A.3.2.6.2 Developing security policies

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

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

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

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

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

A.3.2.6.3 Determining the organization’s tolerance for risk

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

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

A.3.2.6.4 Reviewing and revising cyber security policies

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

A.3.2.6.5 Deploying cyber security policies

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

A.3.2.6.6 Supporting practices

A.3.2.6.6.1 Baseline practices

The following five actions are baseline practices:

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

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

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

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

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

A.3.2.6.6.2 Additional practices

The following ten actions are additional practices:

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

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

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

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

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

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

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

h) Providing a consistent policy management framework.

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

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

A.3.2.6.7 Resources used

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

A.3.3 Element group: Selected security countermeasures

A.3.3.1 Description of element group

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

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

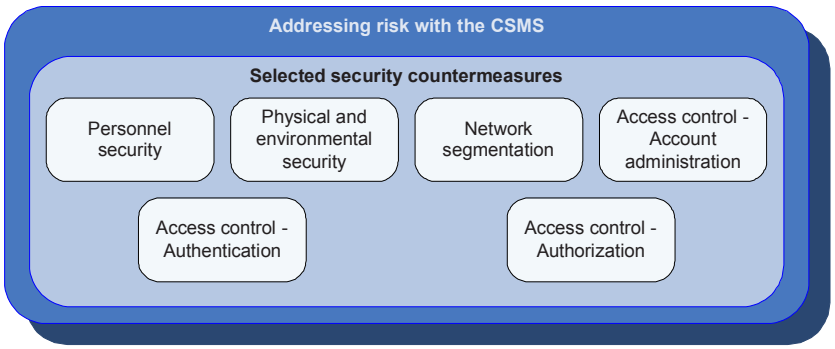

Figure A.7 – Graphical view of element group: Selected security countermeasures

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

A.3.3.2 Element: Personnel security

A.3.3.2.1 Description of element

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

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

A.3.3.2.2 Requirements for personnel security

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

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

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

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

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

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

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

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

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

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

A.3.3.2.3 Supporting practices

A.3.3.2.3.1 Baseline practices

The following eight actions are baseline practices:

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

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

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

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

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

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

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

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

A.3.3.2.3.2 Additional practices

The following two actions are additional practices:

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

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

A.3.3.2.4 Resources used

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

A.3.3.3 Element: Physical and environmental security

A.3.3.3.1 Description of the element

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

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

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

A.3.3.3.2 Considerations for physical and environmental security

A.3.3.3.2.1 General

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

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

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

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

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

A.3.3.3.2.2 Security policy

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

A.3.3.3.2.3 Security perimeter

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

A.3.3.3.2.4 Entry controls

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

A.3.3.3.2.5 Environmental damage protection

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

A.3.3.3.2.6 Security procedures

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

A.3.3.3.2.7 Single points-of-failure

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

A.3.3.3.2.8 Connections

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

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

A.3.3.3.2.9 Equipment maintenance

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

A.3.3.3.2.10 Alarms

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

A.3.3.3.2.11 Equipment lifecycle

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

A.3.3.3.2.12 Physical information

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

A.3.3.3.2.13 Use of assets outside controlled environments

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

A.3.3.3.2.14 Interim protection of critical assets

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

A.3.3.3.3 Supporting practices

A.3.3.3.3.1 Baseline practices

The following nine actions are baseline practices:

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

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

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

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

e) Protecting all external connections from tampering or damage.

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

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

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

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

A.3.3.3.3.2 Additional practices

The following seven actions are additional practices:

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

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

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

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

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

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

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

A.3.3.3.4 Resources used

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

A.3.3.4 Element – Network segmentation

A.3.3.4.1 Description of element

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

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

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

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

A.3.3.4.2 Network segments and zones

A.3.3.4.2.1 General

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

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

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

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

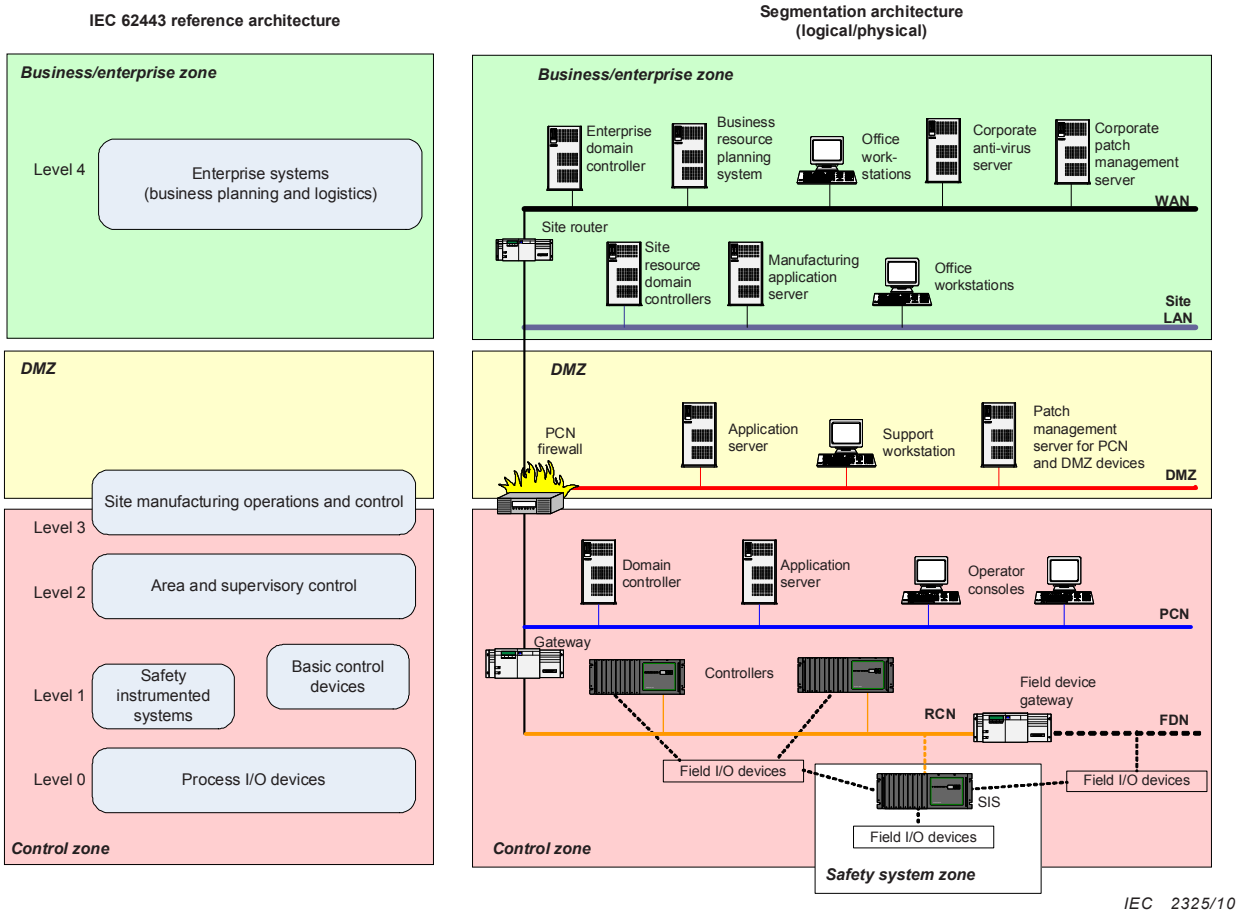

Figure A.8 – Reference architecture alignment with an example segmented architecture

A.3.3.4.2.2 Control zone

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

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

Common filtering strategies at the barrier device include:

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

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