient envoyés à l'ensemble du personnel approprié (c'est-à-dire, les parties prenantes, la direction et le personnel de sécurité).

#### A.4.2.3 Indicateurs de performances clés (KPI)

Les KPI permettent à l'organisation de déterminer les performances du CSMS et contribue à diriger éventuellement des ressources vers des secteurs qui peuvent nécessiter une amélioration. Il convient que les KPI, dans la mesure du possible, soient des grandeurs quantitatives (c'est-à-dire, des nombres ou des pourcentages) indiquant les performances d'une partie particulière du CSMS dans des conditions prévues.

Étant donné qu'il convient d'exprimer les examens ou audits du CSMS en utilisant ces KPI, il est important de sélectionner des indicateurs qui sont pertinents, significatifs et cohérents avec le CSMS et autres exigences de l'organisation. Les résultats des activités périodiques planifiées peuvent être exprimés par les performances exprimées par un ensemble de critères prédéfinis afin de générer des performances de sécurité et des tendances de sécurité. Les résultats d'activités non planifiées peuvent être exprimés par l'efficacité du CSMS pour gérer un événement ou incident non planifié.

Il convient que les données de capacité organisationnelle fassent partie des indicateurs de performance. Il convient que les entreprises suivent le pourcentage de personnel affecté à des rôles IACS et le pourcentage de ce personnel qui a satisfait aux exigences de formation et de qualification pour ses rôles. Bien que ces données puissent sembler ésotériques, des problèmes systémiques peuvent être détectés avant d'être mis en évidence par des résultats d'audit médiocres.

Les essais de performance de KPI et les résultats des examens ou audits comparés à d'autres organisations ou exigences est une bonne méthode pour valider le CSMS. Si les données d'essai de performance sont collectées sur une certaine période, il peut être possible pour l'organisation de déterminer des tendances des menaces ou des contre-mesures. Celles-ci peuvent indiquer des emplacements auxquels il peut être nécessaire d'analyser les exigences du CSMS dans le cadre du paragraphe d'examen, d'amélioration et de maintenance du CSMS (voir A.4.3).

#### A.4.2.4 Pratiques en support

##### A.4.2.4.1 Pratiques de base

Les deux actions suivantes sont des pratiques de base:

a) Donner l'assurance que le caractère approprié de l'environnement de contrôle et la conformité aux objectifs globaux de cyber-sécurité sont satisfaits. Détecter si des ajouts, des mises à niveau ou des suppressions (c'est-à-dire, des correctifs de logiciel, des mises à niveau d'application et des changements d'équipement) ont introduit des expositions de sécurité.

b) Confirmer que, sur une période d'audit périodique spécifiée, tous les aspects du CSMS fonctionnent comme prévu. Il convient qu'un nombre suffisant d'audits soient planifiés de sorte que la tâche d'audit soit uniformément étalée sur la période choisie. Il convient que la direction veille à ce que des audits périodiques soient conduits. Il convient que la direction s'assure qu'il soit possible de:

- vérifier que les procédures documentées sont suivies et satisfont à leurs objectifs souhaités;
- valider que les contrôles techniques (c'est-à-dire, pare-feu et contrôles d'accès) sont en place et fonctionnent comme prévu, de façon régulière et continue.

#### A.4.2.4.2 Pratiques additionnelles

Les trois actions suivantes sont des pratiques additionnelles:

a) Exiger que le programme de mesures d'indices de cyber-sécurité soit basé sur les sept étapes clés suivantes:

1) définir les objectifs du programme de mesures d'indices;
2) décider des indices à générer afin de mesurer le degré d'adoption et de conformité aux politiques et aux procédures définies dans le CSMS:
   - évaluer de façon proactive les éventuelles vulnérabilités de sécurité potentielles (par exemple, % de faiblesses d'audit de sécurité corrigées à la date prévue);
   - suivre la mise en œuvre et l'utilisation des mesures de sécurité et préventives (par exemple, % de conformité aux normes de sécurité).
3) développer des stratégies pour générer les indices;
4) établir des essais de performance et des cibles;
5) déterminer comment les indices sont présentés et à qui;
6) créer un plan d'action et agir conformément à celui-ci;
7) établir un cycle d'examen/amélioration de programme.

b) Examiner les résultats des audits, auto-évaluations, rapports d'incident de cyber-sécurité et les retours transmis par les parties prenantes clés afin de comprendre l'efficacité du CSMS.

c) Conduire des examens de sécurité opérationnelle sur l'IACS par des ingénieurs IACS formés à la sécurité. De plus, les problèmes de sécurité sont fréquemment examinés à un niveau plus large par un comité directeur.

### A.4.2.5 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la Bibliographie: [24], [26], [35], [49], [50].

## A.4.3 Élément: Examen, amélioration et maintenance du CSMS

### A.4.3.1 Description de l'élément

Le processus de surveillance et d'examen continus du CSMS permet à une organisation d'établir, et de prouver, qu'elle satisfait aux objectifs, politiques et procédures définies dans le CSMS. Les KPI définis au cours du développement du CSMS sont utilisés pour évaluer les performances du CSMS au cours du processus d'examen de conformité. L'élément Conformité vérifie que le CSMS fonctionne tel que défini, tandis que le présent élément vérifie que les exigences utilisées pour développer le CSMS satisfont aux objectifs de cyber-sécurité de l'organisation.

Des méthodes de vérification interne, telles que les audits de conformité et les investigations d'incident, permettent à l'organisation de déterminer l'efficacité du système de gestion et s'il fonctionne conformément aux attentes. Il est également important d'établir que le système de gestion satisfait encore aux objectifs et aux cibles définis au cours du processus de planification. S'il existe des écarts par rapport aux objectifs ou cibles originaux, des modifications systématiques du système de gestion peuvent être nécessaires.

Étant donné que les menaces et les technologies relatives à la sécurité évoluent, il est attendu que le programme de cyber-sécurité de l'organisation évolue également, afin de prendre en compte les nouvelles menaces et les capacités disponibles. Il convient que les organisations suivent, mesurent et améliorent les efforts de sécurité afin de maintenir en sécurité les personnes, propriétés, produits, opérations industrielles, données, et systèmes d'information.

L'objectif global est d'assurer que le CSMS reste efficace en incorporant des améliorations apportées sur la base des nouvelles menaces, des nouvelles capacités et des examens périodiques. Une attention continue à la sécurité est un indicateur démontrant que la cyber-sécurité est une valeur essentielle de l'entreprise.

#### A.4.3.2 Examen de la conformité au CSMS

La conformité au CSMS a été abordée dans un élément précédent. Elle vérifie que l'organisation respecte les politiques et procédures définies dans le CSMS. Dans le cadre du processus de conformité, des indicateurs clés de performances (KPI) ont été définis afin de mesurer les performances du CSMS de l'organisation. Des valeurs médiocres de ces KPI dans un cycle d'examen peuvent indiquer un programme particulier qui peut être corrigé par des solutions simples. Des valeurs médiocres pour un grand nombre des KPI ou dans le même KPI lors d'examens répétés peuvent indiquer des problèmes systémiques du CSMS. Cela peut indiquer que la formation ou des améliorations doivent être améliorée, que les ressources sont insuffisantes ou que les procédures mises en œuvre sont irréalisables. La gestion du CSMS comporte ces évaluations. Que les KPI soient évalués par des audits externes ou internes, il est utile de consulter l'organisation dont les actions sont mesurées, afin de faciliter cet examen.

Il est important que le CSMS comprenne les exigences d'amélioration des résultats de conformité. Il convient que la/les personne(s) responsable(s) soient formellement chargées de développer une stratégie à long terme pour l'amélioration afin d'assurer une amélioration constante et économique au cours du temps.

#### A.4.3.3 Mesure et examen de l'efficacité du CSMS

La mesure de l'efficacité du CSMS comprend au minimum l'examen des données d'incident. Plus la capacité d'une organisation à détecter les échecs et les succès de violations de sécurité et enregistrer ceux-ci en tant qu'incidents est grande, plus sa capacité à mesurer l'efficacité du CSMS dans la diminution des risques est grande. Les données d'incident comprennent le nombre d'incidents, le type ou la classe d'incidents et l'impact économique des incidents. Ces données sont extrêmement importantes à la fois pour comprendre l'impact économique actuel de menaces de cyber-sécurité et évaluer l'efficacité de contre-mesures spécifiques utilisées.

Bien que l'analyse des données d'incident puisse mesurer l'efficacité du CSMS dans le passé, l'équipe de gestion du CSMS est également chargée de maintenir l'efficacité du CSMS dans le futur. Pour ce faire, il est nécessaire de suivre les changements de facteurs susceptibles d'augmenter ou diminuer son efficacité dans le futur. Des facteurs clés à surveiller sont les suivants:

- le niveau de risque, qui peut changer en raison d'un changement de menace, de vulnérabilité, de conséquence ou de vraisemblance;
- la tolérance des risques de l'organisation;

- la mise en œuvre de systèmes ou d'opérations industrielles nouveaux ou modifiés;
- les pratiques dans l'industrie;
- les contre-mesures techniques et non techniques disponibles;
- les exigences légales et réglementaires.

Il convient que le CSMS d'une organisation soit examiné à intervalles réguliers, afin d'évaluer son efficacité passée et future. Il convient que cet examen comprenne une évaluation périodique des politiques et des procédures de cyber-sécurité pour confirmer que ces politiques et procédures sont en place et fonctionnent et satisfont aux exigences de sécurité légales, réglementaires et internes. Dans des circonstances appropriées, les évaluations s'appliquent également aux politiques et aux procédures des partenaires d'activité de l'organisation, tels que les fournisseurs, les fournisseurs de service d'assistance, les coentreprises ou les clients.

Conformément aux examens périodiques, il convient que les changements majeurs des facteurs énumérés ci-dessus déclenchent également l'examen des aspects associés du CSMS. Il convient qu'une organisation détermine un ensemble de déclencheurs et de seuils de changements, qui déclencheraient un tel examen. Il convient que ces déclencheurs comprennent les facteurs suivants:

- Facteurs internes: Sur la base des performances du CSMS et les résultats des KPI et d'autres indicateurs internes adaptés (par exemple, la tolérance aux risques, la gestion des changements, et autres).
- Facteurs externes: Un changement des menaces dans l'environnement, des bonnes pratiques de l'industrie, des solutions disponibles et des exigences juridiques peuvent indiquer un besoin ou une opportunité d'amélioration du CSMS.

Il convient que l'organisation assignée à la gestion des modifications du CSMS soit également responsable de l'examen des déclencheurs et des seuils des changements et de leur utilisation pour initier le processus d'examen.

#### A.4.3.4 Implications légales et réglementaires pour le CSMS

L'environnement légal et réglementaire auquel l'organisation est soumise peut changer au cours du temps. L'organisation peut encore être conforme au CSMS tel qu'il a été initialement défini, mais le CSMS peut ne plus satisfaire aux exigences légales et réglementaires en vigueur.

Il convient que l'organisation examine périodiquement ses exigences légales et réglementaires et identifie les domaines dans lesquels ils peuvent affecter le CSMS. De plus, il convient que tous les changements majeurs des exigences légales et réglementaires, tels que les exigences majeures nouvelles ou mises à jour, déclenchent un examen du CSMS pour assurer qu'il satisfait aux nouvelles exigences.

#### A.4.3.5 Gestion des modifications du CSMS

Pour avoir un système coordonné, il convient qu'une organisation/équipe soit assignée pour gérer et coordonner le raffinement et la mise en œuvre des changements du CSMS. Cette organisation/équipe pourrait être une organisation de type matriciel basée sur des personnes clés de différentes organisations d'activité. Il convient que cette équipe utilise une méthode définie pour effectuer et mettre en œuvre des changements.

Plusieurs facteurs internes et externes nécessitent des changements du CSMS. La gestion de ces changements requiert la coordination avec les différentes parties prenantes. Lors de la mise en œuvre des changements du système de gestion, il est important d'examiner des effets secondaires possibles concernant le fonctionnement ou la sécurité du système. La sécurité de l'IACS doit également prendre en compte les différentes organisations, pratiques et exigences de réponse lors de l'incorporation des améliorations. Il convient que des

procédures écrites soient développées pour gérer les changements du CSMS. Ce procédé peut comprendre les étapes suivantes:

a) Définition du système de gestion actuel

Avant de pouvoir affiner le CSMS, il est nécessaire de connaître et comprendre le système de gestion actuel. Il convient que toutes les politiques concernant la cyber-sécurité soient examinées de sorte que toutes les parties prenantes comprennent clairement la politique actuelle et comment elle est mise en œuvre. De plus, il convient que tous les actifs et procédures associés au CSMS soient identifiés.

b) Définition des procédures pour proposer et évaluer des changements du CSMS

Une fois que le système de gestion actuel est connu, il convient d'examiner la conformité et l'efficacité, comme décrit précédemment. Il convient que les faiblesses ou les brèches dans le système de gestion soient identifiées et des corrections proposées. Il convient que l'évaluation du système de gestion identifie des domaines dans lesquels des modifications peuvent être nécessaires. De plus, les bonnes pratiques de l'industrie et les exigences décrites dans la présente norme peuvent être prises en compte dans la définition des changements qui renforceraient le CSMS. La sélection de nouvelles contre-mesures suivra les principes décrits dans l'élément Gestion et mise en œuvre du contrôle des risques de la présente norme (voir A.3.4.2). Une fois définis, il convient que les modifications proposées pour le CSMS soient documentés d'une manière concise de sorte qu'ils puissent être présentés de façon cohérente aux autres parties prenantes.

c) Proposition et évaluation des modifications du CSMS

Une fois les changements identifiés et documentés, il convient de les présenter aux parties prenantes. Il convient que les changements proposés soient examinés afin de déterminer s'ils produisent des effets secondaires négatifs ou imprévus. Il convient de les évaluer pour déterminer si des modifications doivent être apportées au CSMS en fonction des exigences et suites d'essai initiales. Au fur et à mesure que les nouvelles fonctionnalités sont développées, la réaction de nombreuses organisations est d'incorporer les dernières technologies dans le système. Dans l'environnement IACS, il est important de valider une nouvelle technologie ou solution de cyber-sécurité avant de l'intégrer.

d) Mise en œuvre des modifications du CSMS

Une fois que les parties prenantes ont approuvé le changement, il convient que les modifications du CSMS soient mises en œuvre. Il convient que des changements de la politique respectent les procédures de l'entreprise pour les changements de politique et, au minimum, il convient que ces changements soient documentés et que l'approbation écrite des parties prenantes clés soit obtenue. Il est nécessaire d'apporter une attention particulière à l'implication des fournisseurs dans les essais, validation et contrôle des systèmes.

e) Surveillance des modifications du CSMS

Une fois le CSMS nouveau ou révisé en place, il est important de surveiller et évaluer ses performances. Il convient qu'un examen du système de gestion soit effectué de façon périodique et chaque fois qu'il se produit des modifications du CSMS.

#### A.4.3.6 Pratiques en support

##### A.4.3.6.1 Pratiques de base

Les douze actions suivantes sont des pratiques de base:

a) Utiliser une méthode pour déclencher un examen du niveau de risque résiduel et de la tolérance des risques lors des changements de l'organisation, de la technologie, des objectifs de l'activité, des opérations industrielles ou d'événements externes comprenant des menaces et des changements identifiés dans le climat social.

b) Analyser, enregistrer et rapporter les données opérationnelles pour évaluer l'efficacité ou les performances du CSMS.

c) Analyser les résultats des examens et audits périodiques du CSMS pour déterminer si une modification est nécessaire.

d) Examiner les politiques et procédures du CSMS inefficaces pour déterminer les causes initiales en cas de problèmes systémiques. Les actions sont identifiées non seulement pour résoudre le problème, mais également pour réduire au minimum et prévenir les réitérations.

e) Examiner les menaces potentielles et conduire une analyse d'impact de façon périodique afin de déterminer si des contre-mesures sont requises.

f) Identifier les réglementations, législation, obligations et exigences contractuelles de cyber-sécurité applicables et modifiées.

g) Mettre en œuvre les parties prenantes clés dans l'organisation pour confirmation sur des domaines particuliers pour investigation et planification complémentaires. Il convient que les parties prenantes clés comprennent des membres personnel de l'ensemble des différents groupes affectés par le CSMS (c'est-à-dire, IT, IACS et sécurité).

h) Identifier les actions correctives et préventives pour améliorer plus avant les performances.

i) Hiérarchiser les améliorations du CSMS et mettre en place des plans pour les mettre en œuvre (c'est-à-dire, planifier des budgets et des projets).

j) Mettre en œuvre tous les changements en utilisant les processus de gestion des modifications au sein de l'organisation. Une attention particulière doit être apportée à l'implication des fournisseurs dans les essais, validation et contrôle des systèmes en raison des implications HSE de l'environnement IACS.

k) Valider que les actions convenues lors d'audits et d'examens précédents ont été mises en œuvre.

l) Communiquer les plans d'action et les domaines à améliorer à l'ensemble des parties prenantes et du personnel affecté.

#### A.4.3.6.2 Pratiques additionnelles

Les deux actions suivantes sont des pratiques additionnelles:

a) Exiger que le programme de mesure d'indices de cyber-sécurité soit basé sur les sept étapes clés énumérées ci-dessous:

   1) définir les objectifs du programme de mesures d'indices;

   2) décider des indices à générer afin de mesurer l'efficacité du CSMS dans la réalisation des objectifs de sécurité de l'organisation;

      NOTE Il peut être utile de fournir une vue rétrospective du niveau de préparation de sécurité en suivant le nombre et la gravité des incidents passés, y compris les petits événements modélisés.

   3) développer des stratégies pour générer les indices;

   4) établir des essais de performance et des cibles;

   5) déterminer comment les indices sont présentés et à qui;

   6) créer un plan d'action et agir conformément à celui-ci;

   7) établir un cycle d'examen/d'amélioration de programme.

b) Appliquer de nombreuses stratégies différentes pour assurer l'amélioration continue des activités de cyber-sécurité. Les stratégies sont adaptées au risque et dépendent de la culture d'entreprise, des systèmes existants et de la taille ou de la complexité des systèmes numériques. Certaines stratégies potentielles sont les suivantes:

   - conduire des activités d'essais de performance de sécurité à l'intérieur et à l'extérieur de l'industrie comprenant l'utilisation d'une validation externe pour contribuer à valider les améliorations;

   - rechercher activement le retour des employés sous forme de suggestions et communiquer à la direction supérieure sur les limitations et opportunités de performances;

- utiliser des méthodologies d'entreprise normalisées, telles que Six Sigma™, pour mesurer, analyser, améliorer et soutenir les améliorations de cyber-sécurité.

#### A.4.3.7 Ressources utilisées

Cet élément est en partie basé sur le matériel décrit dans les références suivantes, toutes répertoriées dans la bibliographie: [24], [26], [35], [49].

# Annexe B
(informative)

# Processus de développement d'un CSMS

## B.1 Vue d'ensemble

L'Article 4 et l'Annexe A détaillent les éléments individuels associés à un CSMS complet et intégré. Développer un CSMS fonctionnel est un projet qui peut durer des mois ou des années avant d'aboutir. La présente annexe est focalisée sur l'organisation et la nature itérative des activités associées au développement des éléments du CSMS. Les objectifs de cette annexe sont les suivants:

- donner des informations clés sur le succès avec lequel des organisations ont séquencé ces activités, et signaler les pièges courants associés à l'ordre dans lequel les éléments d'un CSMS sont gérés;
- présenter un guide pas à pas auquel une organisation peut faire référence lorsqu'elle commence le processus d'établissement d'un CSMS;
- présenter un guide pas à pas pour utiliser la présente norme.

## B.2 Description du processus

La Figure B.1 présente les six activités du CSMS de niveau supérieur et leurs relations. Les figures suivantes de cette annexe décomposent chacune d'entre elles de manière plus détaillée. Bien que la Figure B.1 présente les relations mutuelles entre l'ensemble des activités, ces relations ne sont pas décrites de manière détaillée dans la présente annexe. Cela a pour but d'uniformiser la représentation concise avec l'ensemble des sujets décrits.

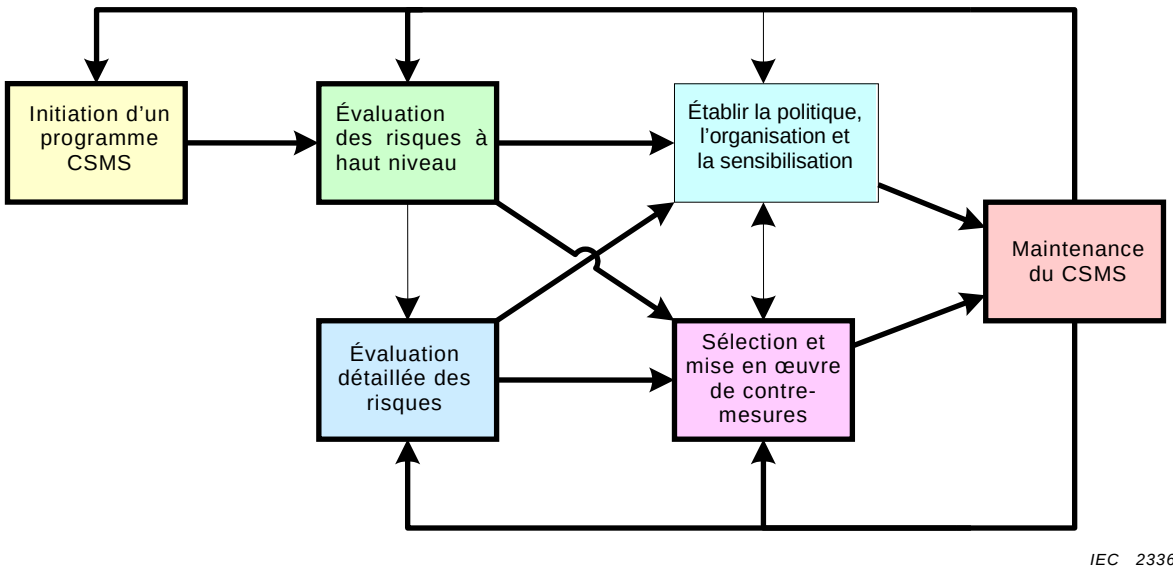



**Figure B.1 – Activités de niveau supérieur pour établir un CSMS**

L'activité "Initiation du programme CSMS" établit le programme sur des fondations solides en définissant l'objectif, le soutien organisationnel, les ressources et le domaine d'application pour le CSMS. Démarrer avec cette activité maximise l'efficacité du projet, comme c'est le cas pour tout programme à large impact. Le domaine d'application initial peut être plus restreint que souhaité, mais peut croître avec le succès du programme.

L'évaluation des risques définit le contenu du CSMS. L'activité "Évaluation des risques à haut niveau" identifie les menaces, la vraisemblance de leur réalisation, les types généraux de vulnérabilités et les conséquences. L'activité d'évaluation détaillée des risques ajoute une évaluation technique détaillée des vulnérabilités au tableau des risques. Il est important d'aborder l'évaluation des risques à un haut niveau dans un premier temps. Un piège courant est de consommer des ressources de façon précoce pour effectuer l'évaluation détaillée de vulnérabilité et recevoir une réponse faible à ces résultats techniques parce que le contexte des risques globaux de haut niveau n'a pas été établi.

Les deux activités "Établir, la politique, l'organisation et la sensibilisation" et "Sélection et mise en œuvre de contre-mesures" diminuent directement les risques au niveau de l'organisation. Ces activités mettent en œuvre des décisions de haut niveau et de niveau inférieur, régies par des évaluations des risques à haut niveau et détaillées. L'activité "Établir, la politique, l'organisation et la sensibilisation" couvre la création de politiques et procédures, l'attribution de responsabilités organisationnelles et la planification et l'exécution de formation. L'activité "Sélection et mise en œuvre de contre-mesures" définit et met en œuvre les défenses de cyber-sécurité techniques et non techniques de l'organisation. Ces deux activités principales doivent être conduites de façon coordonnée. Cela est dû au fait que dans la plupart des cas, les politiques et procédures, la formation et l'attribution de responsabilités associées sont essentielles pour qu'une contre-mesure soit efficace.

L'activité "Maintenance du CSMS" comprend des tâches pour déterminer si l'organisation se conforme à ses politiques et procédures du CSMS, si le CSMS est efficace pour satisfaire aux objectifs de cyber-sécurité de l'organisation et si ces objectifs doivent changer compte tenu d'événements internes ou externes. Cette activité définit à quel moment une révision majeure ou une évaluation détaillée des risques est nécessaire ou peut précipiter un changement des paramètres du programme initial. Elle peut également apporter des éléments pour l'amélioration des politiques, des procédures, des décisions organisationnelles afin de maximiser l'efficacité de contre-mesures ou souligner des faiblesses à corriger dans la mise en œuvre des contre-mesures sélectionnées. Les organisations signalent que l'activité Maintenance du CSMS est très difficile, étant donné que l'enthousiasme initial pour le programme peut s'atténuer alors que d'autres priorités surviennent. Cependant, sans une attention adéquate pour cette activité, les résultats positifs du programme peuvent être finalement annulés, parce que l'environnement dans lequel le programme fonctionne n'est pas stable.

La suite de la présente annexe donnera au lecteur une meilleure compréhension des six activités CSMS de haut niveau. Le numéro d'élément ou de sous-élément a été référencé afin d'aider le lecteur de la présente norme à trouver sur un sujet particulier plus d'informations.

## B.3 Activité: Initiation du programme CSMS

La Figure B.2 illustre les étapes impliquées dans l'activité "Initiation du programme CSMS".

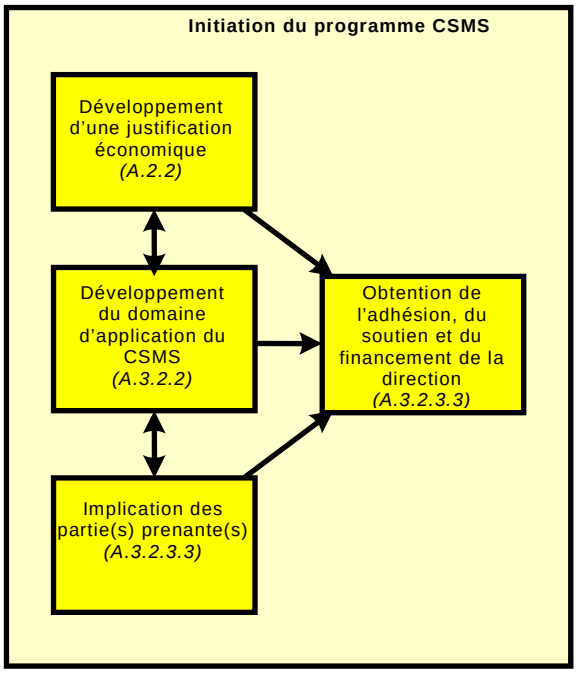



**Figure B.2 – Activités et dépendances pour l'activité: Initiation au programme CSMS**

Le résultat souhaité de l'activité "Initiation au programme CSMS" est l'obtention de l'adhésion, du soutien et du financement du CSMS. Pour ce faire, les premières étapes décrites à la Figure B.2 développent un exposé d'activité qui justifiera le programme auprès de la direction et le domaine d'application proposé pour le programme. Conjointement avec ces étapes, des individus qui sont des parties prenantes, sur la base de cet exposé et du domaine d'application, sont identifiés et impliqués. Il est plus efficace d'identifier ces parties prenantes en amont et dès que possible de les faire participer à l'effort d'obtention de l'adhésion de la direction au programme. Un cadre d'organisation efficace pour la sécurité peut ensuite être construit, à partir du haut. Un piège commun est d'initier un programme CSMS sans avoir au moins un exposé de haut niveau qui relie la cyber-sécurité à l'organisation spécifique et à sa mission. Les activités de cyber-sécurité requièrent de l'organisation des ressources et bien qu'un programme puisse commencer avec le consensus général sur le fait que la cyber-sécurité est bénéfique, la dynamique peut être rapidement perdue au profit de demandes concurrentes si un contexte d'activité n'a pas été établi.

## B.4 Activité: Évaluation des risques à haut niveau

La Figure B.3 illustre les étapes impliquées dans l'activité "Évaluation des risques à haut niveau".

.

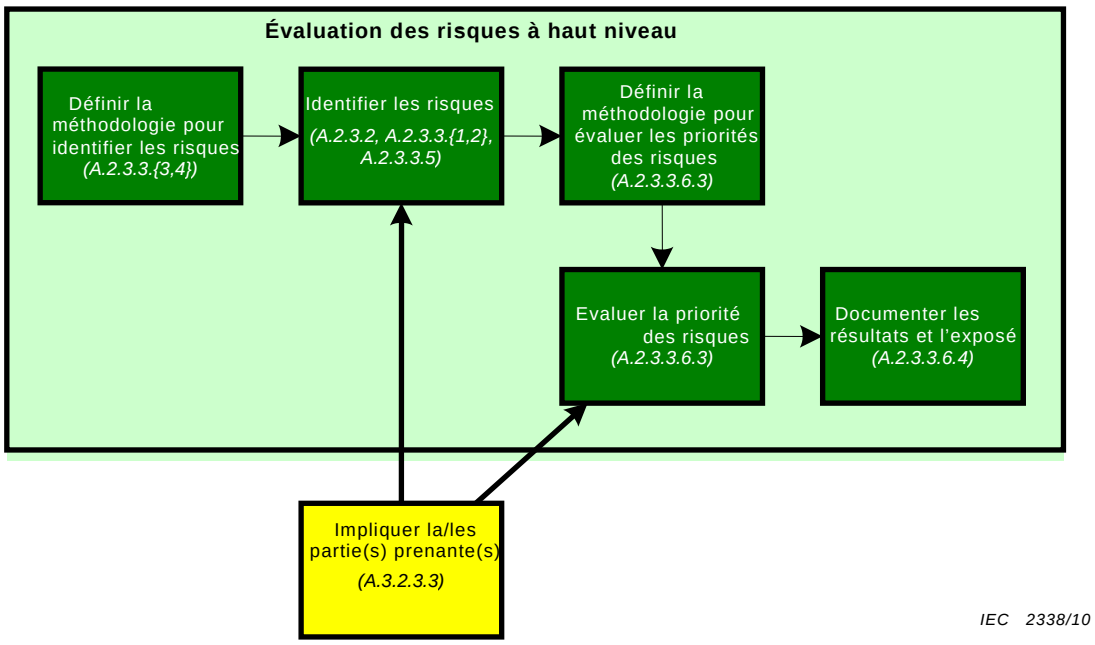



**Figure B.3 – Activités et déendances pour l'activité: Évaluation des risques à haut niveau**

L'activité "Évaluation des risques à haut niveau" met en œuvre la sélection de méthodologies pour identifier et hiérarchiser les risques et exécuter ensuite ces méthodologies. Il est important de définir ces méthodologies en amont afin qu'elles structurent le reste de l'évaluation des risques. La Figure B.3 montre qu'il est important d'impliquer les parties prenantes, identifiées au cours de l'activité Initiation du programme CSMS, dans le processus d'identification et d'évaluation de la priorité des risques. L'étape finale de documentation des résultats et de l'exposé est importante parce que cet enregistrement sera très précieux lorsque l'évaluation des risques devra être confirmée ou mise à jour à l'avenir.

## B.5 Activité: Évaluation détaillée des risques

Comme décrit à la Figure B.4, l'activité "Évaluation détaillée des risques" décrit de manière plus détaillée l'évaluation des risques, en effectuant dans un premier temps un inventaire des systèmes, réseaux et dispositifs spécifiques de l'IACS. Les contraintes de ressources ou de temps peuvent ne pas permettre un examen détaillé de l'ensemble de ces actifs. Dans ce cas, les menaces, conséquences et types de vulnérabilités identifiés dans l'évaluation des risques à haut niveau sont utilisés pour faciliter l'identification des priorités pour les systèmes, réseaux et dispositifs particuliers sur lesquels il convient de se concentrer. D'autres facteurs tels que l'assistance locale ou l'historique des problèmes contribuera également à déterminer les objectifs centraux de l'évaluation détaillée des risques. L'identification des vulnérabilités détaillées est guidée par les types de vulnérabilité de l'évaluation des risques à haut niveau, mais n'est pas limitée à ces types. Par conséquent, une évaluation détaillée de vulnérabilité peut révéler non seulement de nouveaux types de vulnérabilités mais également de nouvelles menaces potentielles et conséquences associées qui n'ont pas été identifiées au cours de l'évaluation des risques à haut niveau, en d'autres termes, de nouveaux risques. Dans ce cas, il convient de faire une évaluation à haut niveau afin de les inclure. Toutes les vulnérabilités observées sont associées à un risque spécifique (menace, vraisemblance et conséquence) et hiérarchisées d'une manière cohérente avec la méthode utilisée au cours de l'évaluation des risques à haut niveau.

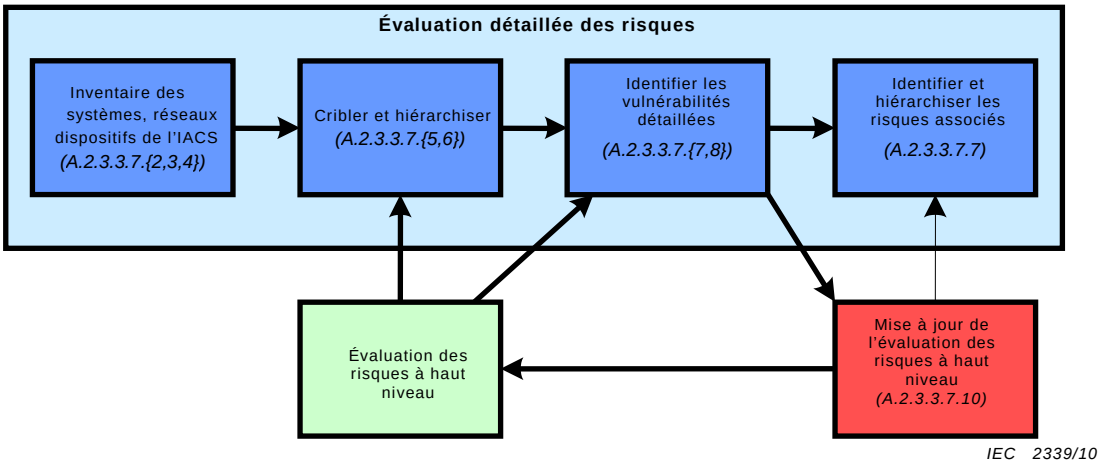



**Figure B.4 – Activités et dépendances pour l'activité: Évaluation détaillée des risques**

## B.6 Activité: Établir la politique, l'organisation et la sensibilisation à la sécurité

Les politiques appropriées pour l'organisation sont une interprétation opérationnelle de la tolérance des risques de l'organisation. Une organisation qui crée une politique avant de comprendre ses risques ou tolérance des risques peut consacrer des efforts inutiles et appliquer une politique inappropriée ou de manière similaire constater que ses politiques ne permettent pas la réduction de niveau de risque requise. La Figure B.5 illustre les étapes impliquées dans l'activité "Établir la politique, l'organisation et la sensibilisation à la sécurité".

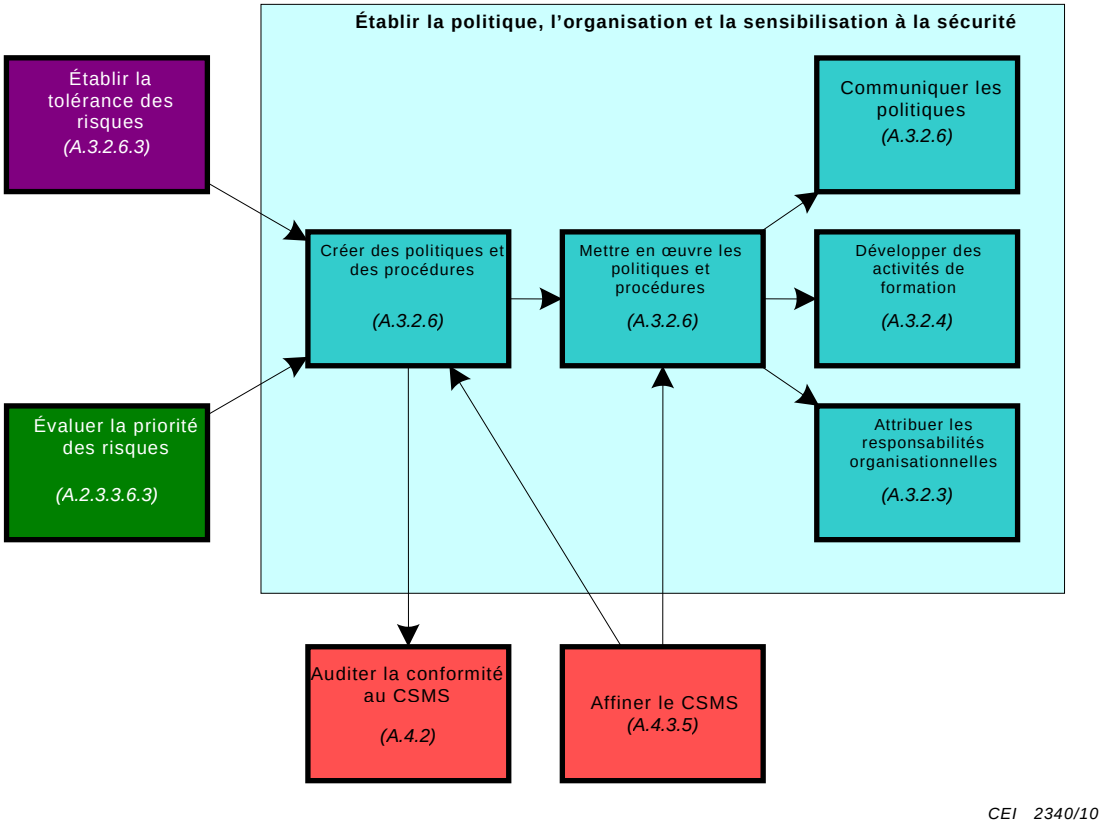



**Figure B.5 – Activités et dépendances pour l'activité: Établir la politique, l'organisation et la sensibilisation à la sécurité**

La mise en œuvre de politiques implique la communication de ces politiques à l'organisation, la formation du personnel de l'organisation et l'attribution de responsabilités pour l'adhésion à la politique. Les politiques et procédures peuvent affecter une activité quelconque du CSMS. Par exemple, des politiques peuvent concerner les contre-mesures communes à utiliser, nécessitant des processus spécifiques de développement et de maintenance de système ou déterminer quand un risque doit être réévalué. Par conséquent, la Figure B.5 ne vise pas à décrire l'ensemble des impacts potentiels des politiques et procédures sur le CSMS.

La Figure B.6 décompose plus avant les deux activités "Développement d'activités de formation" et "Attribution des responsabilités organisationnelles". Elle présente un grand nombre des différentes activités de formation qui constituent un programme de formation, les responsabilités organisationnelles associées à ces activités de formation, et les parties du programme CSMS relatives aux activités associées. Cette figure ne présente pas l'ensemble des responsabilités organisationnelles ou les sujets de formation pouvant être liés au CSMS, mais tente de présenter les principaux points qu'il convient de prendre en compte.

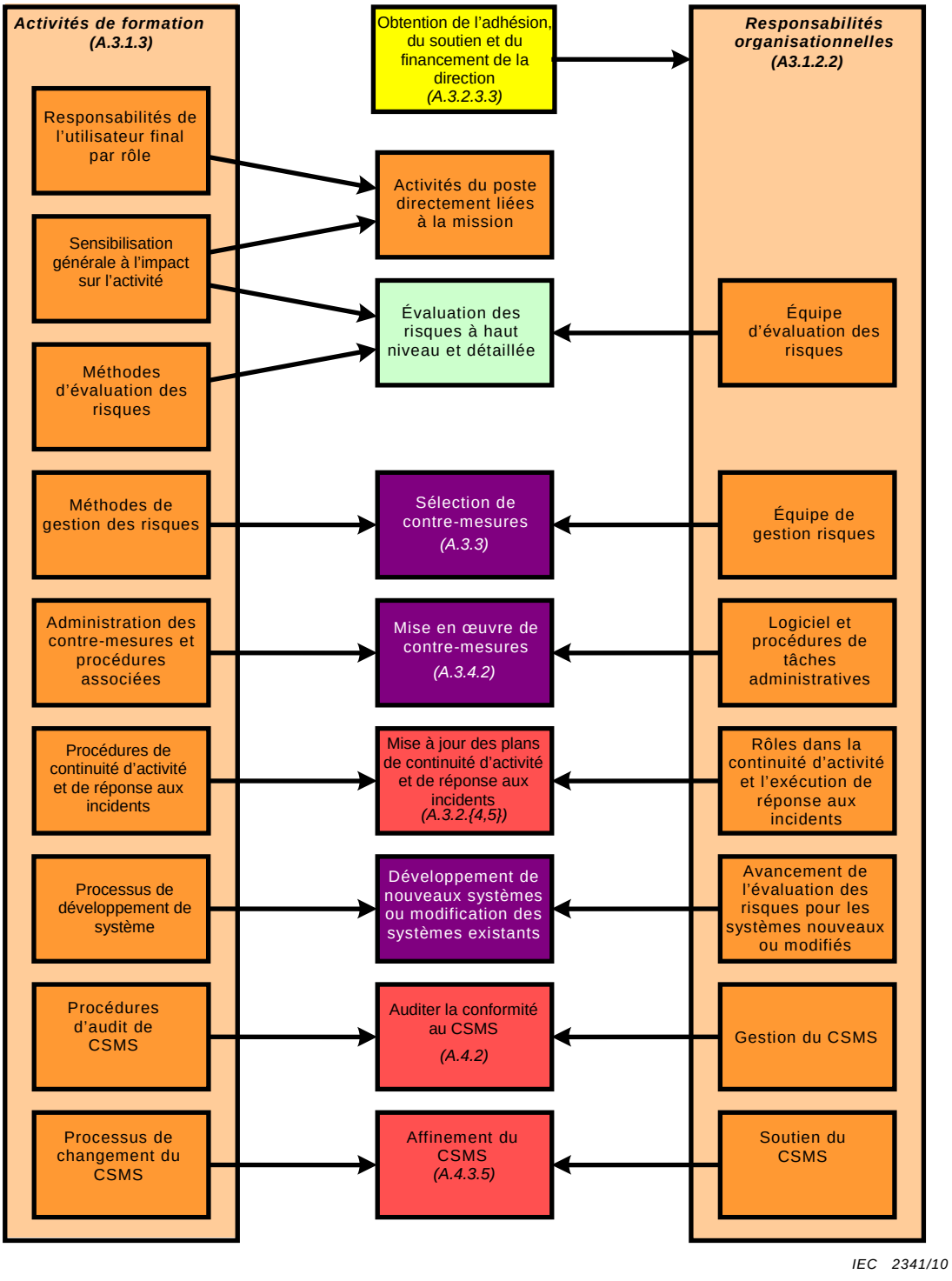



**Figure B.6 – Formation et attribution de responsabilités organisationnelles**

## B.7 Activité: Sélection et mise en œuvre de contre-mesures

La Figure B.7 illustre les étapes impliquées dans l'activité "Sélection et mise en œuvre de contre-mesures".

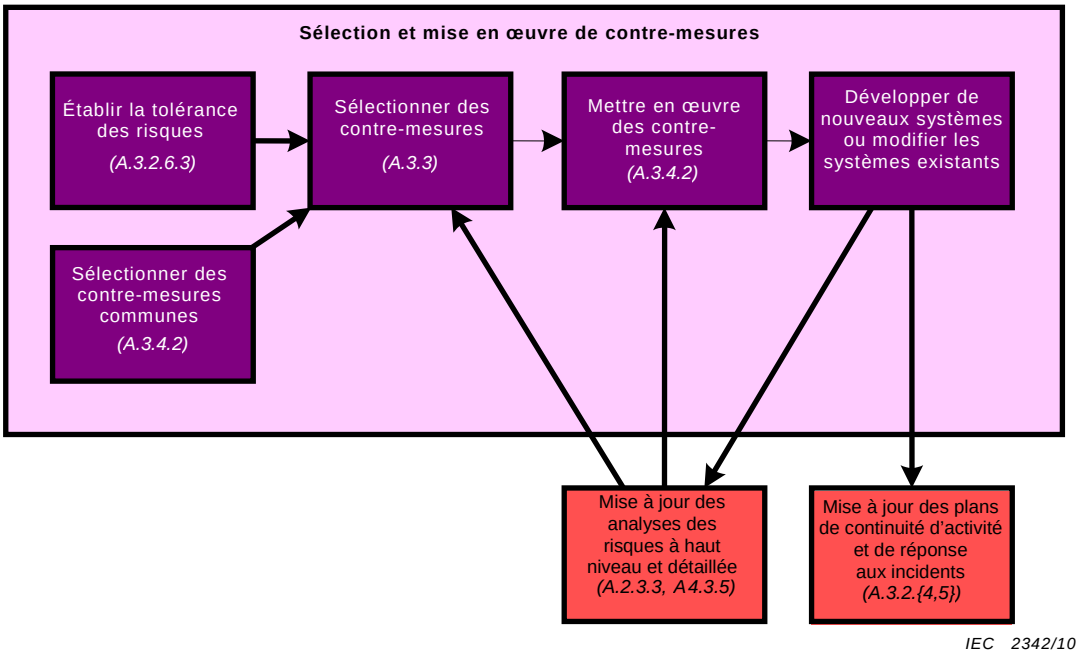



**Figure B.7 – Activités et dépendances pour l'activité: Sélection et mise en œuvre de contre-mesures**

La sélection de contre-mesures est le processus technique de gestion des risques. La tolérance des risques de l'organisation, les contre-mesures communes présélectionnées et les résultats de l'évaluation des risques à haut niveau et détaillée des risques, régissent l'approche de gestion des risques pour sélectionner des contre-mesures. Si l'organisation met en œuvre un nouveau système ou modifie un système existant, cela entraîne une mise à jour des évaluations des risques à haut niveau et détaillée pour le scénario où ce nouveau système est mis en œuvre. La sélection de contre-mesures associées au système nouveau ou modifié est ensuite effectuée sur la base de ces informations de risque mises à jour. Le développement ou la modification de systèmes requiert une mise à jour des plans de continuité d'activité et de réponse aux incidents.

## B.8 Activité: Maintenance du CSMS

Comme décrit à la Figure B.8, l'activité "Maintenance du CSMS" requiert un examen et un affinement périodique du CSMS sur la base des résultats d'examen. Les entrées majeures de cet examen sont les résultats des mesures d'efficacité et des audits de conformité de la surveillance interne du CSMS lui-même. Les autres entrées de cet examen sont les informations externes sur les contre-mesures disponibles, l'évolution des pratiques industrielles et les lois ou les réglementations nouvelles ou modifiées.

Un examen du CSMS identifie les faiblesses et propose des améliorations, qui produisent à leur tour des affinements du CSMS. Certains de ces affinements peuvent prendre la forme de nouvelles contre-mesures ou d'améliorations des contre-mesures mises en œuvre. D'autres affinements peuvent modifier les politiques et les procédures ou améliorer leur mise en œuvre. L'examen de résultats de conformité médiocres peut indiquer le besoin d'améliorations de la formation ou l'attribution de responsabilités organisationnelles.

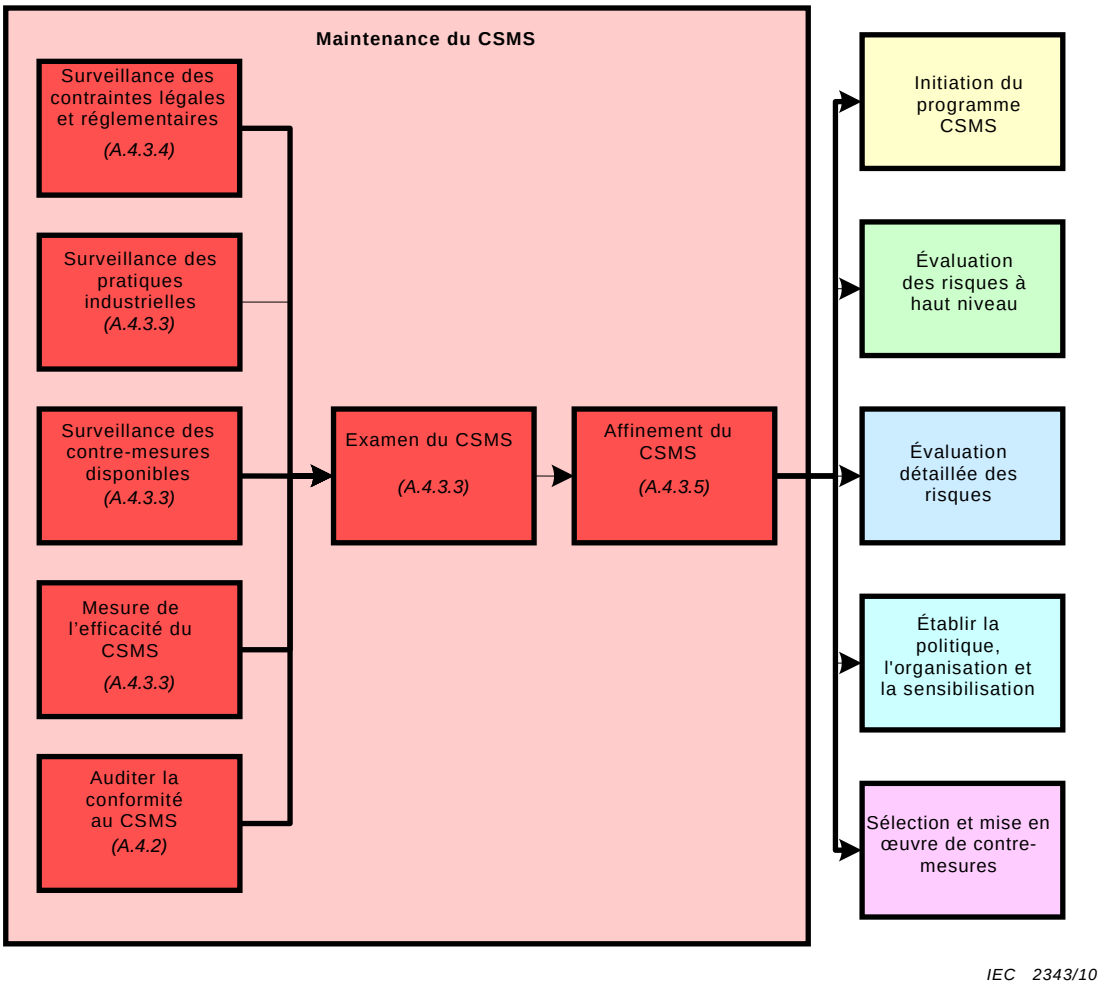



**Figure B.8 – Activités et dépendances pour l'activité: Maintenance du CSMS**

# Annexe C
(informative)

# Mise en correspondance avec les exigences de l'ISO/CEI 27001

## C.1 Vue d'ensemble

Les exigences contenues dans ce document sont très similaires aux exigences contenues dans l'ISO/CEI 27001 [24]. La présente norme, IEC 62443-2-1, a été développée en référence à l'ISO/CEI 27001 et de nombreuses références croisées sont faites dans l'ensemble du document. Cependant, la présente norme n'utilise pas la même organisation pour décrire ses exigences. Cette organisation différente est délibérée, car elle résulte d'un changement effectué pendant le développement de la norme en réponse aux commentaires des examinateurs et utilisateurs finaux de l'IACS, afin de faciliter la lisibilité en combinant des exigences similaires dans des paragraphes plus importants et en introduisant un grand nombre d'instructions dans l'Annexe A. Étant donné que de nombreux membres du personnel ayant des connaissances dans le domaine de la sécurité des informations sont déjà familiarisées avec l'ISO/CEI 27001, cette annexe a été incluse pour aider les lecteurs à comprendre les similarités entre les exigences des deux normes.

NOTE Suite aux commentaires du comité national CEI sur la version de projet de comité pour vote (CDV) de la présente norme, le corps normatif de l'édition suivante de la présente norme reflètera mieux l'organisation de l'ISO/CEI 27001, une grande partie des instructions aux utilisateurs d'IACS précédemment demandées étant reléguées dans les annexes informatives. Le travail sur la prochaine édition de la présente norme commencera après l'adoption de cette édition.

Cette annexe contient deux tableaux de mises en correspondance d'exigences. Le premier tableau contient les exigences de la présente norme et indique les références associées dans la norme ISO/CEI 27001. Le second tableau contient les exigences dans l'ISO/CEI 27001 et indique les références associées de la présente norme. La mise en correspondance des exigences est effectuée au niveau des paragraphes et ne représente pas une analyse exhaustive de l'ensemble des exigences détaillées. Une analyse plus détaillée des exigences pourra être effectuée dans une révision future de la présente norme.

## C.2 Mise en correspondance de la présente norme avec l'ISO/CEI 27001:2005

Le Tableau C.1 représente une mise en correspondance des exigences de cette norme au niveau des paragraphes avec des parties de l'ISO/CEI 27001:2005.

NOTE Une révision de l'ISO/CEI 27001 a été rédigée, mais n'a pas été publiée lors de la rédaction de la présente norme. Il n'a pas été entrepris de conduire une révision de la mise en correspondance des exigences de la présente norme avec la nouvelle version de l'ISO/CEI 27001.

**Tableau C.1 – Mise en correspondance des exigences dans la présente norme avec les références de l'ISO/CEI 27001**

| Exigence de la CEI 62443-2-1 | Références associées de l'ISO/CEI 27001 |
|---|---|
| 4.2.2 Contexte d'activité | 4.2.1e) Analyser et évaluer les risques<br>5.2.1 Mise à disposition des ressources |
| 4.2.3 Identification, classification et évaluation des risques | 4.2.1c) Approche d'évaluation des risques<br>4.2.1d) Identifier les risques<br>4.2.1e) Analyser et évaluer les risques<br>4.3.1 Exigences générales relatives à la documentation<br>A.6.2 Tiers<br>A.7.1 Responsabilités relatives aux actifs |
| 4.3.2.2 Domaine d'application du CSMS | 4.2.1a) Domaine d'application et limites du SMSI<br>4.3.1 Exigences générales relatives à la documentation |
| 4.3.2.3 Actions d'organisation pour la sécurité | 4.2.1b) Politique pour le SMSI<br>4.2.1i) Obtention de l'autorisation de la direction pour mettre en œuvre et exploiter le SMSI<br>4.2.2a) Elaborer un plan de traitement du risque<br>4.2.2b) Mettre en œuvre le plan de traitement du risque<br>4.2.2g) Gestion des ressources pour le SMSI<br>5.1 Adhésion de la direction<br>5.2.1 Mise à disposition des ressources<br>A.6.1 Organisation interne |
| 4.3.2.4 Formation du personnel et sensibilisation à la sécurité | 4.2.2e) Mise en œuvre de programmes de formation et de sensibilisation<br>5.2.2 Formation, sensibilisation et compétences<br>A.8.2 Sécurité des ressources humaines – en cours d'emploi |
| 4.3.2.5 Plan de continuité d'activité | 4.3.2 Contrôle des documents<br>4.3.3 Contrôle des enregistrements<br>A.9.1 Zones sécurisées<br>A.9.2 Sécurité des équipements<br>A.14.1 Aspects de sécurité des informations de la gestion de continuité d'activité |
| 4.3.2.6 Politiques et procédures de sécurité | 4.2.1b) Politique SMSI<br>4.2.1h) Obtention de l'approbation par la direction des risques résiduels proposés<br>4.2.1i) Obtention de l'autorisation de la direction à mettre en œuvre et mettre en service le SMSI<br>4.2.2d) Définition de la méthode de mesure de l'efficacité des contrôles sélectionnés<br>4.3.1 Exigences générales relatives aux documents<br>4.3.2 Contrôle des documents<br>7.1 Examen par la direction du SMSI |
| 4.3.3.2 Sécurité du personnel | A.6.1 Organisation interne<br>A.6.2 Parties externes<br>A.8.1 Sécurité des ressources humaines – avant l'embauche<br>A.8.2 Sécurité des ressources humaines – en cours d'emploi<br>A.8.3 Sécurité des ressources humaines – Fin de contrat ou changement de poste<br>A.10.1 Procédures opératoires et responsabilités |

**Tableau C.1** *(suite)*

| Exigence de la CEI 62443-2-1 | Références associées de l'ISO/CEI 27001 |
|---|---|
| 4.3.3.3 Sécurité physique et environnementale | A.9.1 Zones sécurisées<br>A.9.2 Sécurité des équipements<br>A.10.7 Manipulation des supports de média |
| 4.3.3.4 Segmentation de réseau | A.10.1 Procédures opératoires et responsabilités<br>A.10.3 Planification et acceptation du système<br>A.10.6 Gestion de la sécurité réseau<br>A.11.4 Contrôle d'accès au réseau |
| 4.3.3.5 Contrôle d'accès: Administration des comptes | A.11.1 Exigence relative à l'activité pour le contrôle d'accès<br>A.11.2 Gestion des accès utilisateur |
| 4.3.3.6 Contrôle d'accès: Authentification | A.11.3 Responsabilités des utilisateurs<br>A.11.4 Contrôle d'accès réseau<br>A.11.5 Contrôle d'accès au système d'exploitation |
| 4.3.3.7 Contrôle d'accès: Autorisation | A.11.6 Contrôle d'accès aux applications et à l'information<br>A.11.7 Informatique mobile et télétravail |
| 4.3.4.2 Gestion et mise en œuvre du contrôle des risques | 4.2.1d) Identifier les risques<br>4.2.1e) Analyser et évaluer les risques<br>4.2.1f) Identification et évaluation des options pour le traitement des risques<br>4.2.1g) Sélection d'objectifs de contrôle et contrôles pour le traitement des risques<br>4.2.1h) Obtention de l'approbation par la direction des risques résiduels proposés<br>4.2.1j) Préparation d'un énoncé d'applicabilité<br>4.2.2b) Mise en œuvre du plan de traitement des risques<br>4.2.2c) Mise en œuvre des contrôles<br>4.2.2d) Définition de la méthode de mesure de l'efficacité des contrôles sélectionnés<br>4.2.2h) Mise en œuvre de procédures et de contrôles pour détecter et répondre aux événements de sécurité<br>5.2.1 Mise à disposition des ressources |

**Tableau C.1** *(suite)*

| Exigence de la CEI 62443-2-1 | Références associées de l'ISO/CEI 27001 |
|---|---|
| 4.3.4.3 Développement et maintenance de système | A.10.1 Procédures opératoires et responsabilités<br>A.10.2 Gestion de la fourniture de service par des tiers<br>A.10.3 Planification et acceptation du système<br>A.10.4 Protection contre les codes malveillants et mobiles<br>A.10.5 Sauvegarde<br>A.10.6 Gestion de la sécurité réseau<br>A.10.8 Échange d'informations<br>A.10.9 Services de commerce électronique<br>A.10.10 Surveillance<br>A.12.1 Exigences de sécurité des systèmes d'information<br>A.12.2 Traitement correct dans des applications<br>A.12.3 Contrôles cryptographiques<br>A.12.4 Sécurité des fichiers système<br>A.12.5 Sécurité dans les processus de développement et d'assistance<br>A.12.6 Gestion de la vulnérabilité technique |
| 4.3.4.4 Gestion des informations et des documents | 4.3.1 Exigences générales relatives aux documents<br>4.3.2 Contrôle des documents<br>4.3.3 Contrôle des enregistrements<br>A.10.7 Manipulation des supports de média |
| 4.3.4.5 Planification et réponse aux incidents. | 4.2.2h) Mise en œuvre de procédures et de contrôles pour détecter et répondre aux événements de sécurité<br>4.3.2 Contrôle des documents<br>A.13.1 Rapport d'événements et de faiblesses de sécurité des informations<br>A.13.2 Gestion des incidents et améliorations de sécurité des informations |
| 4.4.2 Conformité | 4.2.2d) Définition de la méthode de mesure de l'efficacité des contrôles sélectionnés<br>4.2.3a) Exécution des procédures de surveillance et d'examen et autres contrôles<br>4.2.3c) Mesure de l'efficacité des contrôles<br>4.2.3e) Conduite d'audits internes du SMSI à des intervalles planifiés<br>6 Audits internes du SMSI<br>A.10.10 Surveillance<br>A.15.1 Conformité aux exigences légales<br>A.15.2 Conformité aux politiques et normes de sécurité, et conformité technique<br>A.15.3 Considérations relatives aux audits des systèmes d'information |

**Tableau C.1** *(suite)*

| Exigence de la CEI 62443-2-1 | Références associées de l'ISO/CEI 27001 |
|---|---|
| 4.4.3 Examen, amélioration et maintenance du CSMS | 4.2.2f) Gestion du fonctionnement du SMSI<br>4.2.3a) Exécution des procédures de surveillance et d'examen et autres contrôles<br>4.2.3b) Conduite de contrôles périodiques de l'efficacité du SMSI<br>4.2.3c) Mesure de l'efficacité des contrôles<br>4.2.3d) Examen des évaluations des risques, des risques résiduels et des niveaux de risque acceptables à intervalles planifiés<br>4.2.3f) Examen du SMSI sur une base périodique pour déterminer si le domaine d'application reste adéquat et les améliorations du SMSI sont identifiées<br>4.2.3g) Mise à jour des plans de sécurité à partir des activités de surveillance et d'examen<br>4.2.3h) Enregistrement des actions et événements pouvant avoir un impact sur l'efficacité ou les performances du SMSI<br>4.2.4a) Mise en œuvre des améliorations identifiées du SMSI<br>4.2.4b) Application d'actions correctives et préventives appropriées<br>4.2.4c) Communication des actions et améliorations à toutes les parties concernées<br>4.2.4d) Assurance que les améliorations atteignent leurs objectifs prévus<br>5.1 Adhésion de la direction<br>6 Audits internes du SMSI<br>7.1 Examen par la direction du SMSI<br>7.2 Examen des supports pour examen par la direction<br>7.3 Examen du résultat d'un examen de la direction<br>8.1 Amélioration continue du SMSI<br>8.2 Action corrective<br>8.3 Action préventive<br>A.13.2 Gestion des incidents liés à la sécurité de l'information et des améliorations |

## C.3 Mise en correspondance de l'ISO/CEI 27001:2005 avec la présente norme

Le Tableau C.2 contient la mise en correspondance inverse de celle du Tableau C.1.

**Tableau C.2 – Mise en correspondance des exigences de l'ISO/CEI 27001 avec la présente norme**

| Exigence de l'ISO/CEI 27001 | Références associées de la CEI 62443-2-1 |
|---|---|
| 4.2.1a) Domaine et limites d'application du SMSI | 4.3.2.2 Domaine d'application du CSMS |
| 4.2.1b) Politique SMSI | 4.3.2.3 Actions d'organisation pour la sécurité<br>4.3.2.6 Politiques et procédures de sécurité |
| 4.2.1c) Approche d'évaluation des risques | 4.2.3 Identification, classification et évaluation des risques |
| 4.2.1d) Identification des risques | 4.2.3 Identification, classification et évaluation des risques<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.1e) Analyse et évaluation des risques | 4.2.2 Contexte d'activité<br>4.2.3 Identification, classification et évaluation des risques<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.1f) Identification et évaluation des options pour le traitement des risques | 4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.1g) Sélection d'objectifs de contrôle et contrôles pour le traitement des risques | 4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.1h) Obtention de l'approbation par la direction des risques résiduels proposés | 4.3.2.6 Politiques et procédures de sécurité<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.1i) Obtention de l'autorisation de la direction à mettre en œuvre et mettre en service du SMSI | 4.3.2.3 Actions d'organisation pour la sécurité<br>4.3.2.6 Politiques et procédures de sécurité |
| 4.2.1j) Préparation d'un énoncé d'applicabilité | 4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.2a) Formulation d'un plan de traitement des risques | 4.3.2.3 Actions d'organisation pour la sécurité |
| 4.2.2b) Mise en œuvre du plan de traitement des risques | 4.3.2.3 Actions d'organisation pour la sécurité<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.2c) Mise en œuvre des contrôles | 4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 4.2.2d) Définition de la méthode de mesure de l'efficacité des contrôles sélectionnés | 4.3.2.6 Politiques et procédures de sécurité<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques<br>4.4.2 Conformité |
| 4.2.2e) Mise en œuvre de programmes de formation et de sensibilisation | 4.3.2.4 Formation du personnel et sensibilisation à la sécurité |
| 4.2.2f) Gestion du fonctionnement du SMSI | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.2g) Gestion des ressources pour su SMSI | 4.3.2.3 Actions d'organisation pour la sécurité |
| 4.2.2h) Mise en œuvre de procédures et de contrôles pour détecter et répondre aux événements de sécurité | 4.3.4.2 Gestion et mise en œuvre du contrôle des risques<br>4.3.4.5 Planification et réponse aux incidents. |
| 4.2.3a) Exécution des procédures de surveillance et d'examen et autres contrôles | 4.4.2 Conformité<br>4.4.3 Examen, amélioration et maintenance du CSMS |

**Tableau C.2** (*suite*)

| Exigence de l'ISO/CEI 27001 | Références associées de la CEI 62443-2-1 |
|---|---|
| 4.2.3b) Conduite de contrôles périodiques de l'efficacité du SMSI | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.3c) Mesure de l'efficacité des contrôles | 4.4.2 Conformité<br>4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.3d) Examen des évaluations des risques, des risques résiduels et des niveaux de risque acceptables à intervalles planifiés | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.3e) Conduite d'audits internes du SMSI à des intervalles planifiés | 4.4.2 Conformité |
| 4.2.3f) Examen du SMSI sur une base périodique pour déterminer si le domaine d'application reste adéquat et les améliorations du SMSI sont identifiées | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.3g) Mise à jour des plans de sécurité à partir des activités de surveillance et d'examen | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.3h) Enregistrement des actions et événements qui peuvent avoir un impact sur l'efficacité ou les performances du SMSI | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.4a) Mise en œuvre des améliorations identifiées du SMSI | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.4b) Application d'actions correctrices et préventives appropriées | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.4c) Communication des actions et améliorations à toutes les parties concernées | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.2.4d) Assurance que les améliorations atteignent leurs objectifs prévus | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 4.3.1 Exigences générales relatives aux documents | 4.2.3 Identification, classification et évaluation des risques<br>4.3.2.2 Domaine d'application du CSMS<br>4.3.2.6 Politiques et procédures de sécurité<br>4.3.4.4 Gestion des informations et des documents |
| 4.3.2 Contrôle des documents | 4.3.2.5 Plan de continuité d'activité<br>4.3.2.6 Politiques et procédures de sécurité<br>4.3.4.4 Gestion des informations et des documents<br>4.3.4.5 Planification et réponse aux incidents. |
| 4.3.3 Contrôle des enregistrements | 4.3.2.5 Plan de continuité d'activité<br>4.3.4.4 Gestion de l'information et des documents |
| 5.1 Adhésion de la direction | 4.3.2.3 Actions d'organisation pour la sécurité<br>4.4.2 Conformité<br>4.4.3 Examen, amélioration et maintenance du CSMS |

**Tableau C.2** (*suite*)

| Exigence de l'ISO/CEI 27001 | Références associées de la CEI 62443-2-1 |
|---|---|
| 5.2.1 Mise à disposition des ressources | 4.2.2 Contexte d'activité<br>4.3.2.3 Actions d'organisation pour la sécurité<br>4.3.4.2 Gestion et mise en œuvre du contrôle des risques |
| 5.2.2 Formation, sensibilisation et compétences | 4.3.2.4 Formation du personnel et sensibilisation à la sécurité |
| 6 Audits internes du SMSI | 4.4.2 Conformité<br>4.4.3 Examen, amélioration et maintenance du CSMS |
| 7.1 Examen par la direction du SMSI | 4.3.2.6 Politiques et procédures de sécurité<br>4.4.3 Examen, amélioration et maintenance du CSMS |
| 7.2 Examen des supports pour examen par la direction | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 7.3 Examen du résultat d'un examen de la direction | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 8.1 Amélioration continue du SMSI | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 8.2 Actions correctives | 4.4.3 Examen, amélioration et maintenance du CSMS |
| 8.3 Actions préventives | 4.4.3 Examen, amélioration et maintenance du CSMS |
| A.5.1 Politique de sécurité des informations | Aucun article spécifique; les politiques de sécurité des systèmes de commande interprètent et applique les politiques générales dans cet environnement. |
| A.6.1 Organisation interne | 4.3.2.3 Actions d'organisation pour la sécurité<br>4.3.3.2 Sécurité du personnel |
| A.6.2 Parties externes | 4.2.3 Identification, classification et évaluation des risques<br>4.3.3.2 Sécurité du personnel |
| A.7.1 Responsabilité relative aux actifs | 4.2.3 Identification, classification et évaluation des risques |
| A.7.2 Classification des informations | Aucun article spécifique; les politiques de sécurité des systèmes de commande interprètent et applique les politiques générales dans cet environnement. |
| A.8.2 Sécurité des ressources humaines – avant l'embauche | 4.3.3.2 Sécurité du personnel |
| A.8.2 Sécurité des ressources humaines – en cours d'emploi | 4.3.2.4 Formation du personnel et sensibilisation à la sécurité<br>4.3.3.2 Sécurité du personnel |
| A.8.3 Sécurité des ressources humaines – Fin de contrat ou changement de poste | 4.3.3.2 Sécurité du personnel |
| A.9.1 Zones sécurisées | 4.3.2.5 Plan de continuité d'activité<br>4.3.3.3 Sécurité physique et environnementale |
| A.9.2 Sécurité des équipements | 4.3.2.5 Plan de continuité d'activité<br>4.3.3.3 Sécurité physique et environnementale |

**Tableau C.2** (*suite*)

| Exigence de l'ISO/CEI 27001 | Références associées de la CEI 62443-2-1 |
|---|---|
| A.10.1 Procédures opératoires et responsabilités | 4.3.3.2 Sécurité du personnel<br>4.3.3.4 Segmentation de réseau<br>4.3.4.3 Développement et maintenance des systèmes<br>4.4.2 Conformité |
| A.10.2 Gestion de la fourniture de service par des tiers | 4.3.4.3 Développement et maintenance des systèmes |
| A.10.3 Planification et acceptation du système | 4.3.3.4 Segmentation de réseau<br>4.3.4.3 Développement et maintenance des systèmes |
| A.10.4 Protection contre les codes malveillants et mobiles | 4.3.4.3 Développement et maintenance des systèmes |
| A.10.5 Sauvegarde | 4.3.4.3 Développement et maintenance des systèmes |
| A.10.6 Gestion de la sécurité réseau | 4.3.3.4 Segmentation de réseau<br>4.3.4.3 Développement et maintenance des systèmes |
| A.10.7 Manipulation des supports de média | 4.3.3.3 Sécurité physique et environnementale<br>4.3.4.4 Gestion de l'information et des documents |
| A.10.8 Échange d'informations | 4.3.4.3 Développement et maintenance des systèmes |
| A.10.9 Services de commerce électronique | 4.3.4.3 Développement et maintenance des systèmes |
| A.10.10 Surveillance | 4.3.4.3 Développement et maintenance des systèmes<br>4.4.2 Elément: Conformité |
| A.11.1 Exigence relative à l'activité pour le contrôle d'accès | 4.3.3.5 Contrôle d'accès: Administration des comptes |
| A.11.2 Gestion des accès utilisateur | 4.3.3.5 Contrôle d'accès: Administration des comptes |
| A.11.3 Responsabilités des utilisateurs | 4.3.3.6 Contrôle d'accès: Authentification |
| A.11.4 Contrôle d'accès au réseau | 4.3.3.4 Segmentation des réseaux<br>4.3.3.6 Contrôle d'accès: Authentification |
| A.11.5 Contrôle d'accès au système d'exploitation | 4.3.3.6 Contrôle d'accès: Authentification |
| A.11.6 Contrôle d'accès aux applications et aux informations | 4.3.3.7 Contrôle d'accès: Autorisation |
| A.11.7 Informatique mobile et télétravail | 4.3.3.7 Contrôle d'accès: Autorisation |
| A.12.1 Exigences de sécurité des systèmes d'information | 4.3.4.3 Développement et maintenance des systèmes |
| A.12.2 Traitement correct dans des applications | 4.3.4.3 Développement et maintenance des systèmes |
| A.12.3 Contrôles cryptographiques | 4.3.4.3 Développement et maintenance des systèmes |
| A.12.4 Sécurité des fichiers système | 4.3.4.3 Développement et maintenance des systèmes |
| A.12.5 Sécurité dans les processus de développement et d'assistance | 4.3.4.3 Développement et maintenance des systèmes |

**Tableau C.2** (*suite*)

| Exigence de l'ISO/CEI 27001 | Références associées de la CEI 62443-2-1 |
|---|---|
| A.12.6 Gestion de la vulnérabilité technique | 4.3.4.3 Développement et maintenance des systèmes |
| A.13.1 Rapport d'événements et de faiblesses de sécurité des informations | 4.3.4.5 Planification et réponse aux incidents |
| A.13.2 Gestion des incidents et améliorations de sécurité des informations | 4.3.4.5 Planification et réponse aux incidents<br>4.4.3 Révision, amélioration et maintenance du CSMS |
| A.14.1 Aspects de sécurité des informations de la gestion de continuité d'activité | 4.3.2.5 Plan de continuité d'activité |
| A.15.1 Conformité aux exigences légales | 4.4.2 Conformité |
| A.15.2 Conformité aux politiques et normes de sécurité, et conformité technique | 4.4.2 Conformité |
| A.15.3 Considérations relatives aux audits des systèmes d'information | 4.4.2 Conformité |

# Bibliographie

NOTE Cette bibliographie comprend des références à des sources utilisées dans la création de la présente norme ainsi que des références à des sources qui peuvent aider le lecteur à développer une meilleure compréhension de la cyber-sécurité dans son ensemble et développer un système de gestion. Les références dans cette bibliographie ne sont pas toutes référencées dans l'ensemble du texte de la présente norme. Les références ont été divisées en différentes catégories suivant le type de source auquel elles correspondent.

## Références à d'autres parties, existantes et prévues, de la série CEI 62443:

NOTE Certaines de ces références sont des références normatives (voir Article 2), des documents publiés, en développement ou prévus. Elles sont toutes présentement énumérées afin de compléter les parties prévues de la série CEI 62443.

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

[2] IEC/TS 62443-1-2[4]– *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations*

[3] IEC/TS 62443-1-3– *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*

NOTE La présente norme est CEI 62443-2-1, *Réseaux de communication industrielle – Sécurité dans les réseaux et les systèmes – Partie 2 1: Établissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industriels*

[4] IEC/TS 62443-2-2[5]– *Industrial communication networks – Network and system security – Part 2-2: Operating an industrial automation and control system security program*

[5] IEC/TS 62443-2-3[4]– *Industrial communication networks – Network and system security – Part 2-3:*

[6] IEC/TS 62443-3-1 *Patch management in the IACS environment*, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

[7] IEC/TS 62443-3-2[4]– *Industrial communication networks – Network and system security – Part 3-2: Target security assurance levels for zones and conduits*

[8] IEC 62443-3-3[4]– *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security assurance levels*

[9] IEC/TS 62443-3-4[4]– *Industrial communication networks – Network and system security – Part 3-4: Product development requirements*

[10] IEC/TS 62443-4-1[4]– *Industrial communication networks – Network and system security – Part 4-1: Embedded devices*

[11] IEC/TS 62443-4-2[4]– *Industrial communication networks – Network and system security – Part 4-2: Host devices*

[12] IEC/TS 62443-4-3[4]– *Industrial communication networks – Network and system security – Part 4-3: Network devices*

---

4 En cours de développement.

5 Compagnon prévu de la présente norme internationale.

[13] IEC/TS 62443-4-4[4]– *Industrial communication networks – Network and system security – Part 4-4: Application, data and functions*

**Autres normes de référence:**

[14] IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

[15] IEC 61512-1, *Batch Control, Part 1: Models and terminology*

[16] IEC 62264-1, *Enterprise-Control System Integration, Part 1: Models and terminology*

[17] Directives ISO/CEI, Partie 2, *Règles de structure et de rédaction des normes internationales*

[18] ISO/CEI 10746-1, *Technologies de l'information — Traitement réparti ouvert — Modèle de référence*: *Présentation*

[19] ISO/IEC 10746-2, *Information technology – Open distributed processing – Reference model: Foundations*

[20] ISO/IEC 15408-1:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

[21] ISO/IEC 15408-2:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

[22] ISO/IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*

[23] ISO/IEC 17799, *Information technology – Security techniques – Code of practice for information security management*

[24] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

[25] 29 CFR 1910.119 – *U.S. Occupational Safety and Health Standards – Hazardous Materials – Process safety management of highly hazardous chemicals*

**Références spécifiques à une industrie ou un secteur:**

[26] Guidance for Addressing Cyber Security in the Chemical Sector, Version 3.0, Mai 2006, American Chemistry Council's Chemical Information Technology Center (ChemITC), disponible à <http://www.chemicalcybersecurity.com/>

[27] Report on Cyber Security Vulnerability Assessments Methodologies, Version 2.0, Novembre 2004, ChemITC, disponible à <http://www.chemicalcybersecurity.com/>

[28] Cyber Security Architecture Reference Model, Version 1.0, Août 2004, ChemITC, disponible à <http://www.chemicalcybersecurity.com/>

[29] Report on the Evaluation of Cybersecurity Self-assessment Tools and Méthodes, Novembre 2004, ChemITC, disponible à <http://www.chemicalcybersecurity.com/>

[30] U.S. Chemicals Sector Cyber Security Strategy, Septembre 2006, disponible à <http://www.chemicalcybersecurity.com/>

**Autres documents et ressources publiées:**

[31] Carlson, Tom, *Information Security Management: Understanding ISO 17799*, 2001, disponible à <http://www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf>

[32] Purdue Research Foundation, A Reference Model for Computer Integrated Manufacturing, 1989, ISBN 1-55617-225-7

[33] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, Juillet 2002

[34] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Mai 2004

[35] NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, Juillet 2003

[36] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, Janvier 2004

[37] NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, Mars 2006, Projet

[38] NIST Process Control Security Requirements Forum (PCSRF), Industrial Control System – System Protection Profile (ICS-SPP)

[39] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration (CMMI) for Software Engineering*, v1.1, Août 2002

**Sites Web:**

[40] NASA/Science Office of Standards and Technology (NOST), disponible à <http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html>

[41] Zachmann Enterprise Reference Model, disponible à <http://www.zifa.com/>

[42] Site Web Sarbanes – Oxley, disponible à <http://www.sarbanes-oxley.com/>

[43] Site Web Sans, disponible à <http://www.sans.org/>

[44] MIS Training Institute, disponible à <http://www.misti.com/>

[45] U.S. National Institute of Standards & Technology, disponible à <http://www.nist.gov/>

[46] Information Systems Technology Audit Programs, disponible à <http://www.auditnet.org/asapind.htm>

[47] NIST eScan Security Assessment, disponible à <https://www.mepcenters.nist.gov/escan/>

[48] American National Standards Institute, disponible à <http://www.ansi.org/>

[49] IDEAL Model, disponible à <http://www.sei.cmu.edu/ideal/ideal.html>

[50] Control Objectives for Information and Related Technology (COBIT), disponible à <http://www.isaca.org/>

[51] Corporate Governance Task Force “Information Security Governance- A call to action”, disponible à <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>

[52] Michigan State Cybersecurity Definitions, disponible à <http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html>

[53] The Free Internet Encyclopedia – Wikipedia, disponible à <http://www.wikipedia.org/>

[54] Bridgefield Group Glossary, disponible à <http://www.bridgefieldgroup.com/>

[55] Six Sigma Information, disponible à <http://www.onesixsigma.com/>

[56] Carnegie Mellon Software Engineering Institute, disponible à <http://www.sei.cmu.edu/>

[57] Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team (CERT), disponible à <http://www.cert.org/>

[58] SCADA and Control Systems Procurement Project, disponible à <http://www.msisac.org/scada/>

[59] Interoperability Clearinghouse, disponible à <http://www.ichnet.org/>

[60] New York State Financial Terminology, disponible à <http://www.budget.state.ny.us/citizen/financial/glossary_all.html>

[61] Search Windows Security, disponible à <http://www.searchwindowssecurity.com/>

[62] Chemical Sector Cyber Security Program, disponible à <http://www.chemicalcybersecurity.com/>

[63] TechEncyclopedia, disponible à <http://www.techweb.com/encyclopedia/>

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch