Annex A
(informative)

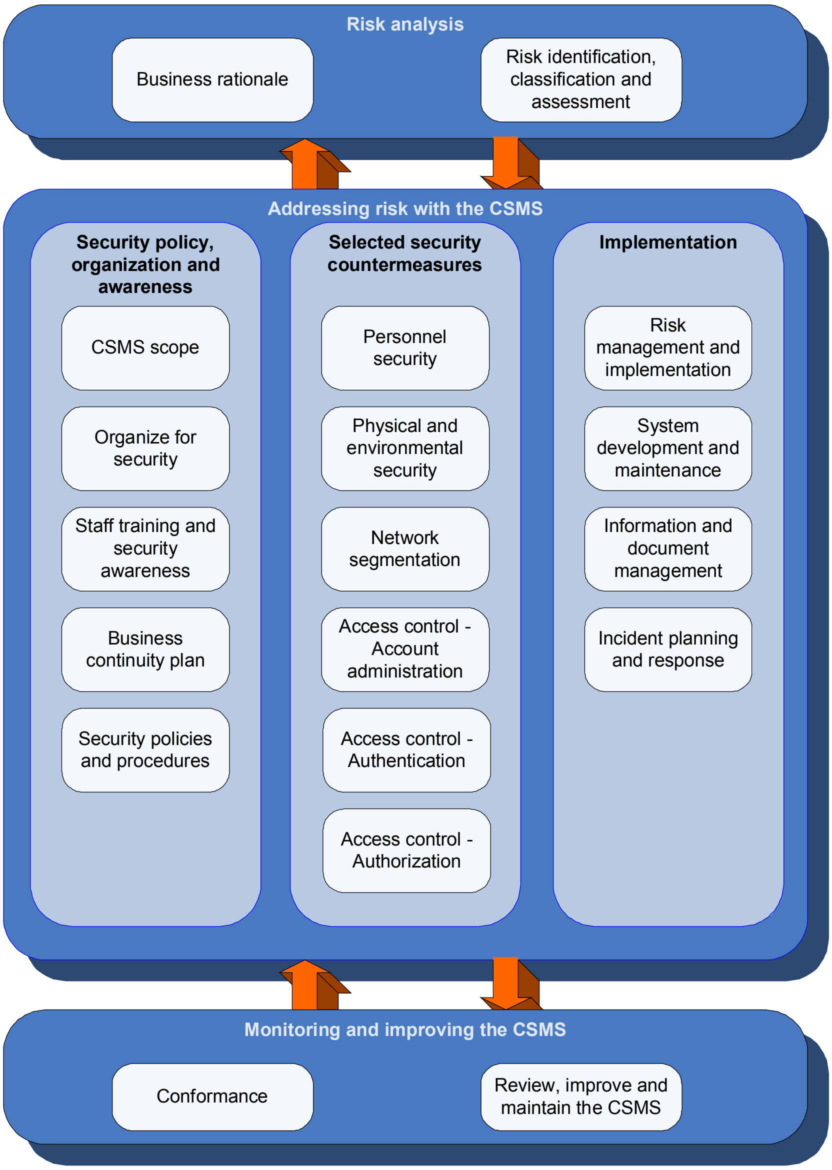
Guidance for developing the elements of a CSMS

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).


Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control - Account administration
Access control - Authentication
Access control - Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

IEC 2318/10

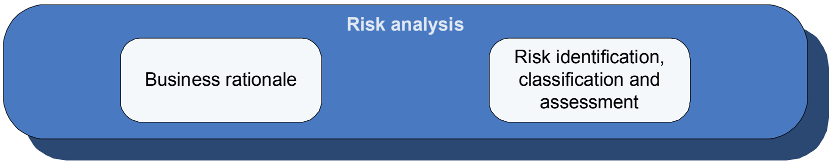
Figure A.1 – Graphical view of elements of a cyber security management system

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.

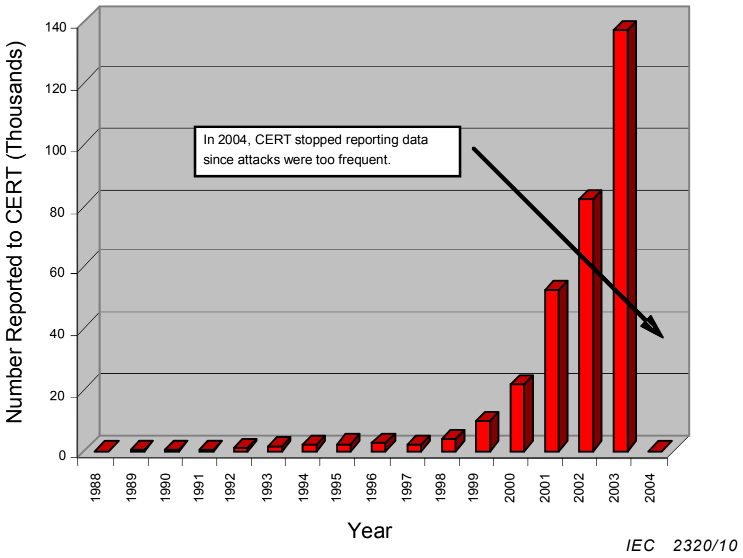


Figure A.3 – Reported attacks on computer systems through 2004 (source: CERT)

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 though corporate firewall defenses 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:

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

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.

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

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								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
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:

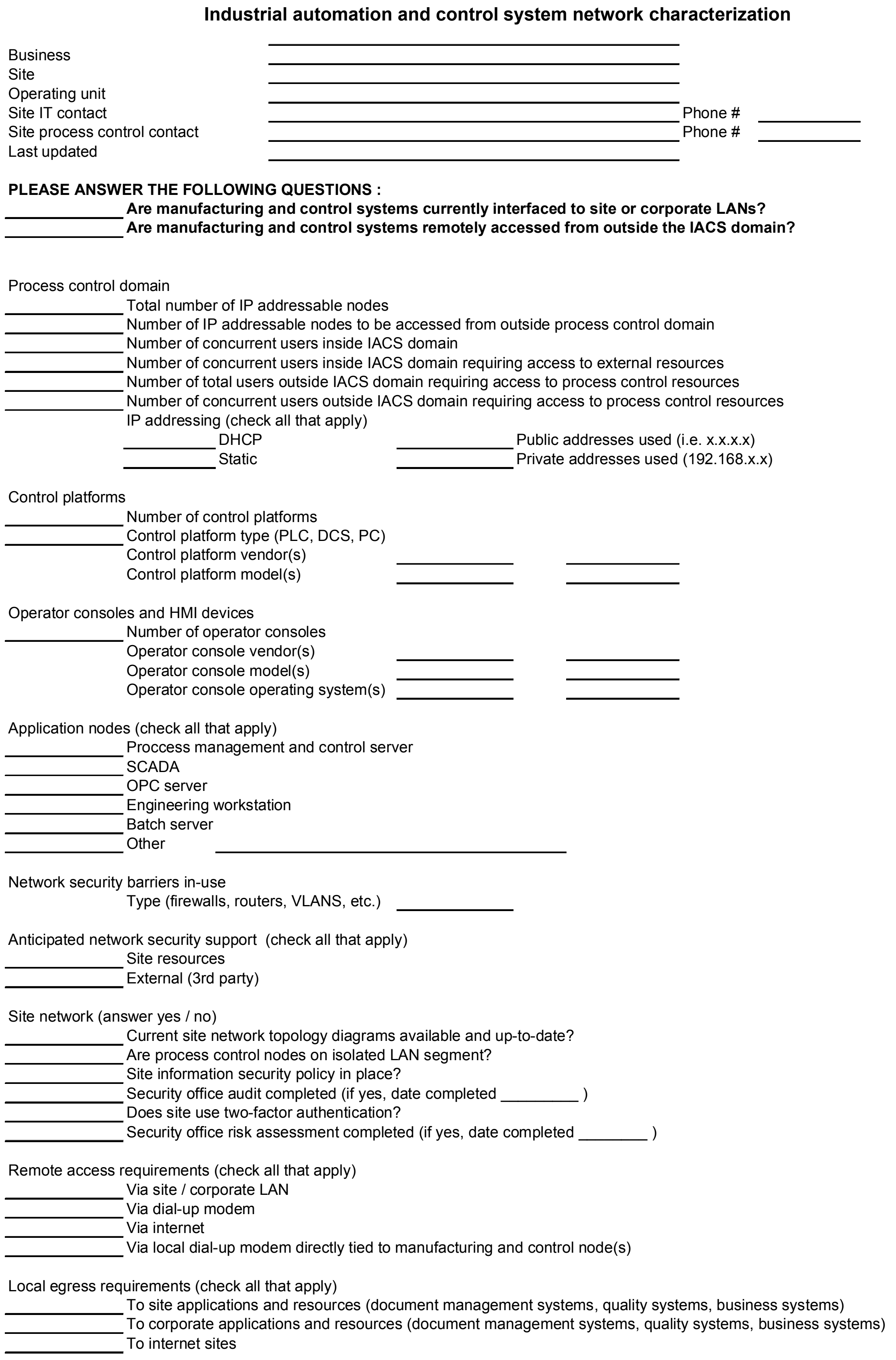
- Whether the field instrumentation and communication from the field transmitter to the controllers is analog-based or digital-based.
- Whether devices/systems are connected to each other and the types of networks used.
- Whether the devices are located within a secured area such as a building or fenced 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.

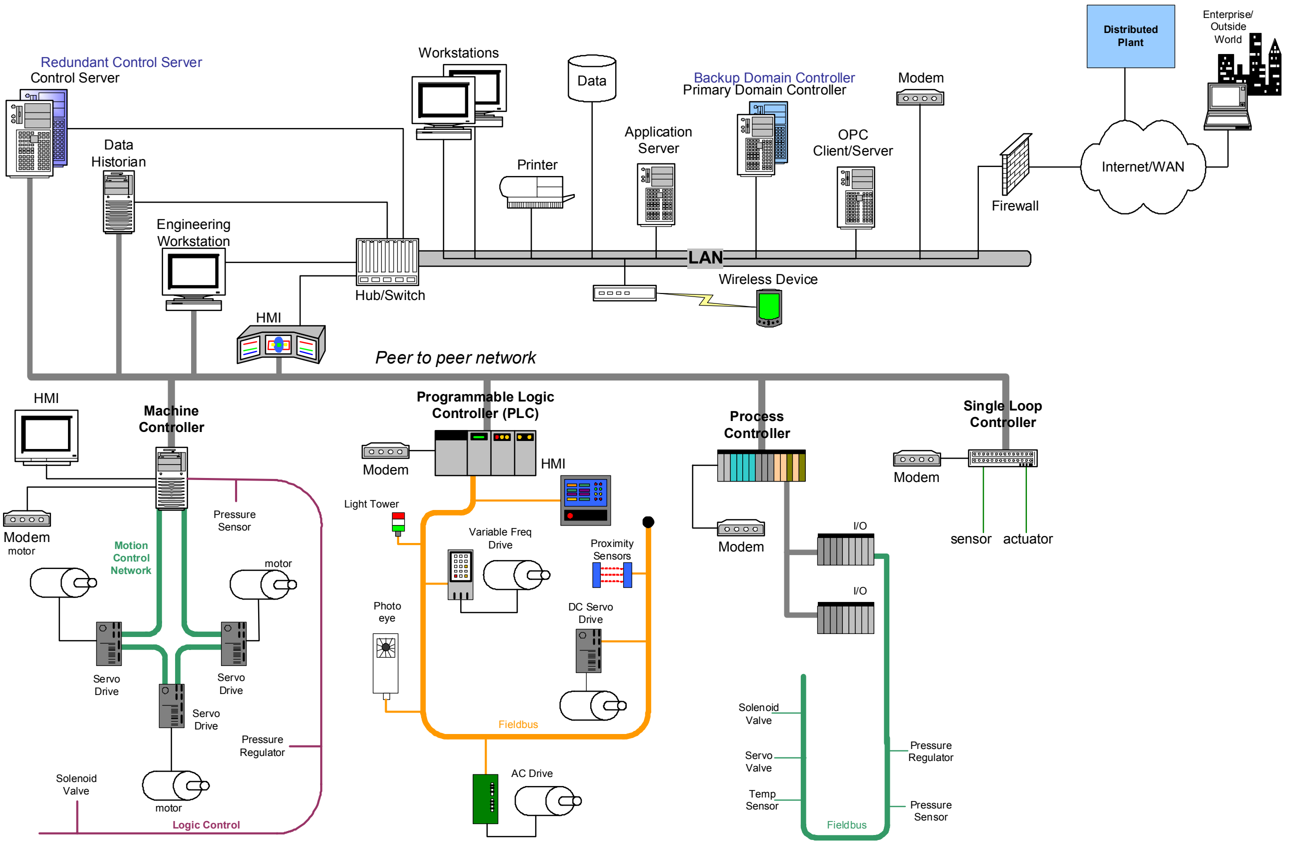
There are several enterprise-wide inventory tools commercially available that will work across networks to identify and document all hardware, systems and software resident on the network. Care shall be taken before using this type of application to identify IACS. Conduct an assessment of how these tools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

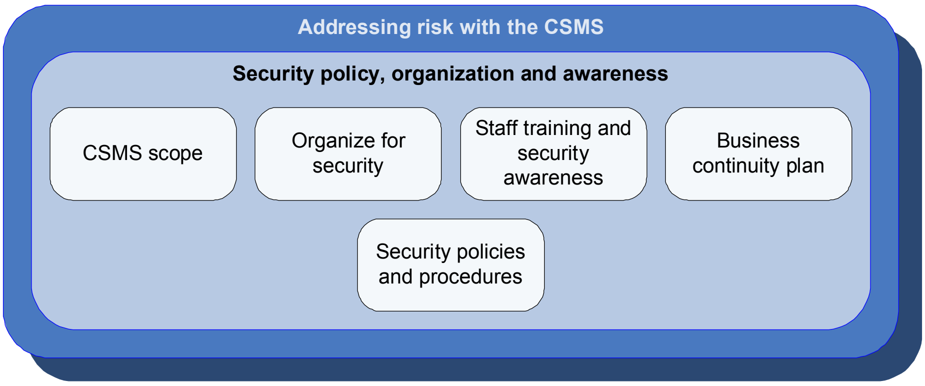
- Security policy, organization and awareness,
- Selected security countermeasures and
- Implementation.

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.


Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures

IEC 2323/10

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.3.2.3.3 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 fulfillment 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 manager 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

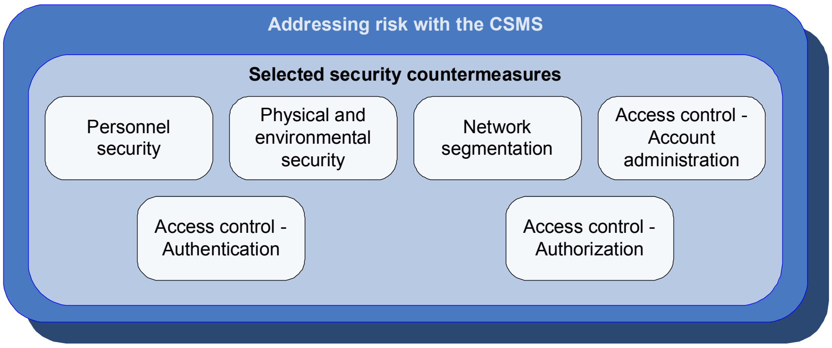
This element was based in part on material found in the following references, all of which are listed in the Bibliography: [23], [26], [30], [43].

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.


Addressing risk with the CSMS
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control - Account administration
Access control - Authentication
Access control - Authorization

IEC 2324/10

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.

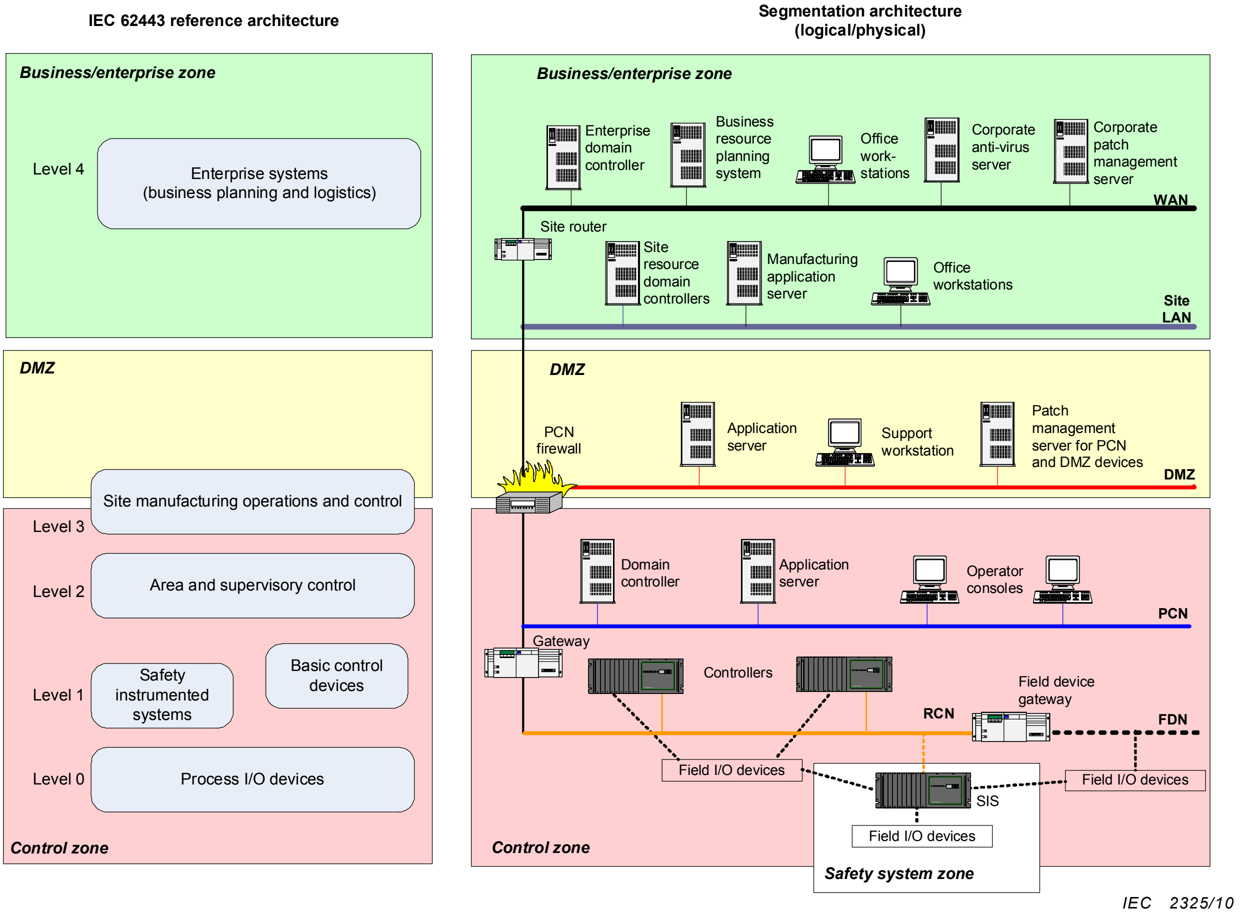

IEC 62443 reference architecture
Segmentation architecture (logical/physical)
Business/enterprise zone
Level 4
Enterprise systems (business planning and logistics)
DMZ
Site manufacturing operations and control
Level 3
Level 2
Area and supervisory control
Level 1
Safety instrumented systems
Basic control devices
Level 0
Process I/O devices
Control zone
Business/enterprise zone
Enterprise domain controller
Business resource planning system
Office work-stations
Corporate anti-virus server
Corporate patch management server
WAN
Site router
Site resource domain controllers
Manufacturing application server
Office workstations
Site LAN
DMZ
PCN firewall
Application server
Support workstation
Patch management server for PCN and DMZ devices
DMZ
Domain controller
Application server
Operator consoles
PCN
Gateway
Controllers
Field device gateway
RCN
FDN
Field I/O devices
SIS
Field I/O devices
Field I/O devices
Safety system zone
Control zone
IEC 2325/10

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.

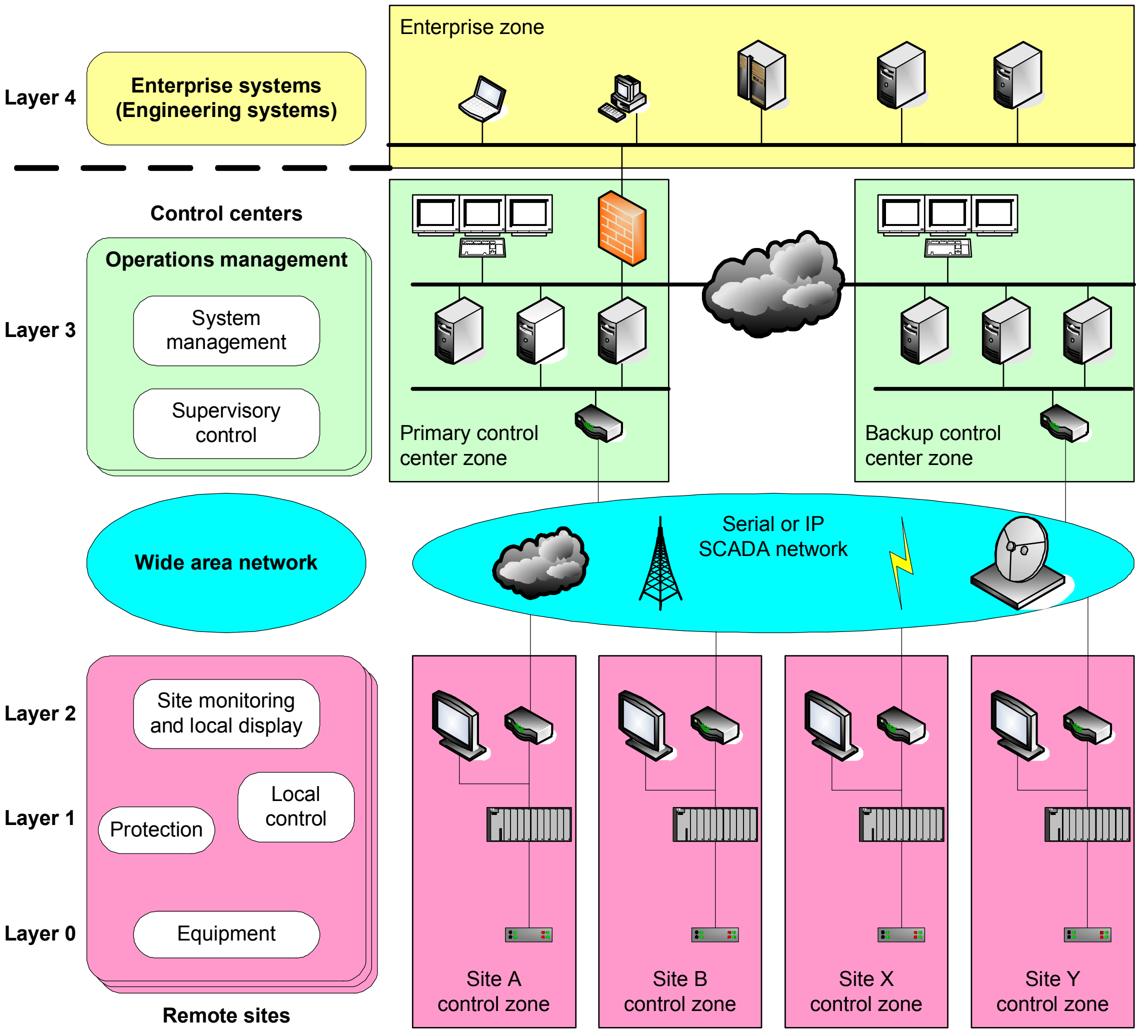
A.3.3.4.2.5 Isolated IACS

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.



IEC 2326/10

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.

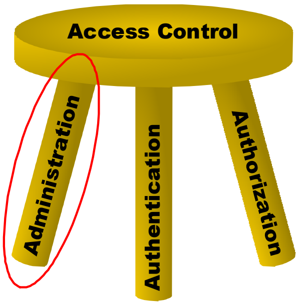
Within each of the three aspects of access control, rules should be established to confirm that a user's access to systems and data is controlled. The rules generally should be applied to roles or groups of users. They should have access to systems and data that are required to meet defined business 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

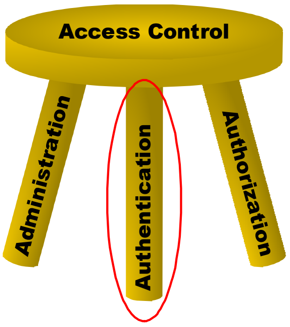
This element was based in part on material found in the following reference, which is listed in the Bibliography: [6].

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.



IEC 2327/10

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:

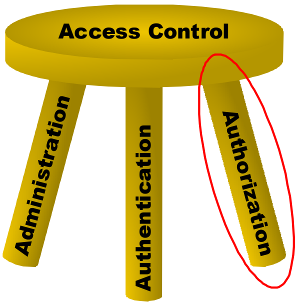
a) Authorizing users inside a locked facility that employs guards and badge-readers to access systems having a greater level of risk than a remote user would be allowed.

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.



IEC 2328/10

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

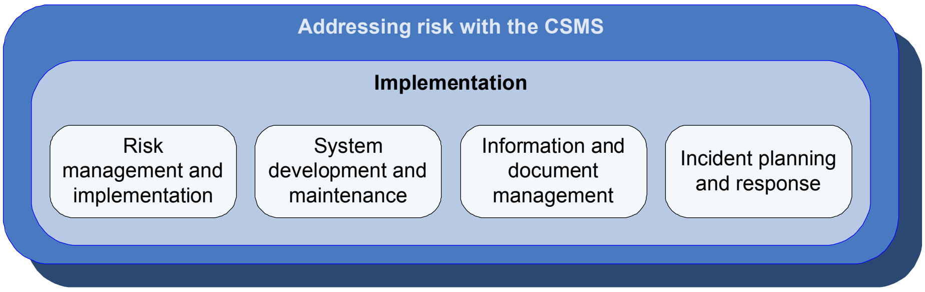
This element was based in part on material found in the following references, all of which are listed in the Bibliography: [6], [23], [27], [30], [43].

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.


Addressing risk with the CSMS
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response

IEC 2329/10

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.

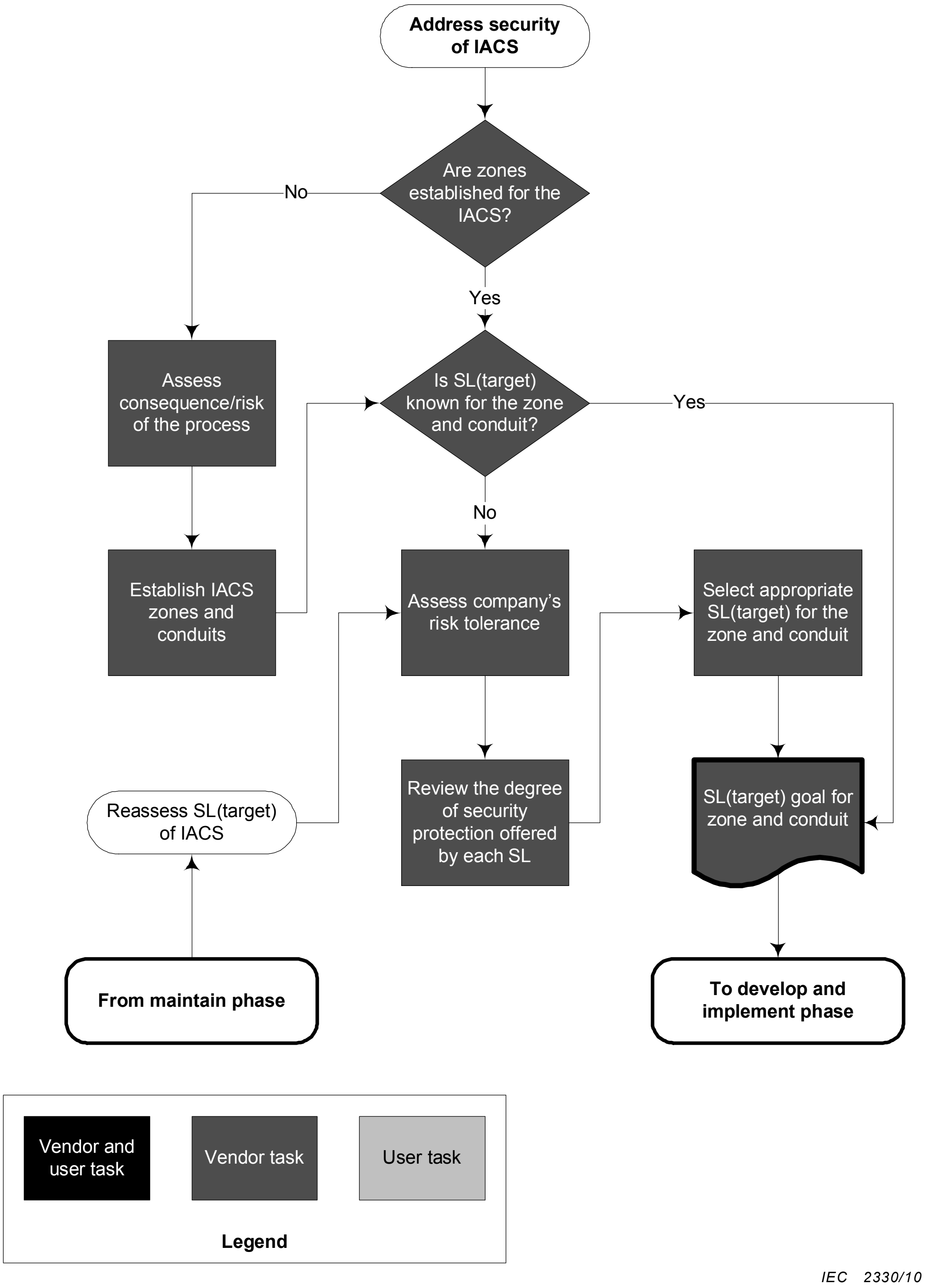

Address security of IACS
Are zones established for the IACS?
No
Yes
Assess consequence/risk of the process
Is SL(target) known for the zone and conduit?
Yes
No
Establish IACS zones and conduits
Assess company's risk tolerance
Select appropriate SL(target) for the zone and conduit
Reassess SL(target) of IACS
Review the degree of security protection offered by each SL
SL(target) goal for zone and conduit
From maintain phase
To develop and implement phase
Vendor and user task
Vendor task
User task
Legend
IEC 2330/10

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.

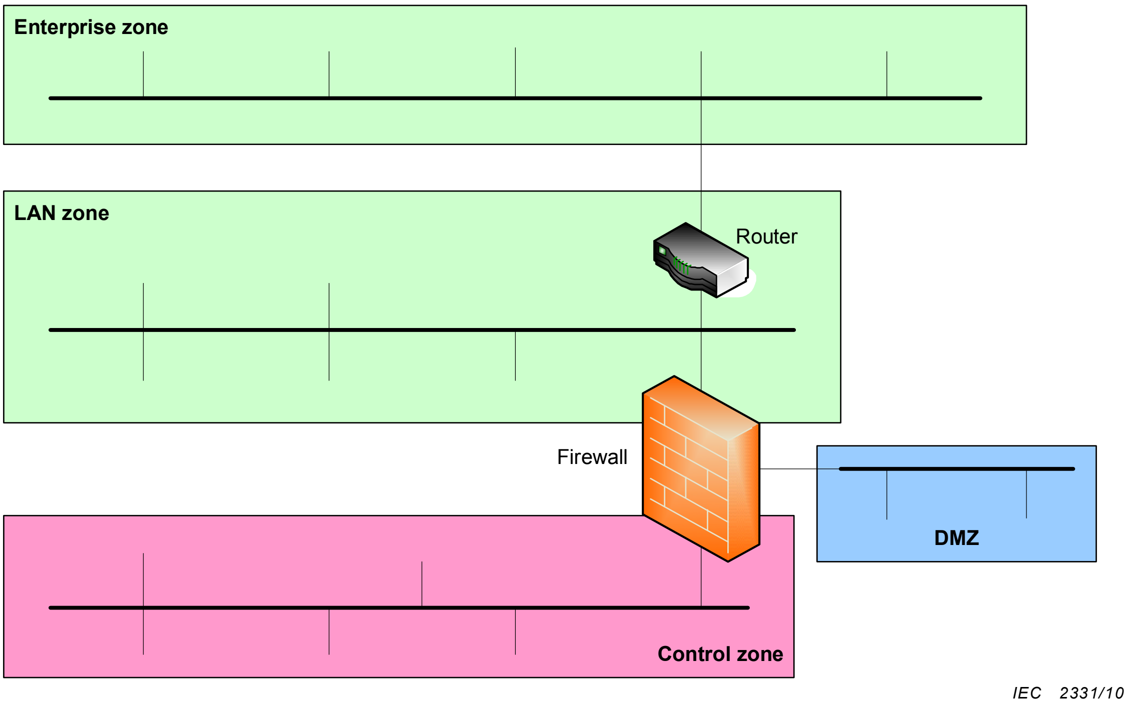


Figure A.15 – Corporate security zone template architecture

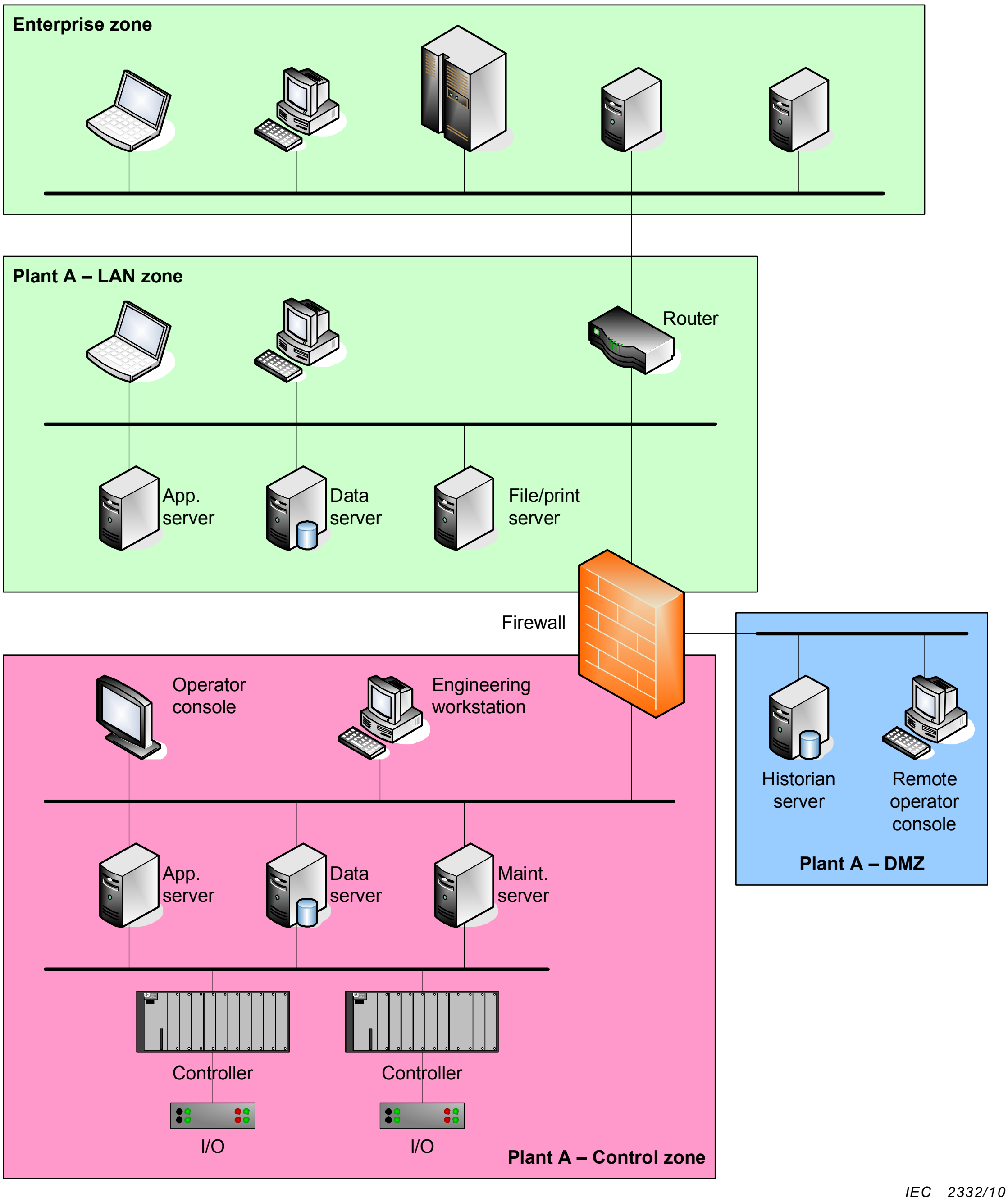


Figure A.16 – Security zones for an example IACS

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.

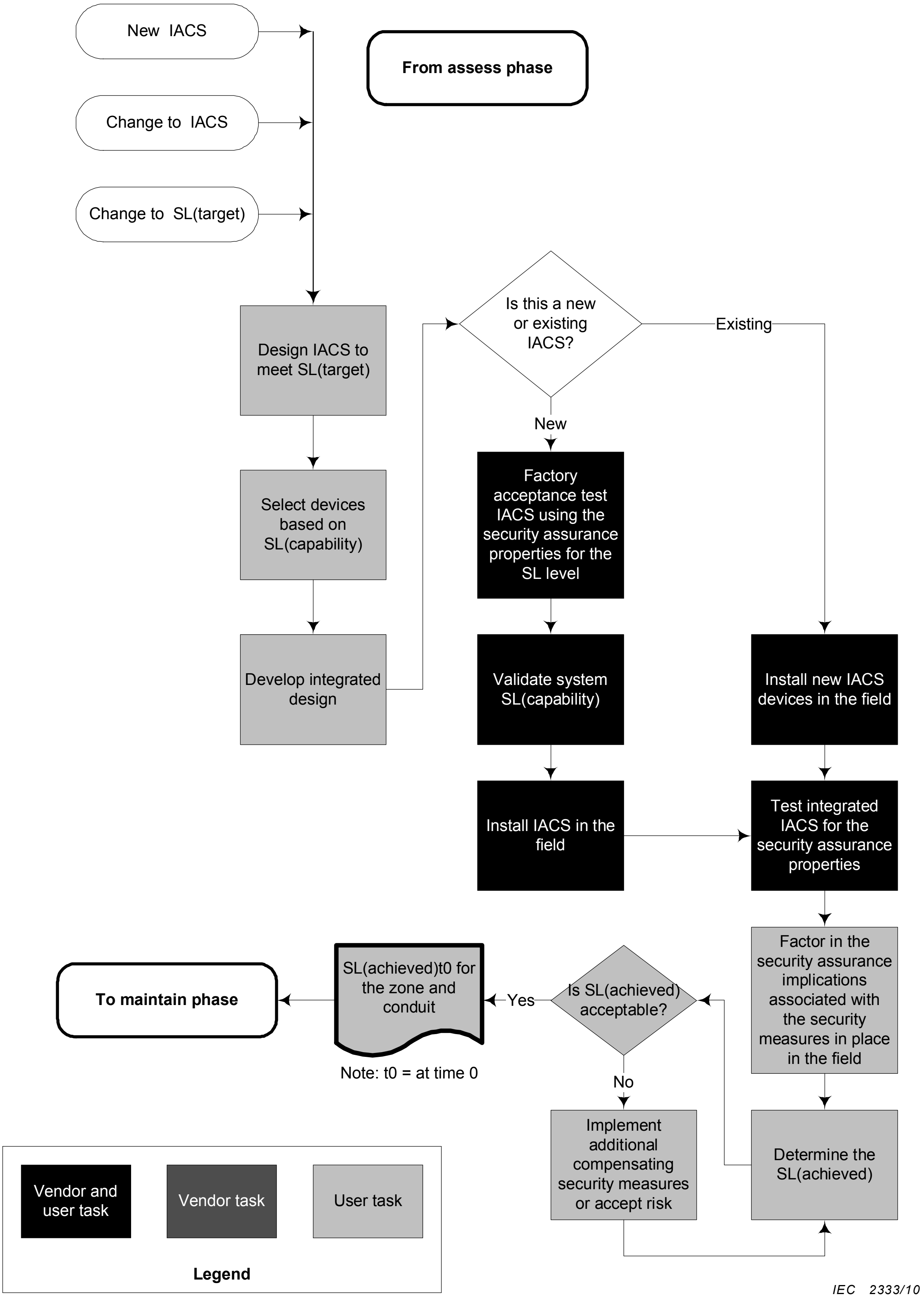

New IACS
Change to IACS
Change to SL(target)
From assess phase
Design IACS to meet SL(target)
Select devices based on SL(capability)
Develop integrated design
Is this a new or existing IACS?
Existing
New
Factory acceptance test IACS using the security assurance properties for the SL level
Validate system SL(capability)
Install IACS in the field
Install new IACS devices in the field
Test integrated IACS for the security assurance properties
Factor in the security assurance implications associated with the security measures in place in the field
Determine the SL(achieved)
Is SL(achieved) acceptable?
Yes
No
Implement additional compensating security measures or accept risk
SL(achieved)t0 for the zone and conduit
Note: t0 = at time 0
To maintain phase
Vendor and user task
Vendor task
User task
Legend
IEC 2333/10

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.

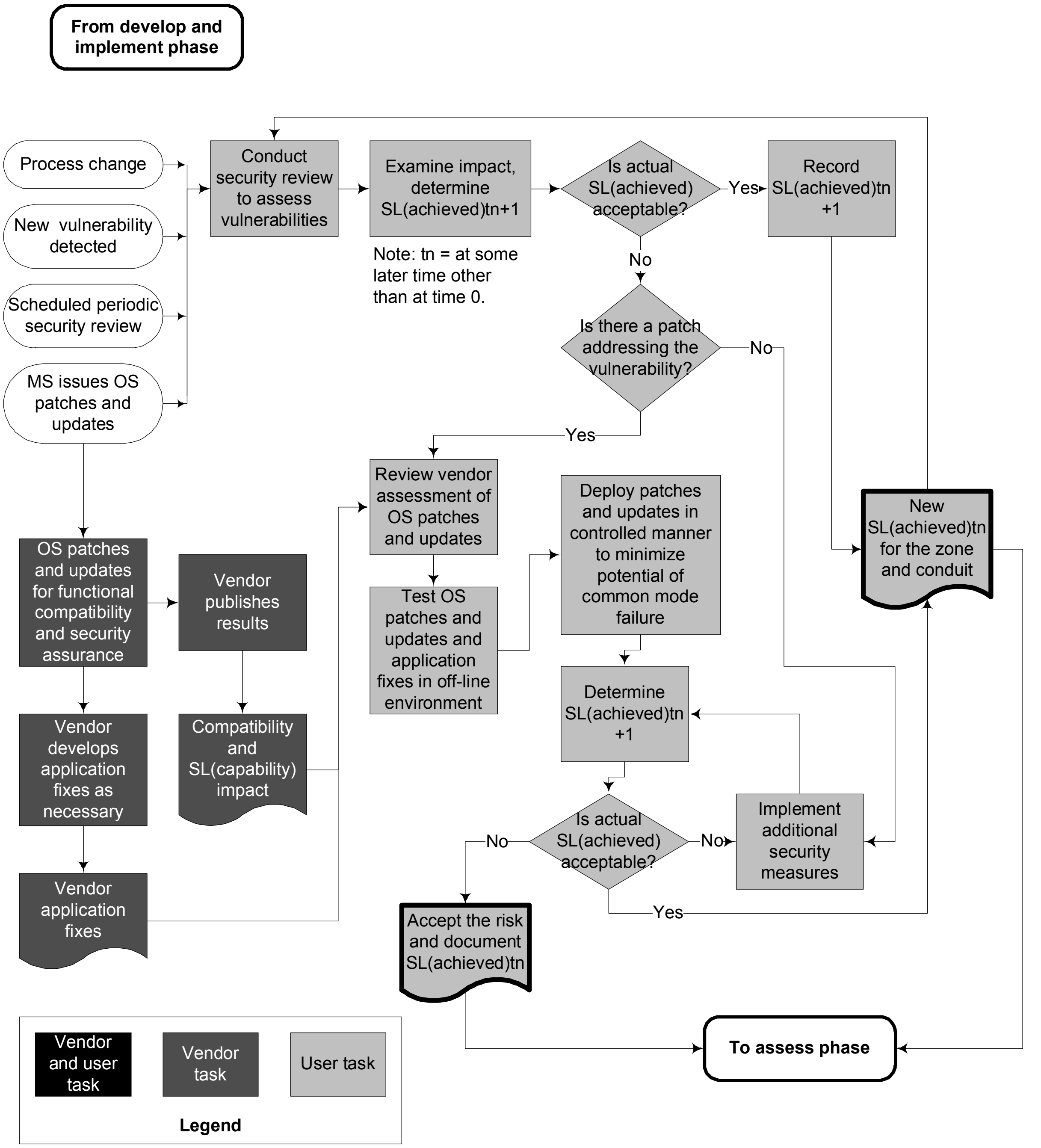

From develop and implement phase
Process change
New vulnerability detected
Scheduled periodic security review
MS issues OS patches and updates
Conduct security review to assess vulnerabilities
Examine impact, determine SL(achieved)tn+1
Note: tn = at some later time other than at time 0.
Is actual SL(achieved) acceptable?
Yes
No
Record SL(achieved)tn +1
Is there a patch addressing the vulnerability?
No
Yes
Review vendor assessment of OS patches and updates
Test OS patches and updates and application fixes in off-line environment
Deploy patches and updates in controlled manner to minimize potential of common mode failure
New SL(achieved)tn for the zone and conduit
OS patches and updates for functional compatibility and security assurance
Vendor publishes results
Vendor develops application fixes as necessary
Compatibility and SL(capability) impact
Vendor application fixes
Determine SL(achieved)tn +1
Is actual SL(achieved) acceptable?
No
No
Yes
Implement additional security measures
Accept the risk and document SL(achieved)tn
To assess phase
Vendor and user task
Vendor task
User task
Legend
IEC 2334/10

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].

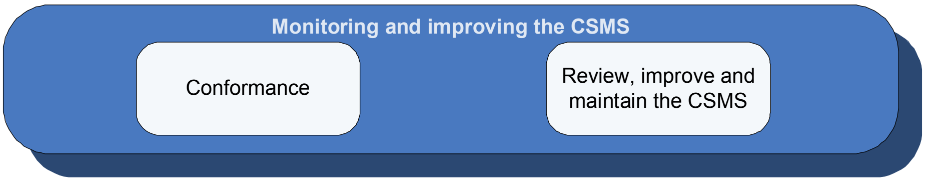
A.4 Category: Monitoring and improving the CSMS

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.


Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

IEC 2335/10

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

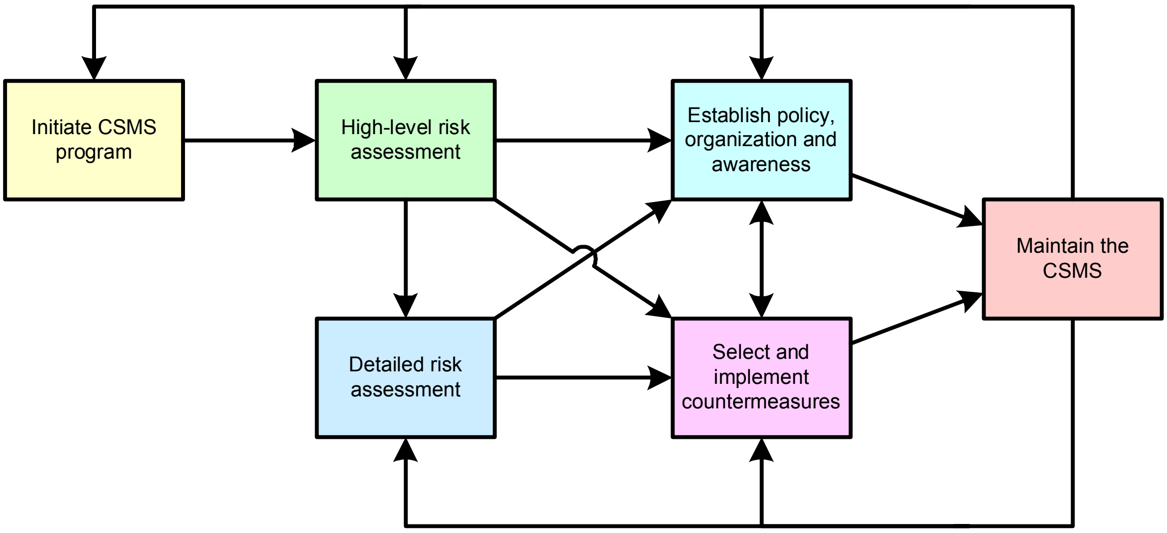
B.1 Overview

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.


Initiate CSMS program
High-level risk assessment
Establish policy, organization and awareness
Maintain the CSMS
Detailed risk assessment
Select and implement countermeasures

IEC 2336/10

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.

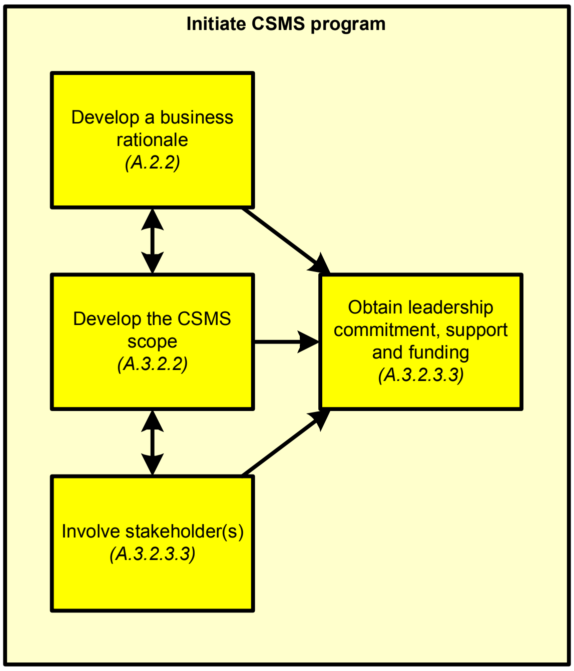
The two activities “Establish policy, organization and awareness” and “Select and implement countermeasures” directly lower risk to the organization. These activities will implement both high-level and low-level decisions, driven by both the high-level and detailed risk assessments. The “Establish policy, 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.



IEC 2337/10

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.

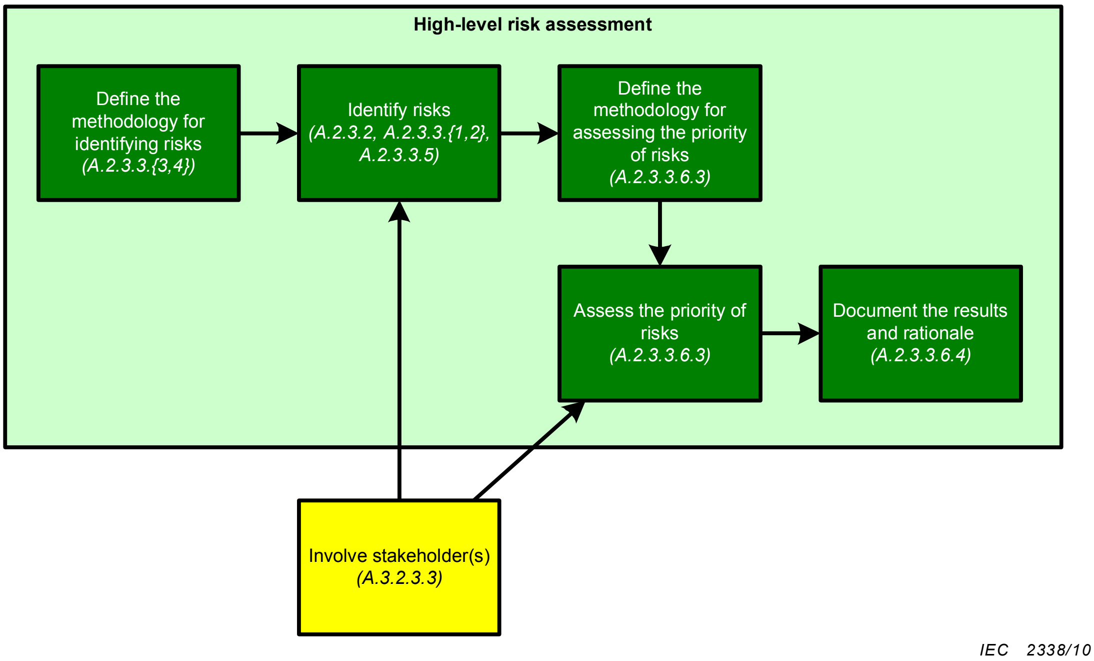
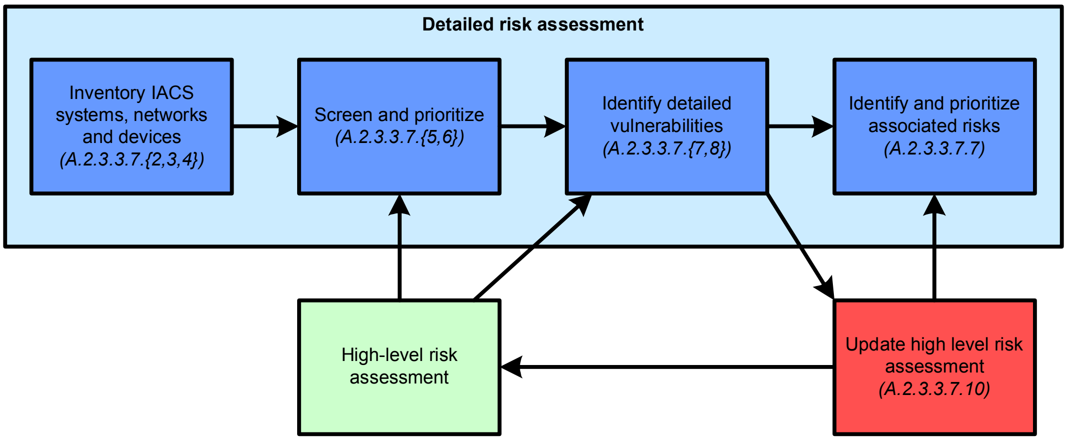

High-level risk assessment
Define the methodology for identifying risks (A.2.3.3.{3,4})
Identify risks (A.2.3.2, A.2.3.3.{1,2}, A.2.3.3.5)
Define the methodology for assessing the priority of risks (A.2.3.3.6.3)
Assess the priority of risks (A.2.3.3.6.3)
Document the results and rationale (A.2.3.3.6.4)
Involve stakeholder(s) (A.3.2.3.3)
IEC 2338/10

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.

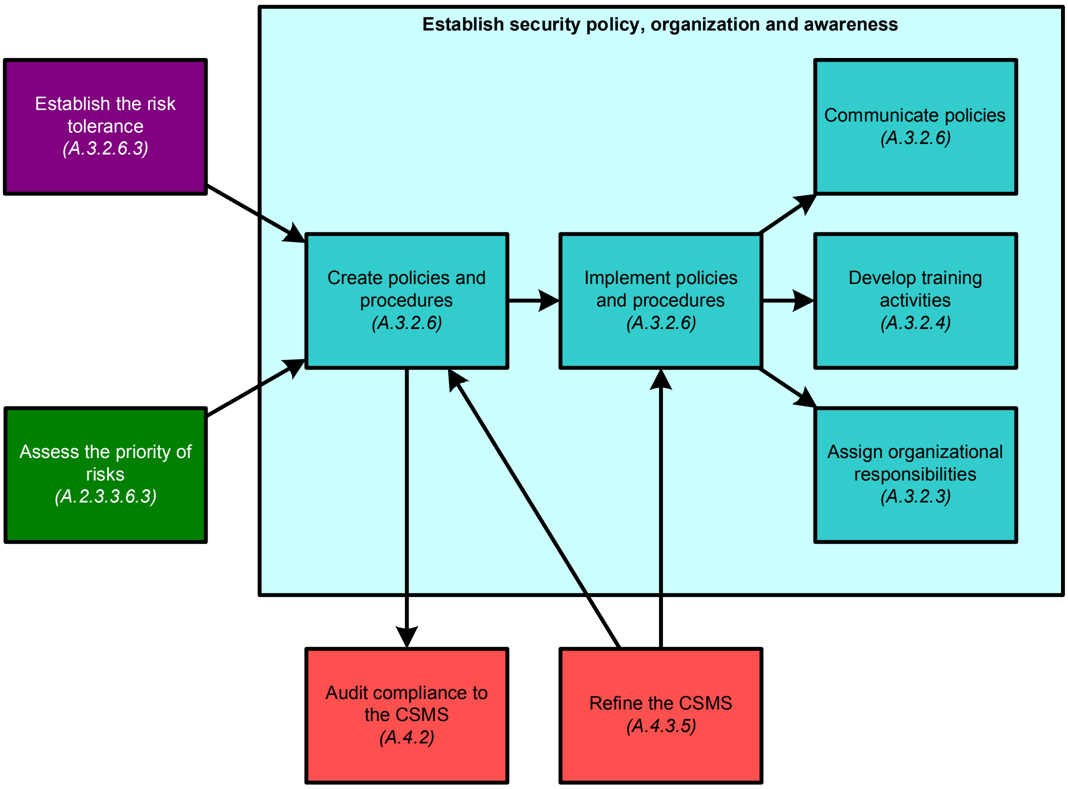

Detailed risk assessment
Inventory IACS systems, networks and devices (A.2.3.3.7.{2,3,4})
Screen and prioritize (A.2.3.3.7.{5,6})
Identify detailed vulnerabilities (A.2.3.3.7.{7,8})
Identify and prioritize associated risks (A.2.3.3.7.7)
High-level risk assessment
Update high level risk assessment (A.2.3.3.7.10)

IEC 2339/10

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.

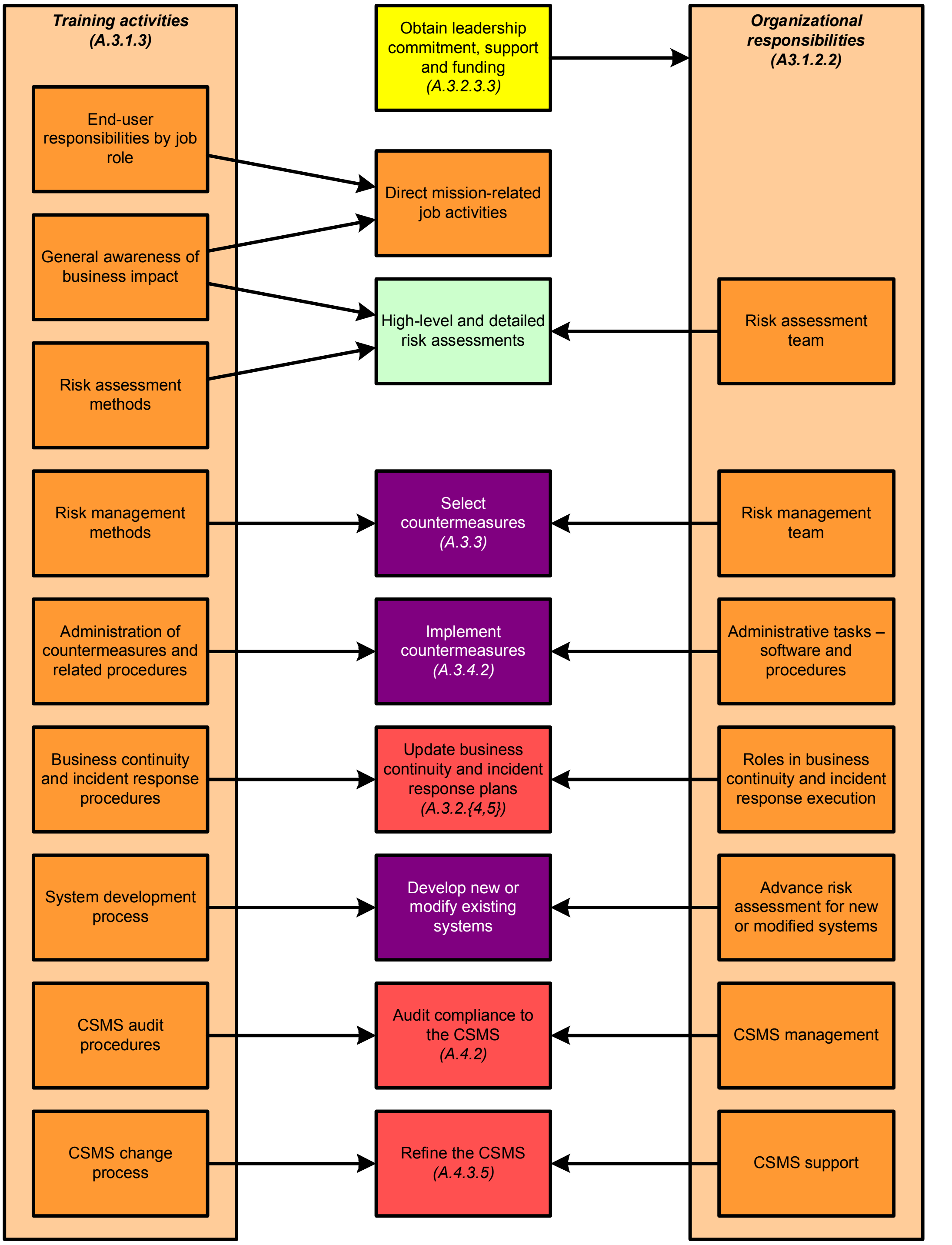

Establish security policy, organization and awareness
Establish the risk tolerance (A.3.2.6.3)
Assess the priority of risks (A.2.3.3.6.3)
Create policies and procedures (A.3.2.6)
Implement policies and procedures (A.3.2.6)
Communicate policies (A.3.2.6)
Develop training activities (A.3.2.4)
Assign organizational responsibilities (A.3.2.3)
Audit compliance to the CSMS (A.4.2)
Refine the CSMS (A.4.3.5)

IEC 2340/10

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.


Training activities
(A.3.1.3)
End-user responsibilities by job role
General awareness of business impact
Risk assessment methods
Risk management methods
Administration of countermeasures and related procedures
Business continuity and incident response procedures
System development process
CSMS audit procedures
CSMS change process
Obtain leadership commitment, support and funding
(A.3.2.3.3)
Direct mission-related job activities
High-level and detailed risk assessments
Select countermeasures
(A.3.3)
Implement countermeasures
(A.3.4.2)
Update business continuity and incident response plans
(A.3.2.{4,5})
Develop new or modify existing systems
Audit compliance to the CSMS
(A.4.2)
Refine the CSMS
(A.4.3.5)
Organizational responsibilities
(A3.1.2.2)
Risk assessment team
Risk management team
Administrative tasks – software and procedures
Roles in business continuity and incident response execution
Advance risk assessment for new or modified systems
CSMS management
CSMS support

IEC 2341/10

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.

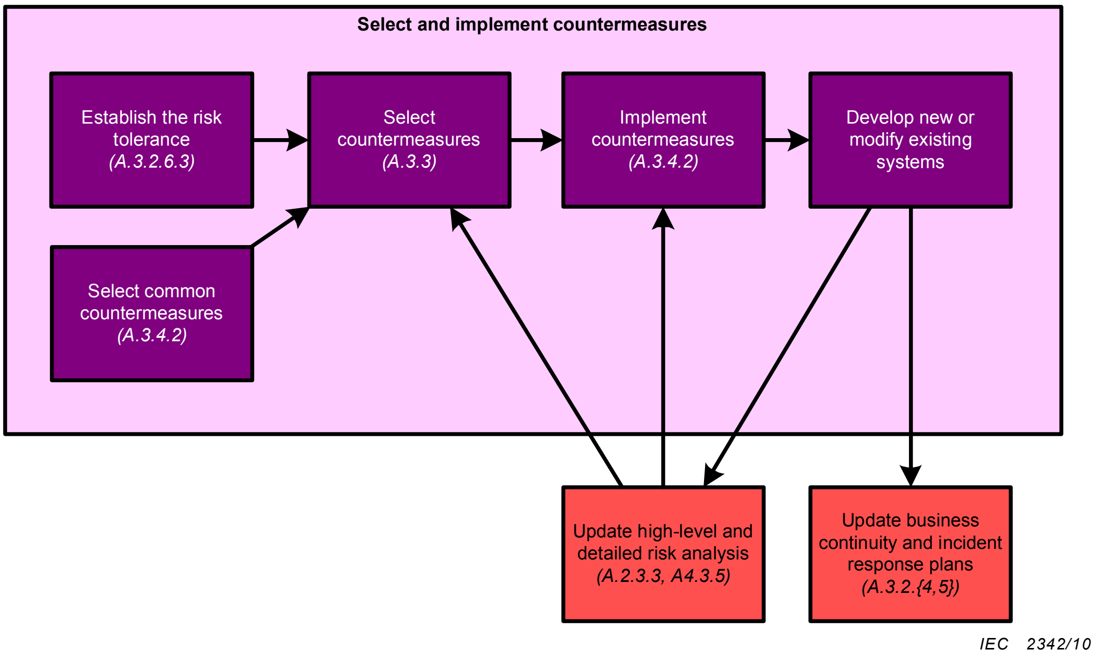

Select and implement countermeasures
Establish the risk tolerance (A.3.2.6.3)
Select countermeasures (A.3.3)
Implement countermeasures (A.3.4.2)
Develop new or modify existing systems
Select common countermeasures (A.3.4.2)
Update high-level and detailed risk analysis (A.2.3.3, A4.3.5)
Update business continuity and incident response plans (A.3.2.{4,5})
IEC 2342/10

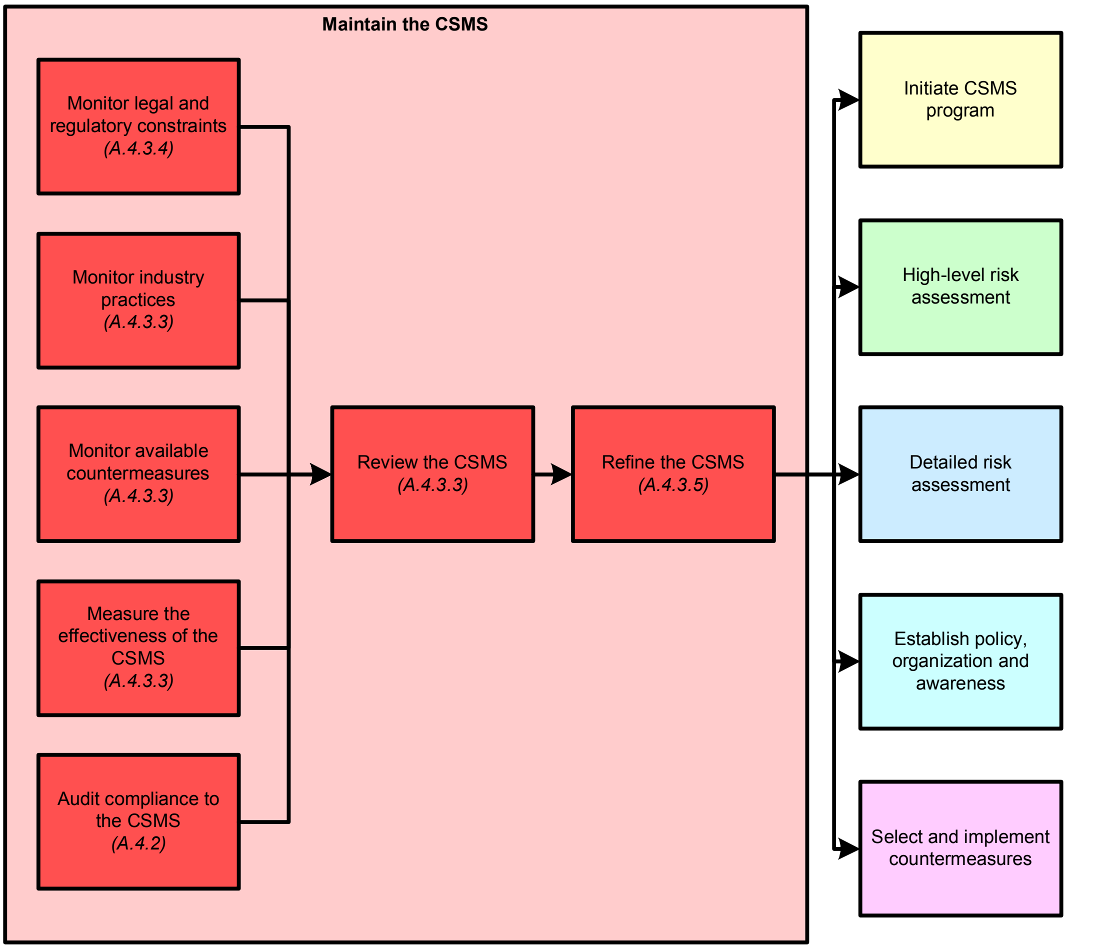
Figure B.7 – Activities and dependencies for activity: Select and implement countermeasures

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.


Maintain the CSMS
Monitor legal and regulatory constraints (A.4.3.4)
Monitor industry practices (A.4.3.3)
Monitor available countermeasures (A.4.3.3)
Measure the effectiveness of the CSMS (A.4.3.3)
Audit compliance to the CSMS (A.4.2)
Review the CSMS (A.4.3.3)
Refine the CSMS (A.4.3.5)
Initiate CSMS program
High-level risk assessment
Detailed risk assessment
Establish policy, organization and awareness
Select and implement countermeasures

IEC 2343/10

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 5.2.1 Provision of resources
4.2.3 Risk identification, classification and assessment	4.2.1c) Risk assessment approach 4.2.1d) Identify the risks 4.2.1e) Analyse and evaluate the risks 4.3.1 General document requirements A.6.2 External parties A.7.1 Responsibility for assets
4.3.2.2 CSMS Scope	4.2.1a) Scope and boundaries of ISMS 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 4.2.1i) Obtain management authorization to implement and operate the ISMS 4.2.2a) Formulate a risk treatment plan 4.2.2b) Implement the risk treatment plan 4.2.2g) Manage resources for the ISMS 5.1 Management commitment 5.2.1 Provision of resources A.6.1 Internal organization
4.3.2.4 Staff training and security awareness	4.2.2e) Implement training and awareness programs 5.2.2 Training, awareness and competence A.8.2 Human resources security – During employment
4.3.2.5 Business continuity plan	4.3.2 Control of documents 4.3.3 Control of records A.9.1 Secure areas A.9.2 Equipment security A.14.1 Information security aspects of business continuity management
4.3.2.6 Security policies and procedures	4.2.1b) ISMS policy 4.2.1h) Obtain management approval of the proposed residual risks 4.2.1i) Obtain management authorization to implement and operate the ISMS 4.2.2d) Define how to measure the effectiveness of the selected controls 4.3.1 General document requirements 4.3.2 Control of documents 7.1 Management review of the ISMS
4.3.3.2 Personnel security	A.6.1 Internal organization A.6.2 External parties A.8.1 Human resources security – Prior to employment A.8.2 Human resources security – During employment A.8.3 Human resources security – Termination or change of employment A.10.1 Operational procedures and responsibilities
4.3.3.3 Physical and environmental security	A.9.1 Secure areas A.9.2 Equipment security A.10.7 Media handling
4.3.3.4 Network segmentation	A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.10.6 Network security management A.11.4 Network access control
4.3.3.5 Access control: Account administration	A.11.1 Business requirement for access control A.11.2 User access management
4.3.3.6 Access control: Authentication	A.11.3 User responsibilities A.11.4 Network access control 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 A.11.7 Mobile computing and teleworking
4.3.4.2 Risk management and implementation	4.2.1d) Identify the risks 4.2.1e) Analyse and evaluate the risks 4.2.1f) Identify and evaluate options for the treatment of risks 4.2.1g) Select control objectives and controls for the treatment of risks 4.2.1h) Obtain management approval of the proposed residual risks 4.2.1j) Prepare a Statement of Applicability 4.2.2b) Implement the risk treatment plan 4.2.2c) Implement controls 4.2.2d) Define how to measure the effectiveness of the selected controls 4.2.2h) Implement procedures and controls to detect and respond to security events 5.2.1 Provision of resources
4.3.4.3 System development and maintenance	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.3 System planning and acceptance A.10.4 Protection against malicious and mobile code A.10.5 Back-up A.10.6 Network security management A.10.8 Exchange of information A.10.9 Electronic commerce services A.10.10 Monitoring A.12.1 Security requirements of information systems A.12.2 Correct processing in applications A.12.3 Cryptographic controls A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical Vulnerability Management
4.3.4.4 Information and document management	4.3.1 General document requirements 4.3.2 Control of documents 4.3.3 Control of records 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 4.3.2 Control of documents A.13.1 Reporting information security events and weaknesses 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 4.2.3a) Execute monitoring and reviewing procedures and other controls 4.2.3c) Measure the effectiveness of controls 4.2.3e) Conduct internal ISMS audits at planned intervals 6 Internal ISMS audits A.10.10 Monitoring A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards, and technical compliance A.15.3 Information systems audit considerations
4.4.3 Review, improve and maintain the CSMS	4.2.2f) Manage operation of the ISMS 4.2.3a) Execute monitoring and reviewing procedures and other controls 4.2.3b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3c) Measure the effectiveness of controls 4.2.3d) Review risk assessments, residual risks, and acceptable levels of risk at planned intervals 4.2.3f) Review the ISMS on a regular basis to determine if the scope remains adequate and improvements to the ISMS are identified 4.2.3g) Update security plans from monitoring and reviewing activities 4.2.3h) Record actions and events that could have an impact of the effectiveness or performance of the ISMS 4.2.4a) Implement the identified improvements of the ISMS 4.2.4b) Take appropriate corrective and preventive actions 4.2.4c) Communicate the actions and improvements to all interested parties 4.2.4d) Ensure that the improvements achieve their intended objectives 5.1 Management commitment 6 Internal ISMS audits 7.1 Management review of the ISMS 7.2 Review input for management review 7.3 Review output from a management review 8.1 Continual improvement of the ISMS 8.2 Corrective action 8.3 Preventive action 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 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 4.3.4.2 Risk management and implementation
4.2.1e) Analyse and evaluate the risks	4.2.2 Business rationale 4.2.3 Risk identification, classification and assessment 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 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 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 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 4.3.4.2 Risk management and implementation 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 4.3.4.5 Incident planning and response
4.2.3a) Execute monitoring and reviewing procedures and other controls	4.4.2 Conformance 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 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 4.3.2.2 CSMS Scope 4.3.2.6 Security policies and procedures 4.3.4.4 Information and document management
4.3.2 Control of documents	4.3.2.5 Business continuity plan 4.3.2.6 Security policies and procedures 4.3.4.4 Information and document management 4.3.4.5 Incident planning and response
4.3.3 Control of records	4.3.2.5 Business continuity plan 4.3.4.4 Information and document management
5.1 Management commitment	4.3.2.3 Organizing for security 4.4.2 Conformance 4.4.3 Review, improve and maintain the CSMS
5.2.1 Provision of resources	4.2.2 Business rationale 4.3.2.3 Organizing for security 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 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 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 4.3.3.2 Personnel security
A.6.2 External parties	4.2.3 Risk identification, classification and assessment 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 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 4.3.3.3 Physical and environmental security
A.9.2 Equipment security	4.3.2.5 Business continuity plan 4.3.3.3 Physical and environmental security
A.10.1 Operational procedures and responsibilities	4.3.3.2 Personnel security 4.3.3.4 Network segmentation 4.3.4.3 System development and maintenance 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 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 4.3.4.3 System development and maintenance
A.10.7 Media handling	4.3.3.3 Physical and environmental security 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 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 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 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/>

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