INTERNATIONAL STANDARD

ISO/IEC 27019

First edition
2017-10

Information technology — Security techniques — Information security controls for the energy utility industry

Technologies de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Reference number
ISO/IEC 27019:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC/TR 27019:2013) which has been technically revised.

The main changes compared to the previous edition are as follows:

— the scope has changed to include the energy oil sector;

— this document has been changed from a Technical Report to an International Standard;

— the previous edition was aligned with ISO/IEC 27002:2005. The new structure has been aligned with ISO/IEC 27002:2013;

— the title has been changed.

— where appropriate the technical content has been revised and updated to reflect current technological developments in the energy sector.

0 Introduction

0.1 Background and context

This document provides guiding principles based on ISO/IEC 27002:2013 "Code of practice for information security controls" 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 contents of ISO/IEC 27002:2013 to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized and specific information security management system (ISMS) that is in accordance with ISO/IEC 27001:2013 and extends from the business to the process control level.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2013, the process control systems used by energy utilities and energy suppliers are subject to further special requirements. In comparison with conventional ICT environments (e.g. office IT, energy trading systems), 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 can represent integral components of critical infrastructures. This 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 family of standards.

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 processes 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 it is important that appropriate protection measures be applied in the same manner as for other organizational units.

Software and hardware (e.g. programmable logic) components based on standard ICT technology are increasingly utilized in process control environments and are also covered in this document. Furthermore, process control systems in the energy utility sector are increasingly interconnected to form complex systems. Risks arising from this trend need to be considered in a risk assessment.

The information and information processing systems in process control environments are 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 27001:2013.

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 document, in order to attain the specific security and business objectives of the organization. It is important to give particular consideration here to the special role of the energy utilities in society and to the economic necessity of a secure and reliable energy supply. Ultimately, the overall success of the cybersecurity of energy industries is based on collaborative efforts by all stakeholders (vendors, suppliers, customers, etc.).

0.2 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 safe, reliable and secure operation of energy supply systems.

c) Energy providers require information security in order to safeguard their business interests, meet customers' needs and comply with the legal regulations.

0.3 Information 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, risk sources and events are identified; potential consequences and likelihood of the occurrence of the risks are assessed.

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 external parties.

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

NOTE It is important that the energy utility organization ensure that security requirements of process control systems are analysed and adequately covered in policies for information security. The analysis of the information security requirements and objectives include the consideration of all relevant criteria for a secure energy supply and delivery, e.g.

— Impairment of the security of energy supply;

— Restriction of energy flow;

— Affected share of population;

— Danger of physical injury;

— Effects on other critical infrastructures;

— Effects on information privacy;

— Financial impacts.

The necessary security measures or controls are determined by the methodical assessment of security risks. It is necessary that the cost of controls be balanced against the economic losses that can 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; and

— 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 can affect the results assessed.

Requirements for the risk assessment and control selection are given in ISO/IEC 27001:2013.

0.4 Selecting controls

Once the security requirements and risks have been identified and decisions taken on how to deal with the risks, appropriate controls are then 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 security management system, this document 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. 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.

0.5 Audience

This document 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 ISO/IEC 27002:2013 and defines specific measures for process control systems of the energy utility industry, their supporting systems and the associated infrastructure.

Information technology — Security techniques — Information security controls for the energy utility industry

1 Scope

This document provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. This includes in particular the following:

— central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices;

— digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements;

— all further supporting information systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes;

— communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;

— Advanced Metering Infrastructure (AMI) components, e.g. smart meters;

— measurement devices, e.g. for emission values;

— digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms;

— energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations;

— distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations;

— all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System);

— any premises housing the above-mentioned equipment and systems;

— remote maintenance systems for above-mentioned systems.

This document does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 62645.

This document also includes a requirement to adapt the risk assessment and treatment processes described in ISO/IEC 27001:2013 to the energy utility industry-sector–specific guidance provided in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
blackout
widespread electrical power outage

3.2
Computer Security Incident Response Team
CSIRT
team of security experts to support the handling of information security incidents

3.3
critical asset
asset which can have a direct impact on production or generation, transmission, storage and distribution of electric power, gas, oil and heat

3.4
critical infrastructure
set of organizations and facilities that are essential for the functioning of society and the economy as a whole

Note 1 to entry: A failure or malfunction of such organizations and facilities can result in sustained supply shortfalls, make a significant impact on public security and have other wide ranging impacts.

3.5
debugging
action of analysing malfunctions in computer systems

3.6
distribution system
distribution grid for the transport of electrical energy using a high, medium or low voltage grid, or a local or regional distribution network for the transport of gas, oil or heat

3.7
energy management system
EMS
equipment/infrastructure used to monitor, measure and control the energy consumption in private households, residential buildings or industrial customer installations

Note 1 to entry: The term EMS is also commonly used to refer to a set of applications used by operators of transmission power grid to monitor, control, and optimize the performance of the generation and/or transmission system.

3.8
energy supply
process of generation, production or storage of energy for delivery to customers and the operation of an energy supply network

3.9
energy utility
legal body or a person that supplies energy in form of electricity, gas, oil or heat to other parties, to an energy distribution network or to a storage complex

3.10
human–machine interface
HMI
user interface for operating and monitoring of a process control system or a plant

3.11
maintenance
measures used in the field of *energy supply* (3.8) that are normally related to inspection, fault clearance and improvement

3.12
process control system
system that serves to control and monitor the generation, production, transmission, storage and distribution of electric power, gas, oil and heat, including the control of associated supporting processes.

Note 1 to entry: Process control systems are often referred to more generally as industrial control systems. In this document, the terms process control system and industrial control system are restricted to technologies and components used in the energy utility industry.

3.13
safety
freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.14
safety system
system and component that are required to ensure *safety* (3.13)

3.15
Supervisory Control And Data Acquisition
SCADA
process control system (3.12) generally used to control dispersed assets using centralized data acquisition and supervisory controls

3.16
smart grid
electric power system that utilizes information exchange and control technologies, distributed computing and associated sensors and actuators

Note 1 to entry: Smart grid technologies are used for purposes such as:

— integrating the behaviour and actions of the network users and other stakeholders;

— efficiently delivering sustainable, economic and secure electricity supplies.

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 Structure of the document

4.1 General

This document is a sector-specific standard related to ISO/IEC 27002:2013. The energy utility-sector–specific reference control objectives and controls are listed in Annex A.

4.2 Refinement of ISO/IEC 27001:2013 requirements

ISO/IEC 27001:2013, 6.1.3 c) is refined as follows:

Compare the controls determined in 6.1.3 b) above with those in ISO/IEC 27001:2013, Annex A and with Annex A of this document to verify that no necessary controls have been omitted.

ISO/IEC 27001:2013, 6.1.3 d) is refined as follows:

Produce a Statement of Applicability that contains:

— the necessary controls [see ISO/IEC 27001:2013, 6.1.3 b) and c)];

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— justification for excluding any of the controls in ISO/IEC 27001:2013, Annex A or Annex A of this document.

NOTE These refinements are necessary due to the introduction of new energy-sector–specific controls in this document.

All the other requirements in ISO/IEC 27001:2013, Clauses 4 to 10 apply unchanged. There are no additional requirements specific to the energy utility industry.

4.3 Energy utility industry specific guidance related to ISO/IEC 27002:2013

All clauses, control objectives, controls, implementation guidance and other information specific to the energy utility sector and those from ISO/IEC 27002:2013 that apply unchanged are listed in Clauses 5 to 18.

NOTE Titles of clauses, subclauses and controls which are not contained in ISO/IEC 27002:2013 are prefixed with ENR.

5 Information security policies

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, Clause 5.

6 Organization of information security

6.1 Internal organization

6.1.1 Information security roles and responsibilities

Additional implementation guidance for ISO/IEC 27002:2013, 6.1.1:

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

6.1.2 Segregation of duties

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 6.1.2.

6.1.3 Contact with authorities

Additional implementation guidance for ISO/IEC 27002:2013, 6.1.3:

The applications and infrastructure of energy utility process control systems can be part of critical infrastructures and can 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 can also include, for instance:

— national and international agencies and cooperation initiatives for the protection of critical infrastructures;

— national and international CSIRT organizations;

— civil protection organizations and disaster-relief teams;

— emergency response organizations and personnel.

For operators of critical infrastructure components, additional laws, local bye-laws and regulations regarding contact with authorities can apply. Energy utilities should ensure that the information received through contacts with authorities is analysed and evaluated in the context of the organization by subject matter experts and distributed to responsible parties within the organization in a timely manner.

Additional other information for ISO/IEC 27002:2013, 6.1.3:

During system operation, operational planning and preparatory work for exceptional situations, weather information can 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).

6.1.4 Contact with special interest groups

Additional implementation guidance for ISO/IEC 27002:2013, 6.1.4:

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. The process of information exchange should take into account the applicable legal context.

Energy utilities should ensure that the information received through contacts with special interest groups is analysed and evaluated in the context of the organization by subject matter experts and distributed to responsible parties within the organization in a timely manner.

6.1.5 Information security in project management

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 6.1.5.

6.1.6 ENR – Identification of risks related to external parties

Additional control for ISO/IEC 27002:2013, 6.1:

Control

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

Implementation guidance

Process control systems can consist of complex individually customized systems and components. System vendors, integrators and other external parties are often involved in the maintenance and operation processes of these systems to a high degree. For maintenance and fault correction processes, it is possible that these external parties need to use remote access connections that allow maintenance to be carried out from remote locations. It is also possible that employees of external parties also need access to security-controlled areas to perform on-site maintenance.

Close cooperation between the different system operators on the production, generation, transmission and distribution levels can require close interconnection of the control systems and communication networks of different organizations. Furthermore, external parties such as vendors, system integrators or business partners can also require access to information related to critical assets.

The risks resulting from such external party access to critical assets and related 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. If external parties have access to critical assets or confidential information, it should be ensured, e.g. through contractual agreements, that they have implemented a comparable security level as defined for the internal organization of the energy utility.

6.1.7 ENR – Addressing security when dealing with customers

Additional control for ISO/IEC 27002:2013, 6.1:

Control

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

Implementation guidance

The complex and diverse relationships between asset owners, system operators, service providers and internal and external customers in the energy utility sector can 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;

— an internal or external customer which is connected to the energy supply infrastructure and the related process control systems and communication 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 or assets. When equipment is sited on premises of other energy utilities or customers, or if process control systems are interconnected, the measures described in 11.3.1, 11.3.2, 11.3.3 and 13.1.5 should be taken into consideration.

6.2 Mobile devices and teleworking

6.2.1 Mobile device policy

Additional implementation guidance for ISO/IEC 27002:2013, 6.2.1:

If mobile devices are used on process control networks, energy utilities should include the following in their mobile device security policies:

a) define and assign roles allowed to perform tasks that require access to process control systems via a mobile device;

b) identify the actions that these devices are allowed to perform, the times during which those actions are allowed and explicitly state emergency exceptions;

c) specify what changes may be made to the device, who is allowed to make those changes, and how those changes may be made.

d) specify locations and communications networks which these devices are allowed to use for access, e.g. home, office, remote office, or service vehicles.

e) define any processes required for managing security mechanisms such as key management, access control, configuration management, and identify management.

f) state how each device may be connected to the process control network, e.g. through a gateway, DMZ, VPN tunnelling;

g) separate the use in process control and other networks (e.g. business networks);

h) specify types of data that may be transferred and explicitly disallow all other types of data transfers.

6.2.2 Teleworking

Additional implementation guidance for ISO/IEC 27002:2013, 6.2.2:

Remote access to process control systems performed by the energy utility organization's personnel, by vendors or other external parties should be subject to multiple security measures including:

a) multi-factor authentication;

b) adoption of techniques that prohibit anything other than an indirect connection to the target system or network;

c) minimizing the functions the remote party can execute, e.g. remote control, remote configuration and programming of process control systems;

d) verification of the security status of the remote access system (e.g. up-to-date patch level and anti-malware status, absence of known blacklisted programmes) and protection against the transmission of malware from the remote access system (see 12.2.1);

e) enforcing a list of allowed access locations and/or systems;

f) ensuring that remote access is monitored and supervised and that changes and modifications to critical assets are traceable;

g) ensuring that only known and approved tools should be used for remote access and remote maintenance.

7 Human resource security

7.1 Prior to employment

7.1.1 Screening

Additional implementation guidance for ISO/IEC 27002:2013, 7.1.1:

A strict screening process for key personnel that have access to critical assets or that are responsible for the operation and maintenance processes of critical assets should be carefully considered and implemented if needed. This is especially the case if the assets 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 can be required, depending upon the appropriate (local) legislation.

7.1.2 Terms and conditions of employment

Additional implementation guidance for ISO/IEC 27002:2013, 7.1.2:

The energy utility should ensure through appropriate terms or conditions of employment that key skills and personnel are always available for the operation of critical infrastructures. The authorization to exceed the maximum working time in emergency situations should be considered for key personnel responsible for the operation of critical infrastructures and systems, taking into consideration the applicable legal requirements. Agreements on the monitoring and recording of specific actions, such as control operations or programming and parameterization access, should also be taken into consideration when formulating the contract of employment.

7.2 During employment

7.2.1 Management responsibilities

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 7.2.1.

7.2.2 Information security awareness, education and training

Additional implementation guidance for ISO/IEC 27002:2013, 7.2.2:

Staff employed in the energy utility sector 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.

7.2.3 Disciplinary process

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 7.2.3.

7.3 Termination and change of employment

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 7.3.

8 Asset management

8.1 Responsibility for assets

8.1.1 Inventory of assets

Additional implementation guidance for ISO/IEC 27002:2013, 8.1.1:

The inventory of assets should include all business processes and process control systems relevant to energy supply, such as information, applications and other assets supporting them.

Additional information for ISO/IEC 27002:2013, 8.1.1:

Assets in the energy supply domain include a wide range of 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, application programming and parameterization data, measurement and message archives, historical and trend data, etc.;

NOTE This also includes application programming and parametrization data of digital controllers and automation components.

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, reporting and historian 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, media and news services, time services, etc.

8.1.2 Ownership of assets

Additional implementation guidance for ISO/IEC 27002:2013, 8.1.2:

The potentially complex structure of organizations that employ process control systems means that highly diverse responsibilities with regard to commercial and operational ownership can 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 defined and documented.

8.1.3 Acceptable use of assets

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 8.1.3.

8.1.4 Return of assets

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 8.1.4.

8.2 Information classification

8.2.1 Classification of information

Additional implementation guidance for ISO/IEC 27002:2013, 8.2.1:

Energy-utility–specific classification criteria should be extended as necessary to include the followings:

— assets, systems and information supporting the operation of critical infrastructures and critical assets;

— 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 occupational health and safety, as well as plant and equipment safety;

— assets, systems and information necessary to fulfil regulatory requirements such as unbundling requirements or other specific requirements;

— information considered as confidential or private by external parties, e.g. customers or regulators.

8.2.2 Labelling of information

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 8.2.2.

8.2.3 Handling of assets

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 8.2.3.

8.3 Media handling

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 8.3.

9 Access control

9.1 Business requirements of access control

9.1.1 Access control policy

Additional implementation guidance for ISO/IEC 27002:2013, 9.1.1:

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 security and traceability, precise rules regarding exceptions should be defined, together with supplementary measures.

b) Conditions and regulations that applies 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 security, supplementary measures should be defined in particular.

c) The need for staff and external emergency services personnel to be able to override security controls in declared emergency situations.

d) Access to services or applications by systems that lack adequate authentication (i.e. in the context of machine-to-machine communication). In order to ensure a sufficient level of security, network access control or other means should be considered.

Additional other information for ISO/IEC 27002:2013, 9.1.1:

IEC/TS 62351-8 gives further advice on implementing access control of users and automated agents to data objects in power systems by means of role-based access control.

9.1.2 Access to networks and network services

Additional implementation guidance for ISO/IEC 27002:2013, 9.1.2:

To protect network equipment allowing access to critical networks, the following should be considered:

a) Ensuring physical access protection of network equipment, especially in remote locations;

b) Removing or disabling, through software or physical disconnection of all services and ports in the network equipment not required for normal operation (e.g. non used switch ports), emergency operation or maintenance including both communication ports and physical input/output ports.

9.2 User access management

9.2.1 User registration and de-registration

Additional implementation guidance for ISO/IEC 27002:2013, 9.2.1:

The use of unique user identifiers is not always 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 logging requirements (see 12.4.1)

9.2.2 User access provisioning

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.2.2.

9.2.3 Management of privileged access rights

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.2.3.

9.2.4 Management of secret authentication information of users

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.2.4.

9.2.5 Review of user access rights

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.2.5.

9.2.6 Removal or adjustment of access rights

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.2.6.

9.3 User responsibilities

9.3.1 Use of secret authentication information

Additional implementation guidance for ISO/IEC 27002:2013, 9.3.1:

In the process control domain it is not always possible to ensure the use of secure secret authentication information, 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 and production units, to central directory services, which means that local accounts need to be used. This makes it practically impossible to change secret authentication information for these accounts regularly.

It should therefore be clearly indicated to the user when the general secret authentication information policy applies and when exceptions are allowed, e.g. different passwords are to be used or where it is not possible to use any passwords at all (legacy systems).

Especially in situations where shared secret authentication information is used for system access, the following should be considered:

— the shared secret authentication information should be as secure as possible;

— it should be changed more frequently than individual secret authentication information;

— it should be changed in case of personnel changes.

In particular, the standard passwords used by the system vendors should be considered as insecure and should therefore be changed. Secret authentication information should only be accessible to persons who are involved in the operation of the system.

9.4 System and application access control

9.4.1 Information access restriction

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.4.1.

9.4.2 Secure log-on procedures

Additional implementation guidance for ISO/IEC 27002:2013, 9.4.2:

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 centres. For such applications the resulting risks of unattended sessions should be taken into consideration and corresponding supplementary countermeasures implemented.

9.4.3 Password management system

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.4.3.

9.4.4 Use of privileged utility programs

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 9.4.4.

9.4.5 Access control to program source code

Additional implementation guidance for ISO/IEC 27002:2013, 9.4.5:

Source code, in the energy utility sector, also includes application programming and parametrization data of digital controllers and automation components.

10 Cryptography

10.1 Cryptography controls

10.1.1 Policy on the use of cryptographic controls

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 10.1.1.

10.1.2 Key management

Additional other information for ISO/IEC 27002:2013, 10.1.2:

IEC 62351-9 specifies how to generate, distribute, revoke, and handle digital certificates and cryptographic keys for power systems communications. It can be used for other energy domains.

11 Physical and environmental security

11.1 Secure areas

11.1.1 Physical security perimeter

Additional implementation guidance for ISO/IEC 27002:2013, 11.1.1:

Especially in energy transmission and distribution systems and in the area of distributed generation and production, components are distributed across decentralized sites. Equipment is situated in control and technical rooms within the organization's building and in peripheral, potentially unoccupied, sites. Sometimes equipment is situated on external party premises or in public environments. It is not normally possible to achieve a comprehensive level of physical protection for the peripheral sites; therefore the risk should be evaluated and mitigated where necessary by means of supplementary measures and compensating controls.

11.1.2 Physical entry controls

Additional implementation guidance for ISO/IEC 27002:2013, 11.1.2:

The use of physical access control systems should also be considered for peripheral sites where critical assets are located. See 11.1.9.

11.1.3 Securing offices, rooms and facilities

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.1.3.

11.1.4 Protecting against external and environmental threats

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.1.4.

11.1.5 Working in secure areas

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.1.5.

11.1.6 Delivery and loading areas

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.1.6.

11.1.7 ENR – Securing control centres

Additional control for ISO/IEC 27002:2013, 11.1:

Control

Measures to ensure the physical security of control centres, e.g. where control system 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 centres or the control rooms of centralized or distributed power plants, generation or production units (hereinafter referred to as control centres), the following points should be taken into consideration:

a) A site located on solid ground should be selected for constructing the control centre; 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 centres where the environmental damage from wind and water, etc., are least expected; if an existing site 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 centres where the potential damage due to strong electromagnetic fields is negligible; if an existing site is exposed to strong electromagnetic fields, appropriate measures should be taken to protect control system equipment rooms using electromagnetic shielding.

d) Control centres 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 centre is located in an area susceptible to natural disasters such as earthquake, tsunami, volcano eruption and tornado, control centre buildings should be of disaster-proof construction.

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

g) Control centre buildings should be designed with adequate structural stability to meet all necessary floor loading requirements; for existing sites appropriate measures should be taken to ensure adequate structural stability to meet all necessary floor loading requirements.

h) Automatic fire alarm systems including appropriate early detection and fire extinguishing systems should be installed in control centres.

Other information for energy utilities

Process control system assets are sometimes 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" are important when external operators operate either the ICT or the control systems. In many cases, this is in a facility distant from a data centre under the control of an energy utility.

11.1.8 ENR – Securing equipment rooms

Additional control for ISO/IEC 27002:2013, 11.1:

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; for existing equipment rooms, appropriate measures should be taken to protect it against dangerous external influences.

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

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. If the room does 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. If the room does 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. Protection measures against electromagnetic interference should be also applied if the control system equipment room is used as data storage room and/or for data backup.

f) Components with increased security requirements should be placed in a dedicated control system equipment room with heightened physical protection.

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

h) Fire-proofing measures should be implemented for control system equipment and data storage rooms.

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

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

m) Control system equipment rooms should be air-conditioned when required. The availability of air conditioning should be ensured, e.g. by protecting it against loss of electric power.

NOTE If a control system equipment room is located at a peripheral site, not all of the implementation guidance is fully applicable (see 11.1.9).

11.1.9 ENR – Securing peripheral sites

Additional control for ISO/IEC 27002:2013, 11.1:

Control

For peripheral sites where control system equipment used by energy utilities is located, physical security controls should be designed, developed and implemented or appropriate countermeasures be applied to mitigate the risk if a sufficient level of physical protection for peripheral sites is not attainable.

Implementation guidance

Especially in energy transmission and distribution networks, and in distributed generation and production systems, components of the control system infrastructure can be distributed across peripheral sites that are frequently unoccupied. In order to protect such decentralized sites where control system facilities are located, the following controls should be considered:

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

b) Where critical assets are operated at peripheral sites, automatic fire control equipment should be installed.

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) Where critical assets are operated at peripheral sites, adequate, physically secure perimeters should be installed using, for example, secure fencing. Additionally, an automatic alarm system should be installed and monitored from a central location.

Where a sufficient level of physical protection for peripheral sites is not attainable, the risk should be taken into consideration and mitigated by the application of appropriate countermeasures. When selecting such countermeasures, the criticality of the assets operated at these peripheral sites as well as redundancy and fall-back concepts implemented for their corresponding system functionality should be given primary consideration.

11.2 Equipment

11.2.1 Equipment siting and protection

Additional implementation guidance for ISO/IEC 27002:2013, 11.2.1:

Under certain circumstances, it is possible that system components of process control systems and supporting infrastructure need 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.

11.2.2 Supporting utilities

Additional implementation guidance for ISO/IEC 27002:2013, 11.2.2:

To avoid cyclic dependencies, all critical assets, 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.

Depending upon plans for system restoration, critical assets essential for system restoration should be capable of being operated independently of an external power supply for an appropriate time defined by system restoration plans. In remote areas, it can 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.

The organization should determine the necessary backup time for uninterruptible power supplies for critical assets.

11.2.3 Cabling security

Additional implementation guidance for ISO/IEC 27002:2013, 11.2.3:

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 on the security requirements of transmitted data, additional non-physical measures such as cryptographic protection should also be considered.

11.2.4 Equipment maintenance

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.2.4.

11.2.5 Removal of assets

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.2.5.

11.2.6 Security of equipment and assets off-premises

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.2.6.

11.2.7 Secure disposal or re-use of equipment

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.2.7.

11.2.8 Unattended user equipment

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 11.2.8.

11.2.9 Clear desk and clear screen policy

Additional implementation guidance for ISO/IEC 27002:2013, 11.2.9:

In the process control domain of energy utilities, HMIs often cannot be left logged off or protected by screen savers, e.g. HMIs of SCADA systems or data logger displays. It should be ensured that such HMIs are either installed in a physical protected location with permanent human supervision (e.g. a control centre) or that they are in a display mode where only non-critical actions can be executed (e.g. view-only mode).

11.3 ENR – Security in premises of external parties

Additional control objective for ISO/IEC 27002:2013, Clause 11:

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

11.3.1 ENR – 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 under 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 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 11.3.3).

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 the necessary security requirements.

Other 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.

11.3.2 ENR – 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 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 persons 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 communication interfaces from that of the customer.

c) It should be possible for the utility to securely monitor the status or operate the equipment remotely.

11.3.3 ENR – Interconnected control and communication systems

Control

Where control systems and related communication lines are interconnected with those of external parties, the range of responsibility and interfaces with the external party 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 identified 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 parties and for reconnecting isolated connections, where necessary.

Energy utility organizations should specify in contracts or agreements that the system interconnections can 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 fall-back measures should be defined and prepared, where necessary.

NOTE This control does not only apply to routed, network-based communication but to serial communication also.

12 Operations security

12.1 Operational procedures and responsibilities

12.1.1 Documented operating procedures

Additional implementation guidance for ISO/IEC 27002:2013, 12.1.1:

In the operating processes documentation, it should be specified exactly under which conditions, emergency or crisis handling procedures are to be invoked.

12.1.2 Change management

Additional implementation guidance for ISO/IEC 27002:2013, 12.1.2:

Changing of hardware systems often results in a change of information systems and process control systems or applications due to the software embedded into these systems. All related changes should be controlled.

12.1.3 Capacity management

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.1.3.

12.1.4 Separation of development, testing and operational environments

Additional implementation guidance for ISO/IEC 27002:2013, 12.1.4:

It should be ensured that development and test systems are adequately secured. According to their criticality, it should be ensured that the test and development systems are sufficiently isolated from other systems and networks (e.g. operation in a separated network environment, no direct Internet access, no direct access to other operational systems, etc.) and that they are exclusively used for development and testing.

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.

12.2 Protection from malware

12.2.1 Controls against malware

Additional implementation guidance for ISO/IEC 27002:2013, 12.2.1:

If the software that protects against malware cannot be deployed for technical reasons (e.g. due to incompatibility of process control systems with anti-malware software, or 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 controls should be implemented that provide at least an equal degree of protection.

Other controls against malware 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.

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.

12.3 Back-up

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.3.

12.4 Logging and monitoring

12.4.1 Event logging

Additional implementation guidance for ISO/IEC 27002:2013, 12.4.1:

In the energy utility sector, relevant event logs may also include certain actions carried out by operating personnel, e.g. control operations, switching operations, parameter or setpoint changes, changes to control programs. Event 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 event protocols and data should be implemented in accordance with all applicable business, statutory, regulatory and internal requirements.

12.4.2 Protection of log information

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.4.2.

12.4.3 Administrator and operator logs

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.4.3.

12.4.4 Clock synchronization

Additional implementation guidance for ISO/IEC 27002:2013, 12.4.4:

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

Integrity and availability of time service should be ensured.

Additional other information for ISO/IEC 27002:2013, 12.4.4:

Depending on the criticality of the process control system in question, the use of dedicated, non-internet synchronized NTP servers or of cryptographically protected NTP time messages should be considered in order to protect the integrity and authenticity of the time synchronization data.

For high precision time synchronization, IEEE 1588 should be used with message authentication codes such as described in IEEE 1588:2008, Annex K. IEEE C37.118 contains information about time synchronisation in the domain of synchrophasor measurements.

12.5 Control of operational software

12.5.1 Installation of software on operational systems

Additional implementation guidance for ISO/IEC 27002:2013, 12.5.1:

Energy utility organizations should minimize any risk of disruption 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 critical assets, 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 (see 12.1.4).

b) In the case of critical assets, sufficient generations of software, parameter sets and configuration data should be retained.

12.6 Technical vulnerability management

12.6.1 Management of technical vulnerabilities

Additional implementation guidance for ISO/IEC 27002:2013, 12.6.1:

To allow for an adequate management of technical vulnerabilities, the energy utility organization should ensure that it receives a comprehensive and up-to-date software inventory (including external party software) from system integrators and system vendors after each relevant software installation, upgrade or change.

12.6.2 Restrictions on software installation

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.6.2.

12.7 Information systems audit considerations

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 12.7.

12.8 ENR – Legacy systems

Additional control objective to ISO/IEC 27002:2013, Clause 12:

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

12.8.1 ENR – Treatment of legacy systems

Control

The energy utility should ensure that all conventional legacy process control system technologies, systems and components (hereinafter referred to as legacy systems) are identified along with their potential information security vulnerabilities and that appropriate controls are implemented according to the defined information security risk treatment process.

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 necessary, proper network isolation, e.g. through the use of secure proxy services should be ensured. These secure proxy services should be hardened and patched regularly. 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 equipment and components used for maintenance and configuration purposes of legacy systems are adequately secured.

12.9 ENR – Safety functions

Additional control objective to ISO/IEC 27002:2013, Clause 12.

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

12.9.1 ENR – 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.

b) Ensuring when possible 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.

13 Communications security

13.1 Network security management

13.1.1 Network controls

Additional implementation guidance for ISO/IEC 27002:2013, 13.1.1:

In the domain of process control systems of the energy utility sector, radio and other wireless communications technologies are often used, e.g. for wide area communication. When designing network controls, special consideration should be given to the security of these technologies.

13.1.2 Security of network services

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 13.1.2.

13.1.3 Segregation in networks

Additional implementation guidance for ISO/IEC 27002:2013, 13.1.3:

Where applicable and technically feasible, the network infrastructure of process control systems should be divided into multiple zones with different functions and protection requirements.[1] In particular, different technical and operational domains should be segregated from one another.

Where technically feasible, the network zones should be separated, e.g. by firewalls, data diodes, 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, e.g. by firewalls, data diodes, filtering routers or gateways.

13.1.4 ENR – Securing process control data communication

Additional control to ISO/IEC 27002:2013, 13.1:

Control

Measures to ensure the security requirements identified during risk assessment (e.g. confidentiality, integrity and availability) of internal and external process control data communication should be designed, developed and implemented.

Implementation guidance

In the field of process control data communication, several sector-specific or generic technical standards and protocols exist, such as:

— IEC 60870-5;

— IEC 60870-6 (TASE.2);

— IEEE 1815 (DNP3);

— IEC 61850;

— IEC 61400-25;

— Modbus.

Some process control communication protocols do not include dedicated security mechanisms. Other protocols define optional security enhancements which are not necessarily included in all implementations. The risks resulting from this, together with the implementation of modified countermeasures, should be taken into consideration. Countermeasures can 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 communication layers.

NOTE The control in 13.1.4 does not only apply to routed, network-based communication but to serial communication also.

13.1.5 ENR – Logical connection of external process control systems

Additional control to ISO/IEC 27002:2013, 13.1:

Control

Before process control systems and related communication links with external parties are connected logically, the energy utility organization should ensure that the risk resulting from such system connection is evaluated and that only authorized communications and information flows, including control system commands and messages, can be exchanged over the link.

Implementation guidance

Process control systems should only be connected with external party systems if this is necessary for operational reasons. Connection should only be carried out at defined connection 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.

13.2 Information transfer

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 13.2.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

14.1.1 Information security requirements analysis and specification

Additional implementation guidance for ISO/IEC 27002:2013, 14.1.1:

To support the acquisition of process control systems, documents specific to the energy utility sector are provided in the Bibliography as examples which can be used during system procurement.

14.1.2 Securing application services on public networks

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.1.2.

14.1.3 Protecting application services transactions

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.1.3.

14.2 Security in development and support processes

14.2.1 Secure development policy

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.1.

14.2.2 System change control procedures

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.2.

14.2.3 Technical review of applications after operating platform changes

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.3.

14.2.4 Restrictions on changes to software packages

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.4.

14.2.5 Secure system engineering principles

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.5.

14.2.6 Secure development environment

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.6.

14.2.7 Outsourced development

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.7.

14.2.8 System security testing

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.8.

14.2.9 System acceptance testing

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.2.9.

14.2.10 ENR – Least functionality

Additional control to ISO/IEC 27002:2013, 14.2:

Control

Process controls systems should be designed, configured, operated, and maintained to provide only required functions.

Implementation guidance

Process control system functionality should be restricted to only those that are defined as required for operations. Unnecessary functions, software, ports, protocols, and services should be documented and then disabled and explicitly prohibited. Required functions, software, ports, protocols, and services should also be documented and explicitly allowed.

14.3 Test data

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 14.3

15 Supplier relationships

15.1 Information security in supplier relationships

15.1.1 Information security policy for supplier relationships

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 15.1.1.

15.1.2 Addressing security within supplier agreements

Additional implementation guidance for ISO/IEC 27002:2013, 15.1.2:

Under the terms of contractual agreements, it should be ensured that the protection requirements of information related to critical assets are given sufficient consideration.

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

Where telecommunication services for the process control systems used by energy utilities are supplied by external 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 can be necessary to take to avoid service overload and to ensure an acceptable degree of independence of the telecommunication services from external energy supply (blackout resistance).

15.1.3 Information and communication technology supply chain

No additional information specific to the energy utility sector for ISO/IEC 27002:2013, 15.1.3.