TECHNICAL REPORT

ISO/IEC TR 27019

First edition
2013-07-15

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Technologies de l'information — Techniques de sécurité — Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie des opérateurs énergétiques

Reference number
ISO/IEC TR 27019:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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

ISO/IEC TR 27019 was prepared by DIN Deutsches Institut für Normung e. V. (as DIN SPEC 27009:2012-04 [4]) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by the national bodies of ISO and IEC.

Introduction

This Technical Report provides guiding principles based on ISO/IEC 27002 “Code of practice for information security management” for information security management applied to process control systems as used in the energy utility industry. The aim of this document is to extend the ISO/IEC 27000 standards to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

At the focus of application of this document are the systems and networks for controlling and supervising the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes. This includes control and automation systems, protection and safety systems and measurement 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 to further, special requirements. In comparison with conventional IT environments (e.g. office IT) there are fundamental and significant differences with respect to the development, operation, repair, maintenance and operating environment of process control systems. Furthermore, the process technology referred to in this document 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 need to be taken into due consideration by the management processes for process control systems and justify separate consideration within the ISO/IEC 27000 series of standards.

In particular, the following fundamental differences exist compared 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 processed is frequently of crucial importance. Incorrect data can lead to incorrect control inputs, resulting in failure of protection or safety systems or trigger incorrect decisions by operating personnel, as a result of an erroneous representation of current process conditions. These requirements therefore need to be taken into consideration during the system design stage as well as in normal operation.

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 larger 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;

— digital metering and measurement devices.

Often, these remote systems cannot be physically protected at the same level as centrally located systems. Therefore, the system architecture needs to take these differences into consideration and it may be necessary to provide additional safeguards 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 systems in critical substations or at other important sites via remote access, 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 outages it has to 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 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 also not be acceptable due to the availability requirements. Maintenance periods have to be planned and scheduled in advance. 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 (e.g. field control elements) of process control systems are generally designed to support only the intended process data applications and frequently do not have sufficient system resources to support additional security features such as encryption or authentication.

Audience

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

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

1 Scope

The scope of this guideline 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;

— all software, firmware and applications installed on above mentioned systems.

Outside the scope of this guideline is the conventional or classic control equipment that is non-digital, i.e. purely electro-mechanical or electronic monitoring and process control systems. Furthermore, energy process control systems in private households and other, comparable residential building installations are outside the scope of this guideline.

Telecommunication systems and components used in the process control environment are also not directly part of the scope of this guideline. These are covered by the standard “ISO/IEC 27011:2008 *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*”. It is recommended that users of this guideline should implement the measures defined in that standard for the telecommunication systems and components 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).

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the definitions in accordance with ISO/IEC 27001:2005 and ISO/IEC 27002:2005 shall apply, together with the following definitions.

3.1
blackout
widespread electrical power outage

3.2
Computer Emergency Response Team
CERT
team of security experts to support the handling of information security incidents

3.3
critical infrastructure
organizations and facilities that are essential for the functioning of society and the economy as a whole

NOTE 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
debugging
analysing malfunctions in computer systems

3.5
distribution
the transport of electrical energy of high, medium or low voltage over a distribution grid or the transport of gas or heat over local or regional distribution networks

3.6
energy equipment installation
equipment or plant for the generation, conversion, storage, transfer or supply of energy

3.7
energy supply
the process of generation, production or storage of energy for delivery to customers and the operation of an energy supply network

3.8
energy utility
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

3.9
human-machine interface
HMI
user interface for operating and monitoring of a process control systems and/or a plant

3.10
maintenance
all measures used in the field of energy supply that are normally related to inspection, maintenance, fault clearance and improvement

3.11
PLC
programmable logic controller

3.12
process control system
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

3.13
safety
functional safety

3.14
safety systems
systems and components that are required to ensure functional safety

3.15
smart grid
electric grid system, which is characterized by the use of communication networks and the control of grid components and loads

3.16
statement of applicability
SOA
Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS

3.17
transmission system
transmission grid for the transport of electrical energy using a high voltage or ultra-high voltage grid or a gas transmission network for the transport of natural gas using a high pressure pipeline network

4 Overview

4.1 Structure of this guideline

This guideline has been structured in a format compatible with 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 this is 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. 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).

4.2 Information security management systems for energy supply utilities

4.2.1 Objectives

From the viewpoint of design and function, 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 using sensors. The systems then process this data and generate control outputs that regulate actions using actuators. The control and regulation is automatic but manual intervention by operating personnel is also possible. Information and information processing systems are therefore an essential part of operational processes within energy utilities. This means that appropriate protection measures should be applied in the same manner as for other organizational units.

Software and hardware components based on standard IT technology are being utilized increasingly in process control environments.

Nowadays, the information and information processing systems in process control environments are consequently also exposed to an increasing number of threats and vulnerabilities. It is therefore essential that, in the process control domain of 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 process control domain of the energy utility sector can be achieved by establishing, implementing, monitoring, reviewing and if necessary improving the applicable measures set forth in this guideline, in order to attain the specific security and business objectives of the organization. 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 framework 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 energy supply systems.

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

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 7.1.1, Inventory of assets.

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 a risk assessment, threats to the organization's own assets will be identified; vulnerabilities and likelihood of occurrence will be evaluated and potential impact estimated.

b) The requirements which result from legislation and bye-laws, regulations and contracts which have to be fulfilled by an organization, and sociocultural requirements. Particular examples include safeguarding a reliable, effective and secure energy supply as well as the reliable fulfilment 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 were 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 losses that may be incurred due to 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 assessed.

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 guideline provides additional assistance and sector-specific measures for the process control systems used by the energy utility sector, taking into consideration the special requirements in these environments. It is therefore recommended that energy utilities implement the measures set forth in this guideline. If necessary, further measures can be developed to fulfil particular requirements. The selection of security measures depends upon the decisions taken by the organization on the basis of its own 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.

4.2.5 Critical success factors

The contents from ISO/IEC 27002:2005 clause 0.7 apply.

5 Security policy

No additional information specific to the energy utility domain.

6 Organization of information security

6.1 Internal organization

6.1.1 Management commitment to information security

No additional information specific to the energy utility domain.

6.1.2 Information security coordination

No additional information specific to the energy utility domain.

6.1.3 Allocation of information security responsibilities

No additional information specific to the energy utility domain.

6.1.4 Authorization process for information processing facilities

No additional information specific to the energy utility domain.

6.1.5 Confidentiality agreements

No additional information specific to the energy utility domain.

6.1.6 Contact with authorities

Control 6.1.6 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility specific implementation guidance

The applications and infrastructure of energy utility process control systems may be considered as part of critical infrastructures and may be essential for the functioning of the community, society and economy as a whole. Operators of such systems should therefore maintain contact with all of the relevant authorities. In addition to relevant public departments (e.g. fire service, inspectorates, etc.) this may for instance, also include:

— national and international agencies and co-operation initiatives for the protection of critical infrastructures;

— national and international CERT organizations;

— civil protection organizations and disaster-relief teams.

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

Other information for the energy utility domain

During the course of system operation, operational planning and during preparatory work 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 from ISO/IEC 27002:2005 is 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 national and international vendor and operator associations and their corresponding working groups dealing with security issues.

6.1.8 Independent review of information security

No additional information specific to the energy utility domain.

6.2 External parties

6.2.1 Identification of risks related to external parties

Control 6.2.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Process control systems may consist of complex individually customized systems and components. System vendors, integrators and other external parties (e.g. cloud service providers) are often involved in the maintenance and operation processes of these systems to a high degree. For maintenance and fault correction processes these external parties may need to 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 levels may require close interconnection 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 physical process that is to be controlled or monitored.

6.2.2 Addressing security when dealing with customers

Control 6.2.2 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

The complex and diverse relationships between asset owners, system operators, service providers and internal and external customers in the energy utility sector may result in demarcated responsibilities with respect to 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 diverse and/or complex business relationships should 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 11.4.8, Logical coupling of external process control systems, should be taken into consideration.

6.2.3 Addressing security in third-party agreements

Control 6.2.3 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

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

Asset owners should review all contracts that involve third party access to their process control systems. Asset owners should also assess the need for third-party access to their process control systems.

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 the case of major blackouts, natural disasters, incidents or other possible emergency situations, should be defined, contractually specified and monitored. This applies in particular to any necessary pre-emptive measures that may need to be taken to avoid service overload and to ensuring an acceptable degree of independence of the telecommunication services of external energy supply (blackout resistance).

7 Asset management

7.1 Responsibility for assets

7.1.1 Inventory of assets

Control 7.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

When developing and maintaining the inventory of all of the organization's important assets, distinct responsibilities should be clearly specified and documented.

The inventory of assets should cover all of the relevant process control systems and include information assets and applications.

Further information for energy utilities

Supplementary to the above classifications, assets in the energy supply domain also include a wide range of other sector-specific asset categories such as:

a) **information**: grid and network plans, scheduling and dispatching data, geographical and geo-referenced information, crisis and emergency plans, grid disaster recovery plans, switching operation data, measured values and measurement data, meter and metered 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 telecontrol components, remote terminal units, data transmission system components, digital protection and safety components, digital metering and measuring devices, smart meters, 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, meteorological services, etc.

7.1.2 Ownership of assets

Control 7.1.2 from ISO/IEC 27002:2005 is augmented as follows:

Further information for energy utilities

The potentially complex structure of organizations that employ process control systems may mean that highly diverse responsibilities with regard to commercial and operational ownership exist. 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

No additional information specific to the energy utility domain.

7.2 Information classification

7.2.1 Classification guidelines

Control 7.2.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

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

- assets, systems and information supporting the operation of critical infrastructures and sensitive systems;
- 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;
- assets, systems and information necessary to ensure functional safety/plant and equipment security;
- assets, systems and information necessary to fulfil regulatory requirements such as unbundling requirements for instance, or that need to be implemented in order to fulfil other specific requirements.

7.2.2 Information labelling and handling

No additional information specific to the energy utility domain.

8 Human resource security

8.1 Prior to employment[1)]

8.1.1 Roles and responsibilities

Control 8.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Staff employed in the energy utility sector to be responsible for process control systems technology should have the appropriate knowledge and skills for managing and supervising the installation, maintenance and secure 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 aspects of these systems.

8.1.2 Screening

Control 8.1.2 from ISO/IEC 27002:2005 is 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 carefully 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 prospective personnel are permitted to work on components that form part of the critical infrastructure, a specific security clearance provided by governmental organizations may be required, depending upon the appropriate (local) legislation.

8.1.3 Terms and conditions of employment

Control 8.1.3 from ISO/IEC 27002:2005 is 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 be considered for key personal responsible for the operation of critical infrastructures and sensitive systems, taking into consideration the applicable legal requirements. 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

No additional information specific to the energy utility domain.

1) Explanation: The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

It should be noted that the controls in this section apply to independent contractors as well as people covered using other employment arrangements.

8.3 Termination or change of employment

No additional information specific to the energy utility domain.

9 Physical and environmental security

9.1 Secure areas

9.1.1 Physical security perimeter

Control 9.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Especially in energy transmission and distribution systems and in the area of distributed generation, components are distributed across decentralized sites. Equipment is situated in control and technical rooms within the organization's building and in peripheral sites. Sometimes 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 peripheral, potentially unoccupied sites; therefore the residual risk should be evaluated and mitigated where necessary by means of supplementary measures and compensating controls.

9.1.2 Physical entry controls

Control 9.1.2 from ISO/IEC 27002:2005 is 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 9.1.9, Securing peripheral sites.

9.1.3 Securing offices, rooms and facilities

No additional information specific to the energy utility domain.

9.1.4 Protecting against external and environmental threats

No additional information specific to the energy utility domain.

9.1.5 Working in secure areas

No additional information specific to the energy utility domain.

9.1.6 Public access, delivery and loading areas

No additional information specific to the energy utility domain.

9.1.7 Securing control centers

A control additional to ISO/IEC 27002:2005, clause 9.1, Secure areas is:

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 should be selected for control centers where the environmental damage from wind and water, etc. can be least expected; if a site is chosen that is vulnerable to such environmental threats, appropriate measures should be taken in order to prevent such damage from occurring.

c) A site should be selected for control centers where the potential damage due to strong electromagnetic fields is negligible; if a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect control system equipment rooms using electromagnetic shielding.

d) Control centers should not be located at sites directly adjacent to facilities used for storing dangerous materials that pose the threat 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 should be designed with adequate structural stability to meet all necessary floor loading requirements.

h) Automatic fire alarm systems should be installed in control centers.

Further information for energy utilities

Process control system assets will sometimes be housed in an externally operated data centre along with other information and telecommunication (ICT) assets. Physical segregation between control systems and other ICT systems and strict “segregation of duties” is important when external operators operate the control systems; in many cases this will be in a facility distant from a data centre under the control of an energy utility.

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 endangered by external influences such as extreme environmental conditions or natural disasters.

b) The control system equipment room should be located where access by unauthorized personnel is restricted; adequate measures should be taken to prevent or detect possible unauthorized intrusion.

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 or other ingress of water. Should the room not fulfil this requirement, then the necessary measures should be taken to prevent this, such as raising the floor level, watertight design of the building or 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 fulfil 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 malfunctions caused by static charges.

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

k) Measures should be taken to protect the control system equipment rooms from electromagnetic interference if they are used as data storage rooms and / or for data backup, where necessary.

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 to 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 equipment used by energy utilities is 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 should 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 these peripheral sites as well as redundancy and fallback concepts implemented for their corresponding system functionality should be given primary consideration.

Implementation guidance

Especially in energy transmission and distribution networks, and in distributed generation systems, components of the control system infrastructure may be distributed across peripheral sites that are frequently unoccupied. In order to protect such decentralized sites where control system facilities are located (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 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, where necessary.

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

d) Adequate, physically secure perimeters should be installed using, for example, secure fencing and an automatic alarm system should be installed and monitored from a central location, where necessary.

9.2 Equipment security

9.2.1 Equipment siting and protection

Control 9.2.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Under certain circumstances, system components of process control systems and supporting infrastructure may have to be installed in areas with extensive exposure to dust, heat, cold, electromagnetic radiation, humidity, etc. The equipment should be suitably designed and constructed to operate in such environmental conditions; otherwise additional protective countermeasures, e.g. suitable external housing cabinets should be implemented to ensure reliable operation.

9.2.2 Supporting utilities

Control 9.2.2 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

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

Further information for energy utilities

Depending upon plans for system restoration, critical components essential for system restoration should be capable of being operated independently of an external power supply for 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 includes for example an automatic emergency power generator as well as the corresponding stockpile of fuel.

9.2.3 Cabling security

Control 9.2.3 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Especially in the sphere of energy transmission and distribution grids, communication networks are installed over wide areas 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 as for in-house cables. The associated risks should be evaluated 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 considered.

9.2.4 Equipment maintenance

No additional information specific to the energy utility domain.

9.2.5 Security of equipment off-premises

No additional information specific to the energy utility domain.

9.2.6 Secure disposal or reuse of equipment

No additional information specific to the energy utility domain.

9.2.7 Removal of property

No additional information specific to the energy utility domain.

9.3 Security in premises of 3rd parties

A control objective additional to ISO/IEC 27002:2005, clause 9, Physical and environmental security, is:

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 sites or premises in areas that are the responsibility of other utilities, such as interconnection stations for instance, 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 range of responsibility and interfaces with other energy utility organizations should be specified and it should be possible to isolate the equipment easily from that of the other organization, where necessary. (See also 9.3.3, Interconnected control and communication systems).

b) Agreements should be concluded contractually 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 equipment is to be installed fulfils all 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 terms and conditions 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 range of responsibility and the interfaces with the customer should be specified and it should be possible to isolate the equipment easily from that of the customer, where necessary.

c) It should be possible to 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 lines are interconnected with those of external third parties, the range of responsibility and interfaces with the customer should be clearly defined such that it is possible to disconnect and isolate each organization from the others within an appropriate period of time in order to avoid known risks.

Implementation guidance

Energy utility organizations should monitor the status of their interconnections.

In order to diagnose problem areas and take corrective actions, organizations should have a means for isolating the connections between themselves and external third parties and for reconnecting isolated connections, where necessary.

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 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

In the operating processes documentation it should be specified exactly under which conditions incident, emergency or crisis handling procedures are to be invoked (see clause 13.2, Management of information security incidents and improvements).

10.1.2 Change management

No additional information specific to the energy utility domain.

10.1.3 Segregation of duties

No additional information specific to the energy utility domain.

10.1.4 Separation of development, test and operational facilities

Control 10.1.4 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

In the process control domain of 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 purposes. 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, these 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, customized change management, incident, emergency and crisis handling procedures should be established that allow a rapid and appropriate reaction to disruptions and problems in the operational system, compatible with the criticality of the system in question.

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

No additional information specific to the energy utility domain.

10.3 System planning and acceptance

No additional information specific to the energy utility domain.

10.4 Protection against malicious and mobile code

10.4.1 Controls against malicious code

Control 10.4.1 from ISO/IEC 27002:2005 is 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 vendor approval or the impossibility of installing timely updates), the resulting risks should be identified and other types of countermeasures should be implemented that provide at least 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;

— deployment 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 against mobile code

Control 10.4.2 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Smart grid technology 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 software 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 Back-up

No additional information specific to the energy utility domain.

10.6 Network security management

10.6.1 Network controls

No additional information specific to the energy utility domain.

10.6.2 Security of network services

No additional information specific to the energy utility domain.

10.6.3 Securing process control data communication

A control additional to ISO/IEC 27002:2005, clause 10.6, Network security management, is:

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 sector-specific or generic technical standards and protocols exists, such as:

— IEC 60870-5;

— IEC 60870-6 (TASE.2);

— DNP3;

— IEC 61850;

— IEC 61400-25;

— 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 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

No additional information specific to the energy utility domain.

10.8 Exchange of information

No additional information specific to the energy utility domain.

10.9 Electronic commerce services

No additional information specific to the energy utility domain.

10.10 Monitoring

10.10.1 Audit logging

Control 10.10.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

In the energy utility sector, relevant audit logs may also include certain actions carried out by operating personnel, such as switching operations for instance. Audit logs and obligations to preserve such records may be stipulated in industry-specific legislation and by regulatory bodies for a wide range of electronic documents.

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

No additional information specific to the energy utility domain.

10.10.3 Protection of log information

No additional information specific to the energy utility domain.

10.10.4 Administrator and operator logs

No additional information specific to the energy utility domain.

10.10.5 Fault logging

No additional information specific to the energy utility domain.

10.10.6 Clock synchronization

Control 10.10.6 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

For all systems that are directly or indirectly interconnected with external partners, a common and agreed time 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 prevent the manipulation of NTP signals.

10.11 Legacy systems

A control objective additional to ISO/IEC 27002:2005, clause 10, Communications and operations management, is:

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 (hereinafter referred to as 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 such legacy 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 risks resulting from continued use of legacy systems and technologies 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 securely.

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

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

10.12 Safety functions

A control objective additional to ISO/IEC 27002:2005, clause 10, Communications and operations management, is:

Objective: To ensure the integrity and availability of safety functions.

10.12.1 Integrity and availability of safety functions

Control

The integrity and availability of information assets, systems, components and functions that are required to ensure safety functions should be protected 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) Using dedicated, isolated communication systems for the transmission of safety-related data communications.

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

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

d) 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 from ISO/IEC 27002:2005 is 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

No additional information specific to the energy utility domain.

11.3 User responsibilities

11.3.1 Password use

Control 11.3.1 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

In the process control domain 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 where 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

No additional information specific to the energy utility domain.

11.3.3 Clear desk and clear screen policy

No additional information specific to the energy utility domain.

11.4 Network access control

11.4.1 Policy on use of network services

No additional information specific to the energy utility domain.

11.4.2 User authentication for external connections

No additional information specific to the energy utility domain.

11.4.3 Equipment identification in networks

No additional information specific to the energy utility domain.

11.4.4 Remote diagnostic and configuration port protection

No additional information specific to the energy utility domain.

11.4.5 Segregation in networks

Control 11.4.5 from ISO/IEC 27002:2005 is 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 [5]. 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 be routed exclusively via especially hardened application proxies, which are located in a separate network zone (i.e. demilitarized zone), designed 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

No additional information specific to the energy utility domain.

11.4.7 Network routing control

No additional information specific to the energy utility domain.

11.4.8 Logical coupling of external process control systems

A control additional to ISO/IEC 27002:2005, clause 11.4, Network access control, is:

Control

Before process control systems and related communication links with external parties are connected logically, 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 evaluated.

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 securely.

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

No additional information specific to the energy utility domain.

11.5.2 User identification and authentication

Control 11.5.2 from ISO/IEC 27002:2005 is 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 controllers / PLCs or for maintenance processes in distributed systems. The resulting risk should be considered and appropriate risk-mitigating countermeasures implemented.

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

11.5.3 Password management system

No additional information specific to the energy utility domain.

11.5.4 Use of system utilities

No additional information specific to the energy utility domain.

11.5.5 Session time-out

Control 11.5.5 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

The activation of session time-outs and screensavers is not appropriate in certain process control applications, for example in HMIs and visualization applications 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

No additional information specific to the energy utility domain.

11.6 Application and information access control

No additional information specific to the energy utility domain.

11.7 Mobile computing and teleworking

No additional information specific to the energy utility domain.

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 from ISO/IEC 27002:2005 is augmented as follows:

Further information for energy utilities

To support the acquisition of process control systems, the BDEW Whitepaper “Requirements for Secure Control and Telecommunication Systems” [1] exemplifies essential control system specific security measures, which can be used during system procurement. A mapping of the controls of this document and the requirements of the BDEW Whitepaper [1] is included in Annex B.

12.2 Correct processing in applications

No additional information specific to the energy utility domain.

12.3 Cryptographic controls

No additional information specific to the energy utility domain.

12.4 Security of system files

12.4.1 Control of operational software

Control 12.4.1 from ISO/IEC 27002:2005 is 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 (e.g. operating system software, firmware) are to be implemented on sensitive systems, comprehensive tests should be carried out beforehand 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, Separation of development, test and operational facilities).

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

No additional information specific to the energy utility domain.

12.4.3 Access control to program source code

No additional information specific to the energy utility domain.

12.5 Security in development and support processes

No additional information specific to the energy utility domain.

12.6 Technical vulnerability management

No additional information specific to the energy utility domain.

13 Information security incident management

13.1 Reporting information security events and weaknesses

No additional information specific to the energy utility domain.

13.2 Management of information security incidents and improvements

No additional information specific to the energy utility domain.

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 from ISO/IEC 27002:2005 is 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

No additional information specific to the energy utility domain.

14.1.3 Developing and implementing continuity plans including information security

No additional information specific to the energy utility domain.

14.1.4 Business continuity planning framework

No additional information specific to the energy utility domain.

14.1.5 Testing, maintaining and re-assessing business continuity plans

No additional information specific to the energy utility domain.

14.2 Essential emergency services

A control objective additional to ISO/IEC 27002:2005, clause 10, Business continuity management, is:

Objective: To ensure the availability of essential emergency services in the case of major disturbances, natural disasters, accidents or other extensive 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 peripheral locations;

— internal and external crisis management;

— power stations;

— distributed energy producers;

— transmission and distribution system operators;

— meteorological organizations;

— flood prevention organizations;

— fire service organizations;

— disaster-relief organizations;

— security 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 should be recognized 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 from ISO/IEC 27002:2005 is augmented as follows:

Energy utility-specific implementation guidance

Requirements specific to the energy utility sector may include:

— 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 with manageable modification effort.

15.1.2 Intellectual property rights (IPR)

No additional information specific to the energy utility domain.

15.1.3 Protection of organizational records

No additional information specific to the energy utility domain.

15.1.4 Data protection and privacy of personal information

No additional information specific to the energy utility domain.

15.1.5 Prevention of misuse of information processing facilities

No additional information specific to the energy utility domain.

15.1.6 Regulation of cryptographic controls

No additional information specific to the energy utility domain.

15.2 Compliance with security policies and standards, and technical compliance

No additional information specific to the energy utility domain.

15.3 Information systems audit considerations

No additional information specific to the energy utility domain.