Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002

Introductory element — Main element — Complementary element

Élément introductif — Élément central — Élément complémentaire
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Definitions</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Overview</td>
<td>7</td>
</tr>
<tr>
<td>4.1</td>
<td>Structure of this specification</td>
<td>7</td>
</tr>
<tr>
<td>4.2</td>
<td>Information security management systems for energy supply utilities</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Security policy</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Organization of information security</td>
<td>10</td>
</tr>
<tr>
<td>6.1</td>
<td>Internal organization</td>
<td>10</td>
</tr>
<tr>
<td>6.2</td>
<td>External parties</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>12</td>
</tr>
<tr>
<td>7.1</td>
<td>Responsibility for assets</td>
<td>12</td>
</tr>
<tr>
<td>7.2</td>
<td>Information classification</td>
<td>13</td>
</tr>
<tr>
<td>8</td>
<td>Human resource security</td>
<td>14</td>
</tr>
<tr>
<td>8.1</td>
<td>Prior to employment</td>
<td>14</td>
</tr>
<tr>
<td>8.2</td>
<td>During employment</td>
<td>15</td>
</tr>
<tr>
<td>8.3</td>
<td>Termination or change of employment</td>
<td>15</td>
</tr>
<tr>
<td>9</td>
<td>Physical and environmental security</td>
<td>15</td>
</tr>
<tr>
<td>9.1</td>
<td>Secure areas</td>
<td>15</td>
</tr>
<tr>
<td>9.2</td>
<td>Equipment security</td>
<td>18</td>
</tr>
<tr>
<td>9.3</td>
<td>Security in premises of 3rd parties</td>
<td>19</td>
</tr>
<tr>
<td>10</td>
<td>Communications and operations management</td>
<td>21</td>
</tr>
<tr>
<td>10.1</td>
<td>Operational procedures and responsibilities</td>
<td>21</td>
</tr>
<tr>
<td>10.2</td>
<td>Third party service delivery management</td>
<td>21</td>
</tr>
<tr>
<td>10.3</td>
<td>System planning and acceptance</td>
<td>21</td>
</tr>
<tr>
<td>10.4</td>
<td>Protection against malicious and mobile code</td>
<td>22</td>
</tr>
<tr>
<td>10.5</td>
<td>Backup</td>
<td>22</td>
</tr>
<tr>
<td>10.6</td>
<td>Network security management</td>
<td>22</td>
</tr>
<tr>
<td>10.7</td>
<td>Media handling</td>
<td>23</td>
</tr>
<tr>
<td>10.8</td>
<td>Exchange of information</td>
<td>23</td>
</tr>
<tr>
<td>10.9</td>
<td>Electronic commerce services</td>
<td>23</td>
</tr>
<tr>
<td>10.10</td>
<td>Monitoring</td>
<td>23</td>
</tr>
<tr>
<td>10.11</td>
<td>Legacy systems</td>
<td>24</td>
</tr>
<tr>
<td>10.12</td>
<td>Operating safety</td>
<td>25</td>
</tr>
<tr>
<td>11</td>
<td>Access control</td>
<td>25</td>
</tr>
<tr>
<td>11.1</td>
<td>Business requirement for access control</td>
<td>25</td>
</tr>
<tr>
<td>11.2</td>
<td>User access management</td>
<td>26</td>
</tr>
<tr>
<td>11.3</td>
<td>User responsibilities</td>
<td>26</td>
</tr>
<tr>
<td>11.4</td>
<td>Network access control</td>
<td>27</td>
</tr>
<tr>
<td>11.5</td>
<td>Operating system access control</td>
<td>28</td>
</tr>
<tr>
<td>11.6</td>
<td>Application and information access control</td>
<td>29</td>
</tr>
<tr>
<td>11.7</td>
<td>Mobile computing and teleworking</td>
<td>29</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>12</td>
<td>Information systems acquisition, development and maintenance</td>
<td>29</td>
</tr>
<tr>
<td>12.1</td>
<td>Security requirements of information systems</td>
<td>29</td>
</tr>
<tr>
<td>12.2</td>
<td>Correct processing in applications</td>
<td>29</td>
</tr>
<tr>
<td>12.3</td>
<td>Cryptographic controls</td>
<td>29</td>
</tr>
<tr>
<td>12.4</td>
<td>Security of system files</td>
<td>29</td>
</tr>
<tr>
<td>12.5</td>
<td>Security in development and support processes</td>
<td>30</td>
</tr>
<tr>
<td>12.6</td>
<td>Technical vulnerability management</td>
<td>30</td>
</tr>
<tr>
<td>13</td>
<td>Information security incident management</td>
<td>30</td>
</tr>
<tr>
<td>13.1</td>
<td>Reporting information security events and weaknesses</td>
<td>30</td>
</tr>
<tr>
<td>13.2</td>
<td>Management of information security incidents and improvements</td>
<td>30</td>
</tr>
<tr>
<td>14</td>
<td>Business continuity management</td>
<td>30</td>
</tr>
<tr>
<td>14.1</td>
<td>Information security aspects of business continuity management</td>
<td>30</td>
</tr>
<tr>
<td>14.2</td>
<td>Essential emergency services</td>
<td>31</td>
</tr>
<tr>
<td>15</td>
<td>Compliance</td>
<td>32</td>
</tr>
<tr>
<td>15.1</td>
<td>Compliance with legal requirements</td>
<td>32</td>
</tr>
<tr>
<td>15.2</td>
<td>Compliance with security policies and standards, and technical compliance</td>
<td>33</td>
</tr>
<tr>
<td>15.3</td>
<td>Information systems audit considerations</td>
<td>33</td>
</tr>
<tr>
<td>Annex A</td>
<td>(Informative) Expanded catalogue of controls for energy utilities</td>
<td>34</td>
</tr>
<tr>
<td>Annex B</td>
<td>(Informative) Requirements for Secure Control Systems</td>
<td>37</td>
</tr>
</tbody>
</table>
Introduction

This specification provides interpretation guidelines for the implementation and management of information security management for process control systems used in the energy utility industry based on ISO/IEC 27002 “Code of practice for information security management”. The aim of this standard is to extend the ISO/IEC 27000 standards to the domain of process control systems and automation technology used in the energy utility industry in order to allow the implementation of a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

In particular as a result of the transformation process of the conventional electricity grid into a Smart Grid digital infra-structure, ensuring a sufficiently high level of security is of paramount importance in order to guarantee a secure and reliable energy supply. While the market and service realm of the Smart grid IT infrastructure is sufficiently covered by the existing controls provided by ISO/IEC 27002, the special information security requirements for the process control domain have to be considered in a sector-specific standard.

At the focus of application of the standard are the systems and networks for controlling the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes. This includes the control and automation systems, the protection and safety systems and the measurement and test engineering systems, including their associated communications and telecontrol applications. For purposes of simplification, these systems will be collectively referred to in the following as, “process control systems”.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2005, the process control systems used by energy utilities and energy suppliers are subject special additional requirements. In comparison with conventional IT environments (e.g. office IT) there are fundamental and significant differences in respect of the development, operation, repair, maintenance and operating environment of process control systems. Furthermore, the process technology to which this standard pertains may represent integral components of critical infrastructures which means they are therefore essential for the secure and reliable operation of such infrastructures. These distinctions and characteristics must be duly taken into consideration by the management processes for the process control systems and justify separate consideration within the ISO/IEC 27000 series of standards.

In particular, the following fundamental differences exist in comparison with conventional IT systems:

Security features

In comparison with conventional IT systems, process control systems exhibit increased requirements with regard to their availability and integrity. In some operational environments failure of the process monitoring and control systems cannot be tolerated. Also, the integrity of the data is frequently of crucial importance. Incorrect data can cause incorrect control inputs, result in failure of protection or safety systems and, as a result of erroneous process images, lead to incorrect process mapping, resulting in wrong decisions being taken by the operating personnel. These requirements must be taken into consideration during the system design stage and also in system operations.

System architecture

Besides the central IT installations within control centers for grid operation or conventional power plants there are several systems which are typically distributed over large areas, e.g.:

- Process control and monitoring systems within substations and gas pressure regulating and metering stations
— Process control and monitoring systems for distributed generation, like wind-farms or photovoltaic generation units
— Process control and monitoring systems for Smart Grid applications
— Digital metering and measurement devices

Often, these remote systems cannot be provided with the same level of physical protection as for centrally located systems. Therefore, the system architecture must take these differences into consideration and where necessary, additional safeguards must be provided at the interface between distributed and central systems.

Also, the operating and management processes for distributed systems may vary in comparison with centralized IT architectures. It is for instance, not normal procedure to apply changes to essential operating systems at critical substations or at other important plants via telecontrol systems, unless the corresponding field service personnel are present on-site.

Furthermore, in many process control environments the architecture should allow for autonomous (local) operation of each distributed site – without network access to central installations. In case of blackouts it must be possible to restart selected sites without an external energy source, e.g. for grid restoration (black start capable systems).

**Maintenance**

Process control systems are often designed for a service life of up to 20 or more years. If standard operating systems or software packages are used, special measures to handle outdated and no-longer supported software are needed.

Frequent shutdowns of process control components, e.g. to install software patches or updates, are normally not possible. System restarts after software installation may not be acceptable due to the availability requirements. Maintenance has to be planned and scheduled in advance within an appropriate time period. Particularly thorough and careful pre-deployment testing is required in order to ensure that the integrity of the process control system is maintained.

**Equipment resources**

The in-process components of process control systems are mostly designed to support only the intended process data and frequently do not have sufficient system resources to support additional security software such as encryption or authentication.

**Target group**

This specification is targeted at the persons responsible for the operation of process control systems used by energy utilities and those responsible for information security, together with vendors, system integrators and auditors. For this target group it details the fundamental measures along with the objectives of the ISO/IEC 27002:2005 standard and defines specific measures for such process control systems, their supporting systems and the associated infrastructure.
1 Scope

The scope of this specification covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes in particular the following systems, applications and components:

- The overall IT-supported central and distributed process control, monitoring and automation technology as well as IT systems used for their operation, such as programming and parameterization devices
- Digital controllers and automation components such as control and field devices or PLCs, including digital sensor and actuator elements
- All further supporting IT systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving and documentation purposes
- The overall communications technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology
- Digital metering and measurement devices, e.g. for measuring energy consumption, generation or emission values
- Digital protection and safety systems, e.g. protection relays or safety PLCs
- Distributed components of future smart grid environments
- Distributed components of smart grid environments
- All software, firmware and applications installed on above mentioned systems

Outside the scope of this specification is the conventional or classic control equipment that is non-digital, i.e. purely electro-mechanical or electronic monitoring and process control systems.

Telecommunication systems and communications engineering used in the process control environment are also not directly part of the scope of this specification. These are covered by the standard “ISO/IEC 27011 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2005”. It is recommended that users of this specification should implement the measures defined in the standard for the telecommunication and communications engineering systems used in the process control environment.

2 Normative references

The documents referred to below are required for the purposes of this document. When such references are made only the version stated shall be applicable. If references are made without stating dates then the latest version of the document in question shall be applicable (including all changes).

3 Definitions

For the purposes of this document the definitions in accordance with ISO/IEC 27001, DIN ISO/IEC 27002 shall apply, together with the following definitions.

3.1 Debugging
Analyzing malfunctions in computer systems.

3.2 Energy utility
An energy supplier is a legal body or a person that supplies energy in form of electricity, gas or heat to other parties, to an energy distribution network or to a storage complex.

3.3 Critical Infrastructure
Critical infrastructure is a term used to describe organizations and facilities that are essential for the functioning of society and the economy as a whole. A failure or malfunction of such organizations and facilities would result in sustained supply shortfalls, make a significant impact on public security and have other wide ranging impacts.

3.4 Human-machine interface
HMI
User interface for operating and monitoring process control systems and/or plant.

3.5 Safety systems:
Systems and components that are required to ensure operating safety.

3.6 PLC
Programmable Logic Controller

3.7 Process control system
A system that serves to control and monitor the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes.

3.8 Maintenance
The general term “maintenance” as used in this document includes all measures used in the field of energy supply that are normally related to inspection, maintenance, fault clearance and improvement.

4 Overview

4.1 Structure of this specification
This specification has been structured in a format similar to ISO/IEC 27002:2005. Where no additional detailed information is necessary direct reference is made here to the specifications applicable to the objectives and measures set forth in ISO/IEC 27002:2005. In cases where the measures set forth in ISO/IEC 27002:2005 require a method of implementation that is specific to the energy supply sector or some form of expanded implementation, then this will be provided in the form of implementation guidelines for the energy supply sector or as further information. A list of the new control objectives and/or measures for the energy supply sector is set forth in Annex A (standard). Supplementary comments and notes are set forth in Annex B.
Further recommendations for implementation and information specific to energy utilities are included in the following clauses:

- Organization of information security (clause 6)
- Asset management (clause 7)
- Human resources security (clause 8)
- Physical and environmental security (clause 9)
- Communications and operations management (clause 10)
- Access control (clause 11)
- Information systems acquisition, development and maintenance (clause 12)
- Business continuity management (clause 14)
- Compliance (clause 15)

An overview of the additional security categories, control objectives and controls for process control systems is listed in Annex A (informative). Annex B (informative) exemplifies technical requirements for control system procurement.

4.2 Information security management systems for energy supply utilities

4.2.1 Objectives

From the viewpoint of design and function, the process control systems used by the energy utility sector are in fact information processing systems. They collect process data and monitor the status of the physical process subject to control using sensors. The systems then process this data and generate control outputs that regulate actions using actuators. The control and regulation of the plant is automatic but manual intervention by operating personnel is also possible. Information and information processing systems are therefore an essential part of the operational processes at energy utilities. This means that appropriate protection measures must be applied in the same manner as for other organizational units.

To an increasing degree, software and hardware components based on standard IT technology are used in process control environments.

Today, the information and information processing systems at the process control level are consequently also exposed to an increasing number of threats and vulnerabilities. It is therefore essential that, in the area of process control as used by the energy utility industry, adequate information security is achieved through the implementation and continuous improvement of an ISMS in accordance with ISO/IEC 27001.

Effective information security in the area process control as used by the energy utility sector can be achieved by establishing, implementing, monitoring, reviewing and if necessary improving the applicable measures set forth in this specification, in order to ensure that the specific security and business objectives of the organization will be reached. Particular consideration should be given here to the special role of the energy utilities in society and to the economic necessity of a secure and reliable energy supply.
4.2.2 Security considerations for process control systems used by the energy utilities

The requirement for a general and overall information security policy for the process control domain of the energy utility industry is based on several basic requirements:

a) Customers expect a secure and reliable energy supply.

b) Legal and regulatory requirements demand secure and reliable operation of the energy supply systems.

c) In their own interests energy providers themselves require information security in order to fulfill customer needs and comply with the legal regulations and to safeguard their business interests.

4.2.3 Information assets to be protected

In order to establish an information security management system, it is necessary for the organization to identify all of its organizational assets. The identification of organizational assets and the clarification of their importance enable the application of appropriate controls.

Further advice regarding the type of organizational assets that should be protected by an energy supply organization can be found in chapter 7.1.1.

4.2.4 Establishment of information security management

4.2.4.1 How to establish security requirements

It is essential that energy utility organizations identify their security requirements. There are three main sources of security requirements:

a) The results of an organization’s risk assessment, taking into account the organization’s general business strategies and objectives. Through risk assessment, threats to the organization’s own assets will be identified; vulnerabilities and likelihood of occurrence will be evaluated and potential impact assessed.

b) The requirements which result from laws and legal ordinances, regulations and contracts which have to be fulfilled by an organization, as well as sociocultural and social requirements. Particular examples include the assurance of a reliable, effective and secure energy supply as well as the reliable support of the requirements of a deregulated energy market, in particular the reliable and secure transfer of data with third parties.

c) The specific principles, objectives and business requirements placed on information processing, which was developed by the organization for supporting its business operations.

4.2.4.2 Assessing security risks

The necessary security measures or controls are determined by the methodical assessment of security risks. The cost of controls has to be balanced against the economic damage that may result from security issues. The results of the risk assessment facilitate the definition of adequate management actions and priorities for the management of information security risks as well as the implementation of the controls chosen to protect against these risks. The risk assessment should be repeated periodically in order to take all changes into account, which could affect the results of the risk assessment.

4.2.4.3 Selecting controls

Once the security requirements and risks have been identified and decisions taken on how to deal with the risks, appropriate controls should then be selected and implemented in order to ensure that the risks are reduced to an acceptable level.
In addition to the controls provided by a comprehensive information management system this specification provides additional assistance and sector-specific measures for the process control systems used by the energy utility sector, taking into consideration the specific special requirements prevailing there. It is therefore recommended that energy utilities implement the measures set forth in this specification. If necessary, further measures can be developed to fulfill special requirements. The selection of security measures depends upon the decisions taken by the organization on the basis of the risk acceptance criteria, the options for dealing with the risk and the general risk management approach of the organization. The selection of measures should also take relevant national and international law, legal ordinances and regulations into consideration.

4.2.4.4 Critical success factors

The content of ISO/IEC 27002:2005 clause 0.7 shall be applied correspondingly.

5 Security policy

The control objectives and the content of DIN ISO/IEC 27002:2005 clause 5 shall be applied correspondingly.

6 Organization of information security

6.1 Internal organization.

6.1.1 Management commitment to information security

Control 6.1.1 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.1.2 Information security co-ordination

Control 6.1.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.1.3 Allocation of information security responsibilities

Control 6.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.1.4 Authorization process for information processing facilities

Control 6.1.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.1.5 Confidentiality agreements

Control 6.1.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.1.6 Contact with authorities

Control 6.1.6 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility specific implementation guidance

The applications and infrastructure of energy utility process control systems may be considered as part of the critical infrastructure and may be essential for the functioning of the local community and society and the economy as a whole. Operators of such systems should therefore maintain contact with all of the relevant authorities. In addition to the public departments already mentioned this may for instance, also include:
— National and international agencies together with structures for co-operation for the protection of critical infrastructures.

— National and international CERT organizations.

— Disaster control organizations and disaster-relief teams

For operators of critical infrastructures additional local laws and regulations might apply, which have to be complied with correspondingly.

Further Information for the energy utility companies

During the course of system operation and operational planning and for making preparations for exceptional weather and operational situations, weather information, forecasts and severe weather advisories may be required. Direct contact should therefore be established with the corresponding local, regional and national meteorological services and corresponding information services (e.g. thunderstorm warning, lightning detection).

6.1.7 Contact with special interest groups

Control 6.1.7 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility specific implementation guidance

For the purpose of exchanging information on process control-specific security issues and to facilitate cross-organizational cooperation, contact should be maintained with the national and international vendor and operator associations and their working groups responsible for security issues.

6.1.8 Independent review of information security

Control 6.1.8 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

6.2 External parties

6.2.1 Identification of risks related to external parties

Control 6.2.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Process control systems may consist of complex individually customized systems and components. System vendors and integrators are often deeply involved in the maintenance and operation processes of these systems. For maintenance and fault clearance processes these external parties may use remote access connections that allow maintenance to be carried out from remote locations. Employees of external parties may also need access to security-controlled areas to perform on-site maintenance.

Close cooperation between the different system operators on the generation, transmission and distribution level, result in the close coupling of the control systems and communication networks of different organizations. Furthermore, external parties such as vendors, system integrators or business partners may also require access to sensitive information.

The risks resulting from such third party access to sensitive systems, networks and information should be assessed and taken into consideration, especially in terms of the exposure to risk of the primary physical process that is to be controlled or monitored.
6.2.2 Addressing security when dealing with customers

Control 6.2.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Energy utility-specific implementation guidance**

The complex and multifaceted relationships between asset owners, system operators, service providers and internal and external customers in the energy utility sector may result in clearly demarcated responsibilities in respect of the maintenance, operation and ownership of assets.

Examples of this include:

- An internal service provider that is responsible for the operation and maintenance of transmission or distribution grid infrastructure that is allocated to a separate internal organizational unit,
- A service provider responsible for the operation and maintenance of power plants or distributed generation units,
- An internal or external service provider that is responsible for the operation of the process control infrastructure.

Such multifaceted and/or complex business relationships must be taken into consideration when identifying and addressing the security requirements necessary for granting customer access to information assets. When process control systems are interconnected, the measures described in section 11.4.8 should be taken into consideration.

6.2.3 Addressing security in third party agreements

Control 6.2.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Energy utility-specific implementation guidance**

Under the terms of the agreement it should be ensured that the protection requirements for sensitive information are given sufficient consideration.

Where telecommunication services for the process control systems used by energy utilities are supplied by third parties, special requirements relating to crisis and emergency communication, in particular in case of major blackouts, natural catastrophes, accidents or other possible emergency situations, must be defined, contractually specified and monitored. This applies in particular to any necessary preemptive measures that may need to be taken in case of service overload and to ensuring an acceptable degree of independence of the telecommunication services of external energy utilities (blackout resistance).

7 Asset management

7.1 Responsibility for assets

7.1.1 Inventory of assets

Control 7.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Energy utility-specific implementation guidance**

When developing and maintaining the inventory of all of the organization’s important assets, the different responsibilities should be clearly specified and clearly documented.
The list of the organization’s own assets should cover all of the relevant process control systems and include information assets and applications.

**Further information for energy utilities**

The organization’s own assets in the area of energy supply should, further to the assets described above, also include a wide range of other sector-specific value categories such as:

a) **Information**: Grid and network plans, scheduling and dispatching data, geographical and georeferenced information, crisis and emergency plans, grid disaster recovery plans, switching operation data, measured values and measurement data, meter data, operating records, parameterization data, measurement and message archives, etc.

b) **Software**: Process control software, visualization systems, energy management and optimization software, simulation software, parameterization software, management and monitoring systems, operational resource planning systems, programming environments, firmware, archiving software, etc.

c) **Physical assets**: Control and automation components, telemetric and remote control components, data transmission system components, digital protection and safety components, digital metering and counting devices, digital sensor and actuating elements, parameterization and programming devices, visualization and operational components, digital monitoring and recording systems, etc.

d) **Services**: Telecommunication services, emergency communication services, information services

### 7.1.2 Ownership of assets

Control 7.1.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Further information for energy utilities**

The potentially complex structure of organizations that employ process control systems may give rise to highly diverse responsibilities with regard to mercantile and operational ownership. As a result, the ownership and the responsibilities in relation to assets, and the roles of the asset owner and asset operator in respect of information security should be exactly defined and documented.

### 7.1.3 Acceptable use of assets

Control 7.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

### 7.2 Information classification

#### 7.2.1 Classification guidelines

Control 7.2.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Energy utility-specific implementation guidance**

Energy utility-specific classification criteria may include the following points:

— Corporate assets, systems and information supporting the operation of critical infrastructures and sensitive systems.

— Corporate assets, systems and information needed for restoration of the energy supply system following a major supply disruption (grid restoration), e.g. blackstart capable systems and components.

— Corporate assets, systems and information necessary to ensure functional safety / plant security.
7.2.2 Information labeling and handling

Control 7.2.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

8 Human resource security

8.1 Prior to employment 1)

8.1.1 Roles and responsibilities

Control 8.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Staff employed in the energy utility sector to be responsible for systems technology should have the appropriate knowledge and skills to be in charge of the management and supervision of the installation, maintenance and safe operation of process control systems. This should also include sufficient expertise in the area of modern information system technology and information security.

The relevant control system engineers and other staff should be notified of their assigned roles and responsibilities, especially with regard to information security in respect of these systems.

8.1.2 Screening

Control 8.1.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

A strict screening process for key personnel that have access to critical information assets or that are responsible for the operation and maintenance processes of critical systems should be considered. This is especially the case if the information assets or systems are part of the critical infrastructure or if they are required for the operation of critical infrastructure.

Before newly employed personnel may be allowed to work on components that form part of the critical infrastructure, a specific security clearance provided by governmental organizations may, depending upon the competent authorities, be required.

8.1.3 Terms and conditions of employment

Control 8.1.3 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Restrictions on employee rights such as the right to strike or the authorization to exceed the maximum working time in emergency situations should, taking into consideration the statutory framework conditions, be considered for key personal responsible for the operation of critical infrastructures and sensitive systems.

1) Explanation: The term "employment" is used in this context to cover the following different situations: The employment of persons (on a short-term or more permanent basis), allocation of work responsibilities, changing of working responsibilities, allocation of contracts and also the termination of such arrangements.
Agreements on the monitoring and recording of specific actions such as switching operations should also be taken into consideration when formulating the contract of employment.

8.2 During employment

The controls and content of clause 8.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

8.3 Termination or change of employment

The controls and content of clause 8.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9 Physical and environmental security

9.1 Secure areas

9.1.1 Physical security perimeter

The controls of section 9.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Especially in energy transmission and distribution systems and in the area of distributed generation, the components are distributed across decentralized sites. Equipment is situated in control and technical rooms within the organization’s building and in peripheral sites. Sometimes the equipment is situated on third-party premises or in public environments. It is not normally possible to achieve a comprehensive level of physical protection for unmanned peripheral sites, therefore the residual risk must be assessed and mitigated where necessary, by means of supplementary measures.

9.1.2 Physical entry controls

Control 9.1.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

The use of physical access control systems should also be considered for peripheral sites where sensitive process control equipment is located. See section 9.1.9.

9.1.3 Securing offices, rooms and facilities

Control 9.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.1.4 Protecting against external and environmental threats

Control 9.1.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.1.5 Working in secure areas

Control 9.1.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.1.6 Public access, delivery and loading areas

Control 9.1.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
9.1.7 Securing control centers

This control is not included in ISO/IEC 27002:2005.

Control

Measures to ensure the physical security of control centers, where central control systems such as control servers, HMI and supporting systems are housed, should be designed, developed and applied.

Implementation guidance

To protect central control system facilities such as grid control centers or the control rooms of centralized or distributed power plants or generation units (hereinafter referred to as control centers), the following points should be taken into consideration:

a) A site located on solid ground should be selected for constructing the control center; where such solid ground is not available, appropriate measures should be taken in order to ensure the sufficient load bearing capacity of the foundation soil.

b) A site where the environment is least susceptible to damage from wind and water, etc., should be selected for control centers. Where a site is chosen that is vulnerable to such environmental damage then appropriate measures should be taken in order to prevent such damage from occurring.

c) A site where the environment is least susceptible to damage from strong electromagnetic field should be selected for control centers; where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect control system equipment rooms using electromagnetic shields.

d) Control centers should not be located at sites adjacent to facilities used for storing dangerous materials that pose the danger of explosion or combustion.

e) If the control center is located in an earthquake zone, control center buildings should be of earthquake-proof construction.

f) Control center buildings should be of fire-proof or fire-resistant construction.

g) Control center buildings must be designed with adequate structural stability to meet the necessary floor loadings.

h) Automatic fire alarms should be installed in control centers.

9.1.8 Securing equipment rooms

This control is not included in ISO/IEC 27002:2005.

Control

Measures to ensure the physical security of equipment rooms where control system facilities used by energy utilities are located, should be designed, developed and implemented.

Implementation guidance

To protect a room in which control system facilities used by energy utilities are located (hereinafter referred to as control system equipment rooms), the following controls should be considered:

a) The control system equipment room should be located where it is least susceptible to external effects such as extreme environmental conditions or natural disasters.
b) The control system equipment room should be located where it is least susceptible to intrusion by unauthorized personnel; adequate measures should be taken to prevent and possibly detect such intrusions.

c) Where possible, the control system equipment room should be unobtrusive. There should be minimum indication of its use as a control system equipment room for process control systems.

d) The control system equipment room should be located where it is least susceptible to flooding and the ingress of water. Should the room not fulfill this requirement, then the necessary measures should be taken such as raising the floor level, watertight design of the building and installing special water drainage facilities etc.

e) The control system equipment room should be located where it is best protected from strong electromagnetic fields. Should the room not fulfill this requirement, then it should be protected by electromagnetic shields or other suitable measures. This is particularly the case in the vicinity of high voltage / high current equipment or transformers etc.

f) Important components should be placed in a dedicated control system equipment room with appropriate physical protection.

g) In areas of high earthquake risk measures should be taken to prevent items and materials used for the floor, walls, ceiling from collapsing and falling.

h) The materials used for the floor, walls, ceiling etc. should be non-combustible or fire-resistant.

i) Measures should be taken to deal with faults caused by static charges.

j) Ducts connecting control system equipment rooms should be designed to slow down or prevent the spread of fire.

k) Where necessary, measures should be taken to protect the control system equipment rooms used as data storage rooms and for data backup from electromagnetic interference.

l) Fire-proofing measures should be implemented for data storage rooms.

m) Automatic fire alarms should be installed in control system equipment rooms and air-conditioning facility rooms.

n) Fire extinguishers should be installed in control system equipment rooms and air-conditioning facility rooms.

o) Control system equipment rooms should be air-conditioned.

p) Air-conditioning for control system equipment rooms and other important facilities should be provided by a separate system from that for offices and other areas of the building.

9.1.9 Securing peripheral sites

This control is not included in ISO/IEC 27002:2005.

Control

For peripheral sites where control system facilities used by energy utilities are located, physical security controls should be designed, developed and implemented.

Where a sufficient level of physical protection for peripheral sites is not attainable, the residual risk must be taken into consideration and mitigated by the application of appropriate countermeasures. When selecting such countermeasures the criticality of the process control systems operated at the peripheral sites and the
redundancy and fallback concepts implemented for the corresponding system function should be afforded primary consideration.

Implementation guidance

Especially in energy transmission and distribution networks and in distributed generation systems, elements of the control system infrastructure may be distributed across peripheral sites that are frequently unmanned. In order to protect such decentralized sites at which control system facilities are located for (hereinafter referred to as peripheral sites), the following controls should be considered:

a) If the peripheral site is located in an area of high earthquake risk, it should be earthquake-proof and comply with the corresponding national and regional standards.

b) Depending upon the criticality of the process control systems operated at peripheral sites, automatic fire control equipment should be installed.

c) Peripheral sites should be monitored for the purpose of detecting facility failures, power failures, fire etc. Where necessary, humidity and temperature should also be monitored.

d) Physically secure perimeters should be provided in a proper manner, for example, using secure fencing should be in-place and an automatic alarm system installed.

9.2 Equipment security

9.2.1 Equipment siting and protection

Control 9.2.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

The system components of process controls systems and supporting infrastructure may, under certain circumstances, have to be installed in areas with extensive exposure to dust, heat, cold, electromagnetic radiation, humidity etc. The equipment should be sufficiently suited to such environmental conditions, otherwise protective countermeasures should be implemented to ensure reliable operation.

9.2.2 Supporting utilities

Control 9.2.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

To avoid cyclic dependencies, all critical systems, communication services and facilities and other equipment that is required for system restoration after a power outage should be designed and operated such that they are independent of external supporting utilities for an appropriate period of time. This applied in particular to external energy supplies.

Further information for energy utilities

Depending upon the concepts for system restoration, the minimal bridging time for critical components essential for system restoration that must be operated independently from the external power supply must be at least 8h to 12h. In remote areas it may be necessary to provide an independent power supply that can operate for several days. This also includes an automatic emergency power generator as well as the corresponding stockpiling of fuel.
9.2.3 Cabling security

Control 9.2.3 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Especially in the sphere of energy transmission and distribution grids, communication networks are installed over long distances to allow communication with peripheral sites and provide remote maintenance access. It is frequently not possible to provide an equivalent level of protection for off-site cabling runs as for in-house cables. The associated risks should be assessed correspondingly and mitigated as far as possible by implementing supplemental physical measures. Depending upon the sensitivity of transmitted data, additional non-physical measures such as cryptographic protection should also be afforded consideration.

9.2.4 Equipment maintenance

Control 9.2.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.2.5 Security of equipment off-premises

Control 9.2.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.2.6 Secure disposal or re-use of equipment

Control 9.2.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.2.7 Removal of property

Control 9.2.7 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

9.3 Security in premises of 3rd parties

This control objective and associated measures are not included in ISO/IEC 27002:2005.

Objective: To protect equipment located outside of the energy utility organizations’ premises against physical and environmental threats.

9.3.1 Equipment sited on the premises of other energy utility organizations

Control

Where energy utility organizations install equipment outside of their own grounds or premises in areas that are the responsibility of other utilities, such as transfer stations for instance, the equipment should be sited in a protected area so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced.

Implementation guidance

To protect the equipment of an energy utility organization that is sited on the premises of other energy utility organizations, the following controls should be considered:

a) The limits of responsibility and interface with other energy utility organizations should be specified and it should – where necessary – be possible to easily isolate the equipment from that of the other organization. (See also 9.3.3).

b) Agreements should be concluded with the other energy utility organization for the supply of supporting infrastructure services such as energy supply, cooling, heating etc.
c) It should be ensured that the operational site where the equipment is to be installed fulfills the necessary security requirements.

**Further information**

In order to ensure that the security level of the other organization's premises is consistent with that of the energy utility organization's own premises, corresponding agreements and rules should be negotiated in advance.

### 9.3.2 Equipment sited on customer's premises

**Control**

Where energy utility organizations install equipment within customer premises, e.g. in order to control or measure the supply of energy and/or to deliver additional services, the organizations’ equipment should be protected so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced.

**Implementation guidance**

To protect equipment located at an energy utility customer’s site, the following controls should be considered:

a) The equipment cabinets installed at the customer’s site should be sturdy and it should not be easy for unauthorized users to open them. Any form of manipulation should be easily detectable

b) The limits of responsibility and interface with the customer should be specified and it should – where necessary – be possible to easily isolate the equipment from that of the customer.

c) It should be possible to remotely monitor the status of the equipment or to operate the equipment remotely.

### 9.3.3 Interconnected control and communication systems

**Control**

Where control systems and related communication links are interconnected with those of external third parties, the limits of responsibility and interface with the customer should be clearly defined such that it is possible to disconnect and isolate every organization within an appropriate period of time in order to avoid identified risks.

**Implementation guidance**

Energy utility organizations should monitor the status of the interconnected interfaces.

In order to diagnose problems and take corrective actions, the organizations should have a means for isolating the connection between itself and external third parties and – where necessary – for reconnecting isolated connections.

Energy utility organizations should specify in contracts or agreements that the system interconnections may be suspended in cases where severe interference occurs with the organization's own services.

The criteria and conditions necessary for the suspension of system interconnections should be clearly defined. Moreover the possible impacts of suspending system interconnections should be evaluated and if necessary fallback measures should be defined and prepared where necessary.
10 Communications and operations management

10.1 Operational procedures and responsibilities

10.1.1 Documented operating procedures

Control 10.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

In the operating processes documentation it should be specified exactly under which conditions the incident, emergency or crisis handling procedures are to be invoked (see section 13.2).

10.1.2 Change management

Control 10.1.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.1.3 Segregation of duties

Control 10.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.1.4 Separation of development, test and operational facilities

Control 10.1.4 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

In the field of process control as used by the energy utilities, the separation of development, test, and operational systems is not always possible to the full extent. This is especially true where real-time process data is needed for development, testing, trouble-shooting and debugging. In these special cases, where interconnections between development, test and operational systems are required or where testing and debugging at operational system level is necessary, overlaps should be reduced to an absolute minimum. The resulting risks should be identified and feasible alternatives, like process data emulators or remote debugging (debugging of the operational system using secured communication system interfaces) should be considered.

If the separation of development, test, and operational systems cannot be implemented, then – depending upon the criticality of the system in question – specially modified change management, incident, emergency or crisis handling procedures should be established that will allow a rapid and appropriate reaction to interferences and problems in the operational system.

Moreover it should be ensured that development and test systems are also secured using the state-of-the-art technology. According to their criticality it should be ensured that the test and development systems are sufficiently isolated from other system and networks (e.g. operation in a separate network environment, no direct Internet access, etc.) and that they are exclusively used for development and testing.

10.2 Third party service delivery management

The controls and the content of clause 10.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.3 System planning and acceptance

The controls and the content of clause 10.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
10.4 Protection against malicious and mobile code

10.4.1 Controls against malicious code

Control 10.4.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

If the software that protects against malicious code cannot be deployed for technical reasons (e.g. as a result of a lack of vendor support or release of updated software, the impossibility of installing timely updates), the resulting risks should be identified and other types of countermeasures should be implemented that provide an equal degree of protection.

Supplementary controls against malicious code include, among others:

- Securing of all physical and logical data interfaces.
- Network isolation and implementation of segmented network security zones that limit the impact of a malware incident.
- Comprehensive system hardening measures to minimize the risk of malware incidents.
- The use of whitelisting solutions, which restrict the execution of non-approved software and code.

In particular, the possible effects of malware incidents on equipment used for real-time process control and associated communications (e.g. through overload and disruption) should be taken into consideration and mitigated by implementing the appropriate controls.

10.4.2 Controls to counter mobile code (mobile agents)

Control 10.4.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

The technology behind the so-called intelligent electricity grids (Smart grids) is based on communicative networking and the installation of distributed control systems that may, among others, be situated on customer’s premises. For this purpose, distributed software and mobile agents may be used which could be provided and installed by the customer or by other third parties. The risks resulting from the use of mobile code should be taken into consideration and treated appropriately.

10.5 Backup

The controls and the content of clause 10.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.6 Network security management

10.6.1 Network controls

Control 10.6.1 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.6.2 Security of network services

Control 10.6.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
10.6.3 Securing process control data communication

This control is not included in ISO/IEC 27002:2005.

Control

Measures to ensure the confidentiality, integrity and availability of internal and external process control data communication should be designed, developed and implemented in accordance with the level of sensitivity of the data transmitted.

Implementation guidance

In the field of process control data communication several technical standards and protocols exist, such as:

- IEC 60870-5
- DNP3
- IEC 61850
- IEC 61400-25
- IEC 62350 – Communications Systems for Distributed Energy Resources (DER)
- Modbus

The standard communication protocols usually do not include dedicated security mechanisms.

The risks resulting from this, together with the implementation of modified countermeasures, should be taken into consideration. Countermeasures may include the activation of supported security features that are already supported (e.g. in accordance with IEC 62351) or additional cryptographic protection (e.g. encryption, integrity checks and authentication of the communication partners) on the lower network levels.

10.7 Media handling

The controls and the content of clause 10.7 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.8 Exchange of information

The controls and the content of clause 10.8 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.9 Electronic commerce services

The controls and the content of clause 10.9 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.10 Monitoring

10.10.1 Audit logging

Control 10.10.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance
In the energy utility sector, relevant audit events may also include certain actions carried out by operating personnel, such as switching operations for instance. Audit and retention requirements may be stipulated in industry-specific legislation and by regulatory bodies for a wide range of electronic records.

The acquisition, processing and management of audit protocols and data should be implemented in accordance with all applicable business, statutory, regulatory and internal requirements.

10.10.2 Monitoring system use

Control 10.10.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.10.3 Protection of log information

Control 10.10.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.10.4 Administrator and operator logs

Control 10.10.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.10.5 Fault logging

Control 10.10.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

10.10.6 Clock synchronization

Control 10.10.6 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

For all systems that are directly or indirectly interconnected with external partners, a common and agreed standard such as Central European Time (CET) or Coordinated Universal Time (UTC) should be used.

Further information for energy utilities

Depending upon the criticality of the process control system in question, the use of dedicated, non-internet synchronized NTP servers or of digitally signed NTP time messages should be considered in order to impede the manipulation of NTP signals.

10.11 Legacy systems

This control objective and associated measures are not included in ISO/IEC 27002:2005.

Objective: To protect against risks resulting from the use of legacy systems, where adequate security measures cannot be implemented.

10.11.1 Treatment of legacy systems

Control

All conventional legacy process control system technologies, systems and components (legacy systems) should be identified along with their potential information security vulnerabilities. Appropriate controls should be implemented in order to mitigate all of the identified risks associated with legacy process control technologies and process control systems.

Implementation guidance
A large number of the process control systems used in the energy utility industry are based on legacy technologies which lack basic security features. To provide an appropriate level of security, the security vulnerabilities of the legacy systems and technologies and the resulting risks should be identified. In situations where standard controls cannot be implemented, other types of countermeasure should be applied, for example:

a) The implementation of strict and appropriate network segregation.

b) Remote access for configuration and maintenance purposes should be avoided. If remote access is absolutely necessary, proper network isolation, e.g. through the use of secure proxy services should be ensured. Access for maintenance purposes should only be provided via defined interconnection points that are operated and monitored in a manner that is technically sound.

c) Strict access control rules should be enforced on the network, system and application level.

d) It should be ensured that only state of the art equipment and components are used for maintenance and configuration purposes.

10.12 Operating safety

This control objective and associated measures are not included in ISO/IEC 27002:2005.

Objective: To ensure the integrity and availability of the functions relating to operating safety (safety functions).

10.12.1 Integrity and availability of operating safety functions

Control

The integrity and availability of information assets, systems, components and functions that are required to ensure operating safety should be provided in accordance with sector-specific standards and legal requirements.

Implementation guidance

In order to ensure the operating safety functions the following measures should be considered:

a) The use of dedicated, isolated communication systems for the transmission of safety related data communications.

b) Ensuring that the operating safety functions are independent of the process control and automation systems.

c) The prevention of changes to critical safety systems and their safety-related configuration data by remote access means.

d) The logging of changes to the configuration of safety systems.

11 Access control

11.1 Business requirement for access control

11.1.1 Access control policy

Control 11.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:
Energy utility-specific implementation guidance

In addition, the policy should take account of the following:

a) The application of conditions and regulations pertaining to the usage of group accounts, where the use of personal user accounts is not possible. In order to ensure a sufficient level of access security and traceability, precise rules regarding exceptions should be defined, together with supplementary measures.

b) Conditions and regulations that are applicable to systems that do not support a strong password policy or where such a password policy is not possible for operational reasons. In order to ensure a sufficient level of access security, supplementary measures should be defined in particular.

11.2 User access management

The controls and the content of clause 11.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.3 User responsibilities

11.3.1 Password use

Control 11.3.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

In the process control environment it is not always possible to ensure the use of secure passwords, e.g.:

- Legacy systems often do not allow for individual passwords and/or passwords with necessary strength.

- It is frequently impossible to connect systems operated at decentralized plants, such as substations or distributed generation units, to central directory services, which means that local accounts and passwords have to be used. This makes it practically impossible to change passwords regularly.

It should therefore be clearly indicated to the user when the general password policy applies and where different passwords are to be used or if it is not possible to use any passwords at all (legacy systems).

Especially in situations where only one unique password is used for general system access, the password should be chosen to be as secure as possible. In particular, the standard passwords used by the system vendors should be considered as insecure and widely known. Passwords should only be accessible to persons who are involved in the operation of the system.

11.3.2 Unattended user equipment

Control 11.3.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.3.3 Clear desk and clear screen policy

Control 11.3.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
11.4 Network access control

11.4.1 Policy on use of network services
Control 11.4.1 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.2 User authentication for external connections
Control 11.4.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.3 Equipment identification in networks
Control 11.4.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.4 Remote diagnostic and configuration port protection
Control 11.4.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.5 Segregation in networks
Control 11.4.5 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Where applicable and technically feasible, the network infrastructure of process control systems should be divided into multiple zones with different functions and protection requirements. In particular, different technical and operational domains should be segregated from one another.

Where technically feasible, the network zones should be separated by firewalls, filtering routers or gateways. Network connections to external networks, such as the corporate office network, external partners or remote maintenance access connections, should exclusively be routed via especially hardened application proxies, which are located in a separate network zone (demilitarized zone) specifically for this purpose.

If applicable and technically feasible, the networks and distributed systems should be divided into independent horizontal segments (e.g. according to different locations or plant units). These segments should be separated by firewalls, filtering routers or gateways.

11.4.6 Network connection control
Control 11.4.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.7 Network routing control
Control 11.4.7 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.4.8 Logical coupling of external process control systems
This control is not included in ISO/IEC 27002:2005.

Control

Before the logical coupling of process control systems and related communication links with external parties, the energy utility organization should ensure that only authorized communications and information flows, including control system commands and messages can be exchanged over the link. The risk resulting from such system coupling should be assessed.
Implementation guidance

Process control systems should only be coupled with external third parties if this is necessary for operational reasons. Coupling should only be carried out at defined coupling points which are operated and monitored in a manner that is technically sound.

The type and extent of authorized communications, including the necessary data exchange and control commands should be defined and approved. The use of filtering devices (such as gateways, proxies or application level firewalls) to allow only authorized communication and information flows should be considered.

11.5 Operating system access control

11.5.1 Secure log-on procedures

Control 11.5.1 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.5.2 User identification and authentication

Control 11.5.2 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

The use of unique user identifiers may not always be feasible in energy utility process control systems, e.g. for accessing the operating system or firmware of embedded systems like PLCs or for maintenance processes in distributed systems. The resulting risk and mitigating countermeasures should be taken into consideration.

The use of individual and group user accounts should be consistent with applicable audit requirements (cf. 10.10.1)

11.5.3 Password management system

Control 11.5.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.5.4 Use of system utilities

Control 11.5.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.5.5 Session time-out

Control 11.5.5 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

The activation of session time-outs and screensavers may not be appropriate in certain process control applications, for example in HMIs and visualizations used for continuous process monitoring by operating personnel, e.g. in control centers. For such applications the resulting risks of unattended sessions should be taken into consideration and corresponding supplementary countermeasures implemented.

11.5.6 Limitation of connection time

Control 11.5.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
11.6 Application and information access control

The controls and the content of clause 11.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

11.7 Mobile computing and teleworking

The controls and the content of clause 11.7 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

12.1.1 Security requirements analysis and specification

Control 12.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Further information for energy utilities

To support the acquisition of control systems annex B exemplifies essential control system specific security measures, which can be used during system procurement.

12.2 Correct processing in applications

The controls and the content of clause 12.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12.3 Cryptographic controls

The controls and the content of clause 12.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12.4 Security of system files

12.4.1 Control of operational software

Control 12.4.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Energy utility organizations should minimize the risk of corruption of operational systems by observing the following guidelines on controlling changes (change management):

a) If changes to applications and core systems (operating system software, firmware) are to be implemented on sensitive systems, comprehensive tests should be carried out in a dedicated test environment that resembles the operational system environment and its interactions with the physical process as closely as possible (cf. 10.1.4).

b) In the case of sensitive process control system applications, at least three generations of software, parameter sets and configuration data should be retained.
12.4.2 Protection of system test data
Control 12.4.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12.4.3 Access control to program source code
Control 12.4.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12.5 Security in development and support processes
The controls and the content of clause 12.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

12.6 Technical vulnerability management
The controls and the content of clause 12.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

13 Information security incident management

13.1 Reporting information security events and weaknesses
The controls and the content of clause 13.1 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

13.2 Management of information security incidents and improvements
The controls and the content of clause 13.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

14 Business continuity management

14.1 Information security aspects of business continuity management

14.1.1 Including information security in the business continuity management process
Control 14.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

Energy utility-specific implementation guidance

Energy utility organizations should consider the continuity of the general energy supply as one of the key elements of business continuity management. For this reason, disaster recovery concepts and procedures for relevant emergency and crisis scenarios affecting critical process control systems, e.g. outages, failures and malfunctions should be considered.

14.1.2 Business continuity and risk assessment

14.1.3 Developing and implementing continuity plans including information security
Control 14.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
14.1.4 Business continuity planning framework

Control 14.1.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

14.1.5 Testing, maintaining and re-assessing business continuity plans

Control 14.1.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

14.2 Essential emergency services

This control objective and associated measures are not included in ISO/IEC 27002:2005.

Objective: To ensure the availability of essential emergency services in the case of major disturbances, natural disasters, accidents or other major emergency situations.

14.2.1 Emergency communication

Control

Should major disturbances, natural disasters, accidents or any other emergencies occur, or if there is a risk of occurrence thereof, energy utility organizations should ensure that essential communication links are maintained with their own emergency staff and/or the emergency staff of other utilities, with essential control systems and with external emergency organizations necessary for the protection and handling of, or recovery from such incidents.

Implementation guidance

Essential communication links may include voice and data transmission, for example with the following:

- Operating and emergency staff in central or decentral locations
- Internal and external crisis management
- Power stations
- Distributed energy producers
- Transmission and distribution grid operators
- Meteorological organizations
- Flood prevention organizations
- Fire service organizations
- Disaster relief organizations
- Safety authorities
- Telecommunication service providers
- Medical institutions
- Other national or local organizations that handle essential public services.
Furthermore, emergency communications may include data links with the following:

- Emergency control systems and related subcomponents
- Emergency alarm and monitoring systems and related subcomponents

Especially in the field of electric power supply it must be considered that the communication links which may be required for system restoration might in turn rely on the electric power supply.

15 Compliance

15.1 Compliance with legal requirements

15.1.1 Identification of applicable legislation

Control 15.1.1 as set forth in ISO/IEC 27002:2005 shall be augmented as follows:

**Energy utility-specific implementation guidance**

Requirements specific to the energy utility sector may include the following provisions:

- Requirements relating to the secure, safe and reliable operation of energy facility components, systems and networks
- Requirements relating to non-discrimination and unbundling in regulated energy markets
- Requirements relating to the protection of critical infrastructures
- National and international data protection legislation
- Other regulatory requirements

In the course of planning systems that will have a long service life, foreseeable changes in requirements should be taken into consideration as far as possible, so that these can be implemented at a manageable cost of modification.

15.1.2 Intellectual property rights (IPR)

Control 15.1.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

15.1.3 Protection of organizational records

Control 15.1.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

15.1.4 Data protection and privacy of personal information

Control 15.1.4 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

15.1.5 Prevention of misuse of information processing facilities

Control 15.1.5 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

15.1.6 Regulation of cryptographic controls

Control 15.1.6 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
15.2 Compliance with security policies and standards, and technical compliance

The controls and the content of clause 15.2 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.

15.3 Information systems audit considerations

The controls and the content of clause 15.3 as set forth in ISO/IEC 27002:2005 shall be applied correspondingly.
Annex A
(Informative)

Expanded catalogue of controls for energy utilities

The specific security categories, control objectives and controls for process control systems used by energy utility organizations set forth in sections 5 to 15 and that are not included in DIN ISO/IEC 27002:2005 are listed once again below in the form of an overview.

Table A.1 Overview of the supplementary security categories and control objectives

<table>
<thead>
<tr>
<th>Section number</th>
<th>Title</th>
<th>Control objectives</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3</td>
<td>Security in premises of 3rd parties</td>
<td>To protect equipment located outside of the energy utility organizations’ premises against physical and environmental threats.</td>
<td>19</td>
</tr>
<tr>
<td>10.11</td>
<td>Legacy systems</td>
<td>To protect against risks resulting from the usage of legacy systems, where adequate security measures cannot be implemented.</td>
<td>24</td>
</tr>
<tr>
<td>10.12</td>
<td>Operating safety</td>
<td>To ensure the integrity and availability of operating safety functions.</td>
<td>25</td>
</tr>
<tr>
<td>14.2</td>
<td>Essential emergency services</td>
<td>To ensure the availability of essential emergency services in the case of major disturbances, natural disasters, accidents or other major emergency situations.</td>
<td>31</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Control</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>9.1.7</td>
<td>Securing control centers</td>
<td>Measures to ensure the physical security of control centers, where central control systems such as control servers, HMI and supporting systems are housed, should be designed, developed and applied.</td>
<td>16</td>
</tr>
<tr>
<td>9.1.8</td>
<td>Securing equipment rooms</td>
<td>Measures to ensure the physical security of equipment rooms where control system facilities used by energy utilities are located, should be designed, developed and implemented.</td>
<td>16</td>
</tr>
<tr>
<td>9.1.9</td>
<td>Securing peripheral sites</td>
<td>For peripheral sites where control system facilities used by energy utilities are located, physical security controls should be designed, developed and implemented.</td>
<td>17</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Equipment sited on the premises of other energy utility organizations</td>
<td>Where energy utility organizations install equipment outside of their own grounds or premises in areas that are the responsibility of other utilities, such as transfer stations for instance, the equipment should be sited in a protected area so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced.</td>
<td>19</td>
</tr>
<tr>
<td>9.3.2</td>
<td>Equipment sited on customer’s premises</td>
<td>Where energy utility organizations install equipment within customer premises, e.g. in order to control or measure the supply of energy and/or to deliver additional services, the organizations’ equipment should be protected so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced.</td>
<td>20</td>
</tr>
<tr>
<td>9.3.3</td>
<td>Interconnected control and communication systems</td>
<td>Where control systems and related communication links are interconnected with those of external third parties, the limits of responsibility and interface with the customer should be clearly defined such that it is possible to disconnect and isolate every organization within an appropriate period of time in order to avoid identified risks.</td>
<td>20</td>
</tr>
<tr>
<td>10.6.3</td>
<td>Securing process control data communication</td>
<td>Measures to ensure the confidentiality, integrity and availability of internal and external process control data communication should be designed, developed and implemented in accordance with the level of sensitivity of the data transmitted.</td>
<td>23</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Control</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>10.11.1</td>
<td>Treatment of legacy systems</td>
<td>All conventional legacy process control system technologies, systems and components (legacy systems) should be identified along with their potential information security vulnerabilities. Appropriate controls should be implemented in order to mitigate all of the identified risks associated with legacy process control technologies and process control systems.</td>
<td>24</td>
</tr>
<tr>
<td>10.12.1</td>
<td>Integrity and availability of operating safety functions</td>
<td>The integrity and availability of information assets, systems, components and functions that are required to ensure operating safety should be provided in accordance with sector-specific standards and legal requirements.</td>
<td>25</td>
</tr>
<tr>
<td>11.4.8</td>
<td>Logical coupling of external process control systems</td>
<td>Before the logical coupling of process control systems and related communication links with external parties, the energy utility organization should ensure that only authorized communications and information flows, including control system commands and messages can be exchanged over the link. The risk resulting from such system coupling should be assessed.</td>
<td>27</td>
</tr>
<tr>
<td>14.2.1</td>
<td>Emergency communication</td>
<td>Should major disturbances, natural disasters, accidents or any other emergencies occur, or if there is a risk of occurrence thereof, energy utility organizations should ensure that essential communication links are maintained with their own emergency staff and/or the emergency staff of other utilities, with essential control systems and with external emergency organizations necessary for the protection and handling of, or recovery from such incidents.</td>
<td>31</td>
</tr>
</tbody>
</table>
Annex B
(Informative)

Requirements for Secure Control Systems

To support the acquisition of control systems the following catalog sets forth essential control system-specific security requirements that can be used during system procurement. The guideline defines fundamental requirements for the systems, applications and components as well as the corresponding development, maintenance and service processes.

The procurement requirement catalog is directed at manufacturers, system integrators and external planners on the vendor side as well as in-house planners, implementers and operators on the purchaser side. It is suggested that before the procurement phase commences, an individual security requirements analysis and possibly a supplementary individual risk analysis are carried out early in the planning process. Based on the findings of the security requirements and risk analysis, the planned system should then specify in detail how the individual requirements should be fulfilled.

B.1.1 General and Documentation Requirements

B.1.1.1 General Requirements

B.1.1.1.1 Secure System Architecture

The system should be designed and built for secure operations, following secure design principles.

Examples of secure design principles are minimal-privileges/need-to-know, defense-in-depth/redundancy, default-deny, diversity-in-defense, secure-by-default, input-validation etc.

B.1.1.1.2 Contact Person

The contractor shall provide a contact person who will be the single point of contact for information security related topics during the procurement process, the system design and implementation phase and throughout the projected period of system operations.

B.1.1.1.3 Patching and Patch Management

The system should allow the patching of all system components during normal system operation. The installation of a patch should usually be possible without interruptions to normal system operations and with little impact on the system’s availability and primary processes.

The contractor should support a patch management process for the entire system. This process should manage the testing, installation and documentation of security patches and system updates.

In general, it should be possible for the operating staff who administer the system to be able to install the patches and updates. Installation and de-installation of patches and updates should be authorized by the system owner/operator and must not be performed automatically.

B.1.1.1.4 Provision of Security Patches for all System Components

The contractor should provide security updates for all system components throughout the entire, contractually agreed lifecycle of the system.
The contractor should obtain updates for basic system components which are not developed by the contractor but by third parties (e.g. operating system, library, database management system etc.) from the component vendor. He should also test and approve them for installation. The contractor should provide security updates or approvals in an appropriate timeframe, which should be defined in the contract specifications.

**B.1.1.1.5 Third-Party Support**

The contractor should ensure that security support for third-party system components (e.g. operating systems, libraries, database management systems etc.) will be available for the full scheduled life cycle of the system. The end-of-life terms (e.g. last customer ship date, end of support date) of all system components should be defined in the contract specifications.

**B.1.1.1.6 Encryption of Sensitive Data during Storage and Transmission**

Sensitive data should be stored or transmitted in encrypted form only. Sensitive data may include, but is not limited to: log files, passwords, or sensitive data as defined by regulatory or legal requirements (e.g. data protection laws).

If necessary, the system should allow for the secure deletion of selected data, for example by overwriting with random data.

**B.1.1.1.7 Cryptographic Standards**

When selecting cryptographic standards, regulations and national restrictions should be taken into consideration. Only state-of-the-art cryptographic standards and key lengths should be used. From the current state of scientific and technical knowledge these standards and key lengths should also be considered secure for the foreseeable future.

Cryptographic algorithms developed in-house should not be used. Whenever possible, well-known cryptographic libraries should be used when implementing cryptographic functions to avoid implementation bugs.

**B.1.1.1.8 Internal and External Software and Security Tests and Related Documentation**

The contractor should perform a detailed security and stress test on the individual system components and on the entire system and its essential functions using a representative system configuration.

The team undertaking these tests should be independent from the development team. The test procedure should be coordinated with the customer. The results of these tests and the related documentation (software versions, test configuration, etc.) should be provided to the customer. Additionally, the customer shall be entitled to carry out security and stress tests or have them conducted by an external third party.

**B.1.1.1.9 Secure Standard Configuration, Installation and Start-Up**

After initial installation and start-up the system should be configured in a fail-safe and secure manner. The defined secure base configuration should be documented. System services, data and functions, which are used during development or for system testing only should be verifiably removed or deactivated before the systems goes live.

**B.1.1.1.10 Integrity Checks**

It should be possible to verify the integrity of system and application files, firmware and executables, system configuration and application parameter files, for example through the use of cryptographic check sums.
B.11.2 Documentation Requirements

B.1.1.2.1 Design Documentation, Specification of Security Architecture and Relevant System Components

The contractor should provide the customer with documentation covering the high level design and security architecture of the entire system. The documentation should be available not later than the time of the acceptance test and should include the description of the system concept and of the interaction of all system components. The documentation should characterize especially the details, interactions and dependencies of the system components that are security-relevant or which deserve special protection. Furthermore the documentation should list and describe in brief the implementation details relating to security related functions (e.g. the cryptographic standards used).

B.1.1.2.2 Administrator and User Documentation

The contractor should provide separate user and administrator documentation. Both sets of documentation should include a list of security functions and parameters as well as instructions and responsibilities for secure operation of the system.

B.1.1.2.3 Documentation of Security Parameters and Security Log Events or Warnings

The administrator documentation should include a description of all security-relevant parameters and their default values. The documentation should warn of the consequences of grossly insecure parameter settings.

Furthermore, documentation should be provided that includes all security events, warnings and log messages that the system generates, their possible causes and the related administrative action that should be taken.

B.1.1.2.4 Documentation of Requirements and Assumptions needed for Secure System Operation

The administrator documentation should provide a description of requirements relevant for secure system operation. The description may for example, contain assumptions about user behavior and network environment or requirements for interaction and communication with other systems or networks.

B.1.2 Base System

B.1.2.1 System Hardening

All components of the base system should be permanently hardened according to well-known best-practice guides. Furthermore, the latest security patches and service packs should be installed. Unnecessary user accounts, default users, system services, programs, network protocols and services should be removed, or – if removal is technically not possible – should be permanently disabled and secured against accidental re-activation. The secure base system configuration should be reviewed and documented.

B.1.2.2 Malware Protection

Where technical feasible, the base systems should be secured with malware protection software. As an alternative to installing malware protection, the contractor may implement a comprehensive protection concept, which provides an equivalent level of protection.

B.1.2.3 Autonomous User Authentication

Data used for user identification and authentication should not solely be obtained from sources located outside of the secure process network. Integration of user identification and authentication into a central isolated directory service within the process network should be considered.
B.1.3 Networks / Communication

B.1.3.1 Secure Network Design and Communication Standards

B.1.3.1.1 Deployed Communication Technologies and Network Protocols

a) Where technically feasible, the systems should only use secure communication standards and protocols which provide integrity checks, authentication and, if applicable, encryption. In particular, secure communication should be used for remote administration or transmission of user log-on information. The unsecured transmission of password or other authentication information (e.g. in clear text) should not be allowed.

b) The system and its network components should be easily integrateable into the network conception of the purchaser. Secure protocols should be used for administration and monitoring purposes. The network components should be hardened, unnecessary services and protocols should be deactivated, management interfaces should be protected.

c) It should be possible to integrate network components which are provided by the contractor into a central asset and patch management process. It should be possible to manage relevant network configuration parameters like IP addresses centrally.

d) In wide area networks, insecure application layer protocols should be secured cryptographically on lower network layers.

e) All used network protocols should support the deployment of firewalls.

f) If shared network infrastructure components are to be used, then the network with the highest protection level requirement shall determine the security requirements of the shared hardware components and their configuration. Concurrent use of the network hardware for networks with different protection levels is permitted only if this concurrent use does not decrease the security level or the availability.

B.1.3.1.2 Secure Network Design

a) Functional network segmentation: Where applicable and technically feasible, the network infrastructure of the system should be divided into multiple zones with different functions and protection requirements. Where technically feasible, the network zones should be separated by firewalls, filtering routers or gateways. Network connections to external networks should be deployed only using communication protocols approved by the customer and in compliance with the security policies in effect.

b) Site network segmentation: Where applicable and technically feasible the network infrastructure of the system should be divided into independent site segments, e.g. according to different plant zones or geographical sites. The segments should be separated by firewalls, filtering routers or gateways.

c) Firewalls and VPN components should be provided and managed centrally by the customer through a defined process.

B.1.3.1.3 Documentation of Network Design and Configuration

The contractor should provide documentation which should describe the network design and configuration, all physical, virtual and logical network connections, the network protocols used, and all network perimeter components which are part of, or which interact with the system.

All changes to the network configuration should be included in the documentation using a document management process. The documentation should provide values for normal and maximum expected data rates for all network connections.

B.1.3.2 Secure Maintenance Processes and Remote Access

B.1.3.2.1 Secure Remote Access

d) It should be possible to perform administration, maintenance and configuration of all networked com-
ponents via out-of-band channels, such as local access, serial interfaces, network or direct control of input devices (KVM).

e) Remote access should be performed through dedicated centrally administered proxy or terminal servers which ensure isolation of the process network and which are located in a DMZ. Strong 2-factor authentication should be used for remote access.

f) Direct dial-in access to devices should not be used.

g) Remote access should be (centrally) logged, multiple failed login attempts should result in a security event audit message.

h) All remote access possibilities and ports should be documented.

B. 1.3.2.2 Maintenance Processes

i) Interactive remote access users should use personal accounts. Restricted accounts should be used for non-interactive, automated processes, for which interactive access is disabled.

j) Technical measures should ensure that remote access sessions are explicitly activated by the administrative personnel. For external service personnel activation must be performed for each individual session. Where applicable, each session should be disconnected after a reasonable time period.

k) Maintenance should be performed by defined and trained contractor personnel only, using secure systems only. The systems used for remote access should be physically or logically disconnected from other systems and networks during a remote access session. A physical form of separation is preferred.

l) A defined maintenance process should ensure that maintenance personnel can only access systems, services and data they need for maintenance tasks.

m) Local maintenance by service personnel poses a significant security threat. Attachment of contractor’s hardware (e.g. laptops, USB devices) to the process network should be avoided. If this is not feasible, the hardware should be approved by the client, specifically secured and should be scanned for malware before attaching it. The contractor should provide evidence that an adequate internal security policy is implemented.

B.1.3.3 Wireless Technologies: Assessment and Security Requirements

Wireless network technology should not be used for systems with high or very high protection level requirements. In consultation with the customer WLAN technology may be deployed after a risk analysis has been performed and if the following essential security requirements are complied with:

• Wireless networks should only be deployed in separate network zones that are segregated from other networks by firewalls and application level proxies.

• Wireless network technology should be secured according to state-of-the-art practice.

B.1.4 Application Level

B.1.4.1 User Account Management

B. 1.4.1.1 Role-Based Access Model

The system should utilize a role-based user model that allows the separation of privileges according to operational requirements. The system should allow for granular access control to data and resources. The default access permissions should conform to a secure system configuration.

Examples of applicable user roles include:

• Operator: User who performs regular system operations. This may include the privilege to change op-
Read-only-user: User who is allowed to view the status of the system and to read defined data values but is not allowed to make changes to the system.

Administrator: A user who installs, maintains and administers the system. Therefore the administrator role has the authorization and the associated privileges to change the system and security configuration and settings.

Backup operator: A user who is allowed to backup relevant system and application data.

Auditor: User role which solely has the permission to inspect and archive the audit logs.

Security-relevant system configuration data can only be read or changed by the administrator role. For normal system use the operator or data-display role permissions should be sufficient. Individual user accounts can be disabled without removing them from the system.

B. 1.4.1.2 User Authentication and Log-On Process

a) Users should be identified and authenticated with personal accounts; group accounts should only be used in precisely defined exceptional cases.

b) Before allowing any actions the system should require each user to be successfully authenticated.

c) If password-based authentication is used, the system should force passwords with configurable strength and expiration periods. The password strength and expiration period should be configurable by the customer.

d) Where technically feasible, 2-factor authentication should be used for sensitive systems

e) Data used for user identification and authentication should not solely be provided from sources external to the process network. Integration with a central, process-net internal directory service should be considered.

f) Successful and failed log on attempts should be logged centrally.

Where applicable, the following items should be implemented after paramount consideration of safe system operation and availability issues:

- The system should implement mechanisms which allow for a secure and reproducible switching of user sessions during system operations.

- Where applicable and technically feasible, user sessions should be locked after a configurable time of inactivity.

- After a configurable number of failed log-on attempts a security event message should be logged and, where applicable, the account should be locked out

B.1.4.2 Authorization of Activities on User and System Level

Before security-relevant or security-critical activities are performed, the system should check the authorization of the requesting user or system component.

B.1.4.3 Application Protocols

Only standard application-level protocols approved by the client should be used. Exceptions should be approved by the customer and documented. Protocols which protect the integrity of the transferred data and ensure correct authentication and authorization of the communication partners should be preferred. The protocols should provide protection against replay attacks. Where applicable, encryption of the protocol data should be implemented. These requirements also apply to proprietary protocols.
B.1.4.4 Integrity Checks of Relevant Data

The system should check the sanity and integrity of all input data before this data is processed in security-relevant activities (e.g., check for plausibility, correct syntax and value ranges).

B.1.4.5 Logging, Audit Trails, Timestamps, Alarm Concepts

a) All system components should use a uniform system time which can be synchronized with an external time source.

b) The system should log user actions and security-relevant actions, events and errors to an audit trail using a format which is appropriate for later and central analysis. The system should record date, time, involved users and systems, as well as the event and its result for a configurable time period.

c) The logging function should be easy to configure and customize.

d) Security events should be highlighted in the system logs to allow for an easy automatic analysis.

e) The central storage location of the log files should be configurable.

f) A mechanism for automatic transfer of the log files to a central logging component should be available.

g) The log files should be protected against subsequent modification.

h) The system should overwrite the oldest stored audit records if the audit trail is full. The system should issue a warning if the storage capacity decreases below a reasonable threshold.

i) Security-relevant events should be integratable into an existing alarm management.

B.1.4.6 Self-Test and System Behavior

The system or the security modules, respectively, should perform integrity checks of security-relevant settings and data at start-up and in regular intervals. If the security modules or the integrity checks fails, the system should fall back into a system state which maintains the primary system functions as long as the prevention of personal injury or equipment damage can be ensured.

B.1.5 Development, Test and Rollout

B.1.5.1 Secure Development Standards, Quality Management and Release Processes

a) On the contractor side, the system should be developed by trained and trustworthy personnel. Outsourcing of the system development as a whole or in parts to third parties shall require the written approval of the customer. The third party should at least comply with the same security requirements as the original contractor.

b) The system should be developed according to well-known development and software security standards and quality management/assurance processes. Development and testing of the system should be carried out by independent teams. Test plans, test concepts, expected and actual test results should be documented in a comprehensible way and the documentation should be available for inspection by the customer.

c) The contractor should have a documented development security program that covers the physical, procedural and personnel security measures to protect the integrity and confidentiality of the system’s design and implementation. The contractor should be available for an external audit of the effectiveness of the security program.

d) The contractor should have a programming guideline which covers security requirements and secure programming practice. The guideline should deprecate insecure programming style and the use of insecure functions.

e) System release and the release of updates and security patches should be managed and controlled through a well-defined and documented release process.
B.1.5.2 Secure Data Storage and Transmission

Sensitive customer data, which is used or produced during development and maintenance, should be transmitted in encrypted form if it is to be sent over public networks. If the data is stored on mobile devices it should be stored in encrypted form. Sensitive data may include, but is not limited to, internal customer information and documents, log files, error logs, and relevant system documentation. The amount of stored data and the storage time should be limited to the necessary minimum.

B.1.5.3 Secure Development, Test and Staging Systems, Integrity Checks

a) Development should be conducted on secure development systems. The development environment, the source code and binaries should be protected against unauthorized access.

b) Development and testing of the system and of updates, enhancements and security patches should be conducted on staging environments which should be separated from the production system.

c) No source code should be installed on production systems.

d) It should be possible to verify the integrity of the system source code and binaries to detect unauthorized changes.

e) A version history of all deployed software packages should be maintained, which allows all software changes to be traced.

B.1.5.4 Secure Update and Maintenance Processes.

a) Provision and installation of updates, enhancements and patches should be carried out in consultation with the customer according to a pre-defined process.

b) On the contractor side, maintenance should be carried out by dedicated and trained personnel, using secured systems.

B.1.5.5 Configuration and Change Management, Rollback

a) The system should be developed and maintained using a configuration and change management.

b) The system should support rollback of a specified number of configuration changes.

B.1.5.6 Vulnerability Management process

The contractor should have a well-defined vulnerability management process to address security vulnerabilities. The process should allow all involved and external parties to report security vulnerabilities. Furthermore the contractor should obtain up-to-date information about security problems and vulnerabilities which may affect the system or its components. The vulnerability management process should define how a potential vulnerability is verified, classified, fixed, and how recommendations are reported to all system owners. Furthermore the process should define timelines for each step in the vulnerability management process. The contractor should inform the customer about known security vulnerabilities, even if there is no patch available. The customer should treat this information confidentially.

B.1.5.7 Source Code Escrow

If applicable, a source code escrow agreement should be considered in order to ensure security updates in case of failure of the contractor. The agreement should cover the system source code and the associated source code documentation.
B.1.6 Backup, Recovery and Disaster Recovery

B.1.6.1 Backup: Concept, Method, Documentation, Test

There are documented backup and recovery procedures which cover single applications and the entire system, respectively, together with the associated configuration data. The configuration data of distributed systems can be saved in a central repository. The backup and recovery processes should be tested by the client regularly. Documentation and tests should be adjusted after relevant system updates and the procedures should be re-tested. The backup process should provide a verification operation and should take into account the protection requirements of the backup data (e.g. by encrypting sensitive data).

B.1.6.2 Disaster Recovery

For critical systems, the contractor should provide documented operational concepts and tested disaster recovery concepts and procedures for defined emergency and crisis scenarios. The recovery concepts should include a specification of the recovery time objectives. The documentation and procedures shall be adjusted after relevant system updates and the procedures are re-tested during system release acceptance procedures.
References
