International Standard

ISO/IEC 27019

Second edition
2024-10

Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Reference number
ISO/IEC 27019:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27019:2017), which has been technically revised.

The main changes are as follows:

— alignment of the controls to the organizational, people, physical and technological themes covered in ISO/IEC 27002:2022;

— the “Guidance” and “Other information” in Clauses 5 to 8 have been updated, to avoid redundancies with ISO/IEC 27002:2022;

— attributes have been added to the controls specific to this document.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 Background and context

This document provides guidance based on ISO/IEC 27002:2022 for information security management when applied to process control systems used in the energy utility industry. The aim of this document is to extend the contents of ISO/IEC 27002:2022 to the domain of process control systems and automation technology for the energy industry.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2022, the process control systems used by energy utilities and energy suppliers are subject to further special requirements. In comparison with conventional information and communication technology (ICT) environments (e.g. office information technology, 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 should be taken into due consideration by the management processes for process control systems and justify separate consideration within ISO/IEC 27001 and related standards.

From the viewpoint of design and function, process control systems used by the energy utility industry 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 are 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. It is important that appropriate controls 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 industry are increasingly interconnected to form complex systems. Risks arising from this trend should 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.

Effective information security in the process control domain of the energy utility industry can be achieved by establishing, implementing, monitoring, reviewing and, if necessary, improving the applicable controls 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 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 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 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 assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) are expected to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

NOTE It is important that energy utility organizations 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, such as:

— 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.

0.4 Determining 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 industry, taking into consideration the special requirements in these environments. If necessary, further controls can be developed to fulfil particular requirements. The selection of controls 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.

NOTE National and international law, legal ordinances and regulations can apply.

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, this document details the fundamental controls according to the objectives of ISO/IEC 27002:2022 and defines specific measures for process control systems in the energy utility industry, their supporting systems and the associated infrastructure.

Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry

1 Scope

This document provides information security controls for the energy utility industry, based on ISO/IEC 27002:2022, 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. for distributed energy resources (DER), electric charging infrastructures, and for 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. distribution management system (DMS) applications or outage management systems (OMS);

— any premises housing the abovementioned equipment and systems;

— remote maintenance systems for abovementioned systems.

This document does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 63096.

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 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002 and the following apply.

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

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

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

3.1.1
blackout
widespread electrical power outage

3.1.2
black start
start-up of an electric power system from a total or partial blackout through internal or external energy resources

3.1.3
computer security incident response team
CSIRT
team of security experts to support the handling of information security incidents

3.1.4
critical asset
asset which can have a direct impact on production or generation, transmission, storage and distribution of electric power, gas, oil and heat

3.1.5
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.

3.1.6
debugging
action of analysing malfunctions in computer systems

3.1.7
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

3.1.8
energy management system
equipment or 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 “energy management system” is also commonly used to refer to a set of applications used by operators of a transmission power grid to monitor, control and optimize the performance of the generation and/or transmission system.

3.1.9
energy supply
process of generation, production or storage of energy for delivery to customers and the operation of an energy supply network

3.1.10
energy utility
legal body or a person that supplies energy in the form of electricity, gas, oil or heat to other parties, to an energy distribution network or to a storage complex

3.1.11
human–machine interface
HMI
user interface for operating and monitoring a *process control system* (3.1.13) or a plant

3.1.12
maintenance
measures used in the field of *energy supply* (3.1.9) that are normally related to inspection, fault clearance and improvement

3.1.13
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.

3.1.14
safety
freedom from risk which is not tolerable

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

3.1.15
safety system
system and component that are required to ensure *safety* (3.1.14)

3.1.16
supervisory control and data acquisition
SCADA
process control system (3.1.13) generally used to control dispersed assets using centralized data acquisition and supervisory controls

3.1.17
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.

3.1.18
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

3.2 Abbreviated terms

CSIRT	computer security incident response team
HMI	human–machine interface
ICT	information and communication technology
SCADA	supervisory control and data acquisition

4 Structure of this document

This document has the same structure as ISO/IEC 27002:2022 with:

— controls from ISO/IEC 27002 that are unchanged;

— controls with additional guidance and other information specific to the energy utility industry;

— new controls not contained in ISO/IEC 27002:2022, which are prefixed with "ENR".

Table A.1 shows the specific security controls related to energy, which can be considered when implementing ISO/IEC 27001:2022 in addition to the security controls in ISO/IEC 27001:2022.

Table B.1 shows the correspondence between the controls specified in Clauses 5 to 8 and those in ISO/IEC 27019:2017.[1)] Table B.2 shows the correspondence between the controls specified in previous edition (ISO/IEC 27019:2017) with those in this document.

5 Organizational controls

5.1 Policies for information security

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.1.

5.2 Information security roles and responsibilities

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.2, includes:

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.

5.3 Segregation of duties

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.3.

5.4 Management responsibilities

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.4.

1) Withdrawn.

5.5 Contact with authorities

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.5, includes:

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 relevant authorities.

In addition to relevant public departments (e.g. fire service, inspectorates), this can also include:

— 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 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.

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 5.5, includes:

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).

5.6 Contact with special interest groups

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.6, includes:

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.

5.7 Threat intelligence

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.7.

5.8 Information security in project management

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 5.8, includes:

Guidelines specific to the energy utility industry to support the acquisition of process control systems can be used during system procurement. Examples of these guidelines are provided in References [20] and [21].

5.9 Inventory of information and other associated assets

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.9, includes:

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

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 information and other associated assets should be defined and documented. The roles of the information and other associated assets' owners and operators in respect of information security should also be defined and documented.

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 5.9, includes:

Examples of information and other associated assets specific to the energy supply domain include:

a) information: grid and network plans, scheduling and dispatching data, geographical and georeferenced information, crisis and emergency plans, grid disaster recovery plans, switching operation data, measured values and measurement data, meter and metered data, operating records, application programming and parameterization data, measurement and message archives, historical and trend data;

   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;

c) hardware: 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;

d) services: telecommunication services, emergency communication services, information services, meteorological services, media and news services, time services.

5.10 Acceptable use of information and other associated assets

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.10.

5.11 Return of assets

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.11.

5.12 Classification of information

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.12, includes:

Classification criteria which is specific to energy utility should consider the following:

— information and other associated assets supporting the operation of critical infrastructures and critical assets;

— information and other associated assets needed for restoration of the energy supply system following a major supply disruption (grid restoration), e.g. systems and components capable of initiating a black start;

— information and other associated assets necessary to ensure occupational health and safety, as well as plant and equipment safety;

— information and other associated assets 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.

5.13 Labelling of information

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.13.

5.14 Information transfer

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.14.

5.15 Access control

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.15, includes:

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 apply 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.

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

e) ensuring physical access protection of network equipment, especially in remote locations;

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

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 5.15, includes:

IEC 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.

5.16 Identity management

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.16, includes:

Examples of shared identities in energy utility process control systems (i.e. where the use of unique user identifiers is not feasible) include the access of operating systems or firmware of embedded systems such as controllers/PLC and maintenance processes in distributed systems. The associated resulting risks should be considered and appropriate controls implemented.

The use of individual and shared identities should be consistent with applicable logging requirements (see 8.15).

5.17 Authentication information

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.17, includes:

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 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 are required 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. when different passwords are required 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;

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

— the shared secret authentication information should be changed in case of personnel changes.

5.18 Access rights

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.18.

5.19 Information security in supplier relationships

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.19, includes:

Process control systems can consist of complex individually customized systems and components. System vendors, integrators and other suppliers 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 suppliers are required to use remote access connections that allow maintenance to be carried out from remote locations. For such remote access connections, the control and the energy utility industry specific guidance in 6.7 should also be considered for external suppliers. It is also possible that employees of suppliers require access to security-controlled areas to perform on-site maintenance. Furthermore, suppliers such as vendors and system integrators can also require access to information related to critical assets.

5.20 Addressing information security within supplier agreements

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.20, includes:

Under the terms of contractual agreements, the protection requirements of information related to critical assets should be 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 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).

5.21 Managing information security in the ICT supply chain

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.21.

5.22 Monitoring, review and change management of supplier services

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.22.

5.23 Information security for use of cloud services

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.23.

5.24 Information security incident management planning and preparation

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.24.

5.25 Assessment and decision on information security events

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.25.

5.26 Response to information security incidents

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.26, includes:

Examples of relevant interested parties to contact in case of incident include national or energy sector-specific CSIRT.

5.27 Learning from information security incidents

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.27.

5.28 Collection of evidence

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.28, includes:

Collecting evidence can conflict with the need for timely system restoration to meet high availability requirements and ensure secure energy supply. The energy utility organization should define in which cases and for which systems evidence collection is possible.

5.29 Information security during disruption

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.29.

5.30 ICT readiness for business continuity

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.30.

5.31 Legal, statutory, regulatory and contractual requirements

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.31, includes:

Requirements specific to the energy utility industry can 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;

— specific data protection requirements imposed by applicable regulators.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 smoothly.

5.32 Intellectual property rights

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.32.

5.33 Protection of records

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.33.

5.34 Privacy and protection of PII

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.34.

5.35 Independent review of information security

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.35.

5.36 Compliance with policies, rules and standards for information security

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 5.36.

5.37 Documented operating procedures

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 5.37, includes:

The operating processes documentation should specify exactly under which conditions, emergency or crisis handling procedures are invoked.

5.38 ENR – Identification of risks related to external business partners

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

The risks to the organization's information and information processing facilities resulting from relationships with external business partners should be identified and appropriate controls implemented before granting access.

Purpose

To maintain an agreed level of information security in external business partners relationships.

Guidance

External business partners, such as system operators on the production, generation, transmission and distribution levels, have different relationships with the organization in comparison to suppliers of products or services (see 5.19). These relationships can also include providing or consuming information.

The close cooperation with external business partners can require close interconnection of the control systems and communication networks of different organizations. This cooperation can also require access to information related to critical assets.

The risks resulting from the access of external business partners 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 controlled or monitored. If external business partners have access to critical assets or confidential information, it should be ensured (e.g. through contractual agreements) that they have implemented a security level that is comparable to the one defined for the internal organization of the energy utility.

Other information

No other information.

5.39 ENR – Addressing security when dealing with customers

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Identity_and_access_management	#Governance_and_Ecosystem #Protection

Control

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

Purpose

To protect information and other associated assets from unauthorized access of customers.

Guidance

The complex and diverse relationships between asset owners, system operators, service providers and internal and external customers in the energy utility industry 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 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 the premises of other energy utilities or customers, or if process control systems are interconnected, the measures described in 7.9, 7.18, and 8.38 should be taken into consideration.

Other information

No other information.

6 People controls

6.1 Screening

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 6.1, includes:

A strict screening process for key personnel who have access to critical assets or are responsible for the operation and maintenance processes of critical assets should be carefully considered and implemented, if necessary. 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 legislation.

6.2 Terms and conditions of employment

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 6.2, includes:

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.

6.3 Information security awareness, education and training

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 6.3, includes:

Staff employed in the energy utility industry 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.

6.4 Disciplinary process

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 6.4.

6.5 Responsibilities after termination or change of employment

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 6.5.

6.6 Confidentiality or non-disclosure agreements

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 6.6.

6.7 Remote working

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 6.7, includes:

Remote access to process control systems performed by the energy utility organization's personnel should be subject to additional security measures such as:

a) ensuring remote access takes place via secured access servers that do not allow a direct connection to the target system or network;

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

c) verifying the security status of the remote access system (e.g. up-to-date patch level and anti-malware status, absence of known blacklisted programmes);

d) enforcing a list of allowed access locations or systems, or both;

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

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

6.8 Information security event reporting

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 6.8.

7 Physical controls

7.1 Physical security perimeters

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.1, includes:

In energy transmission and distribution systems and in the area of distributed generation and production, it is especially common for components to be 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.

7.2 Physical entry

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.2, includes:

The use of physical access control systems should also be considered for peripheral sites where critical assets are located. See 7.17.

7.3 Securing offices, rooms and facilities

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.3.

7.4 Physical security monitoring

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.4.

7.5 Protecting against physical and environmental threats

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.5.

7.6 Working in secure areas

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.6.

7.7 Clear desk and clear screen

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.7, includes:

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).

7.8 Equipment siting and protection

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.8, includes:

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.

7.9 Security of assets off-premises

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.9, includes:

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 7.18);

b) agreements should be concluded contractually with the other energy utility organization for the supply of supporting infrastructure services such as energy supply, cooling and heating;

c) it should be ensured that the operational site where equipment is installed fulfils all the necessary security requirements.

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

d) The equipment cabinets installed at the customer's site should be sturdy and not easily opened by unauthorized persons. Any form of manipulation should be easily detectable.

e) The range of responsibility and the interfaces with the customer should be specified. It should be possible to isolate communication interfaces from that of the customer.

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

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 7.9, includes:

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

7.10 Storage media

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.10.

7.11 Supporting utilities

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.11, includes:

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, it should be possible to operate critical assets which are essential for system restoration 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.

7.12 Cabling security

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 7.12, includes:

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 assessed accordingly 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.

7.13 Equipment maintenance

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.13.

7.14 Secure disposal or re-use of equipment

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 7.14.

7.15 ENR – Securing control centres

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

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.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in control centres.

Guidance

To protect central control system facilities such as grid control centres or the control rooms of centralized or distributed power plants, or 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 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 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

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.

7.16 ENR - Securing equipment rooms

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

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.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in equipment rooms.

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 a data storage room, for data backup, or both.

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 and 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 7.17).

Other information

No other information.

7.17 ENR – Securing peripheral sites

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

To protect peripheral sites, physical security controls should be designed, developed and implemented or appropriate countermeasures applied.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in peripheral sites.

Guidance

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 applied to mitigate risks if a sufficient level of physical protection for peripheral sites is not attainable.

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.

NOTE Relevant national and regional regulations can apply.

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.

Other information

No other information.

7.18 ENR – Interconnected control and communication systems

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_Security	#Protection

Control

For interconnected control and communication systems, responsibilities and interfaces with external parties should be clearly defined to allow organizations to disconnect and to be isolated within an appropriate period of time in case of security incidents.

Purpose

To protect interconnected control systems and related communication lines from interference and compromise over the interconnection.

Guidance

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 case a security incident occurs.

To protect interconnected control systems and related communication lines, energy utility organizations should:

a) monitor the status of their interconnections;

b) have a means for isolating the connections between themselves and external parties and for reconnecting isolated connections, where necessary, in order to diagnose problem areas and take corrective actions;

c) specify in contracts or agreements that the system interconnections can be suspended in cases where severe interference occurs with the organization's own services;

d) clearly define the criteria and conditions necessary for the suspension of system interconnections. 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.

Other information

No other information.

8 Technological controls

8.1 User endpoint devices

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.1, includes:

If user endpoint devices are used on process control networks, energy utilities should include the following in their topic-specific policy on user endpoint devices:

a) define and assign roles allowed to perform tasks that require access to process control systems via user endpoint devices;

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 identity 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.

8.2 Privileged access rights

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.2.

8.3 Information access restriction

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.3.

8.4 Access to source code

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.4, includes:

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

8.5 Secure authentication

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.5, includes:

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.

8.6 Capacity management

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.6.

8.7 Protection against malware

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.7, includes:

In the energy utility industry, it is not always possible to deploy software that protects against malware due to 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 in order to provide at least an equal degree of protection.

Additional controls against malware include:

— securing all physical and logical data interfaces;

— comprehensive system hardening measures to minimize the risk of malware incidents.

Isolation of environments (see ISO/IEC 27002:2022, 8.7, k) should consider network isolation and implementation of segmented network security zones that limit the impact of a malware incident.

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

8.8 Management of technical vulnerabilities

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.8, includes:

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.

Tools to be used during a vulnerability assessment or penetration testing activities on process control systems in operation should be safely configured in order to avoid disruptions. To this purpose, passive mode analyses should always be favoured where applicable, even if their performance is worse than active ones. Exploiting of detected vulnerabilities should always be performed only if necessary and with incident response personnel ready to counter any disruption that can be caused, including the failure or malfunction of the target process control system.

8.9 Configuration management

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.9.

8.10 Information deletion

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.10.

8.11 Data masking

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.11.

8.12 Data leakage prevention

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.12.

8.13 Information backup

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.13.

8.14 Redundancy of information processing facilities

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.14, includes:

Energy utility organizations should consider the continuity of the general energy supply as one of the key elements of business continuity management while ensuring safety of the general public and the security of information and other associated assets. 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 to ensure the availability of these process control systems.

When required, energy utility organizations should ensure redundancy for communications with remote facilities taking into account factors such as weather conditions.

8.15 Logging

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.15, includes:

In the energy utility industry, relevant event logs can 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 retain such records can be required by industry-specific legislation or by regulatory bodies for a wide range of electronic documents.

The acquisition, processing and management of event protocols and data is expected to be implemented according to all applicable business, statutory, regulatory and internal requirements.

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 8.15, includes:

ISO/IEC 27031 provides guidance on information and communication technology readiness for business continuity.

8.16 Monitoring activities

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.16.

8.17 Clock synchronization

Guidance

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.17, includes:

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.

Other information

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 8.17, includes:

Depending on the criticality of the process control system in question, the use of dedicated, non-internet synchronized Network Time Protocol (NTP) servers or 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, additional guidance on security can be found in IEC 61588. For information about time synchronisation in the domain of synchrophasor measurements, see IEEE/IEC 60255-118-1.

8.18 Use of privileged utility programs

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.18.

8.19 Installation of software on operational systems

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.19, includes:

Energy utility organizations should minimize any risk of disruption of operational systems. In particular, if changes to applications and core systems (e.g. operating system software, firmware) are 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 8.31).

8.20 Networks security

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.20.

8.21 Security of network services

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.21.

8.22 Segregation of networks

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.22, includes:

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.

The segregation of domains in the energy utility industry should consider additional criteria such as physical units (e.g. different sites or plant units).

8.23 Web filtering

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.23.

8.24 Use of cryptography

Additional other information specific to the energy utility industry for ISO/IEC 27002:2022, 8.24, includes:

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.

8.25 Secure development life cycle

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.25.

8.26 Application security requirements

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.26.

8.27 Secure system architecture and engineering principles

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.27.

8.28 Secure coding

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.28.

8.29 Security testing in development and acceptance

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.29.

8.30 Outsourced development

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.30.

8.31 Separation of development, test and production environments

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.31, includes:

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 are 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 (i.e. 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.

8.32 Change management

Additional guidance specific to the energy utility industry for ISO/IEC 27002:2022, 8.32, includes:

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.

8.33 Test information

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.33.

8.34 Protection of information systems during audit testing

There is no additional information specific to the energy utility industry for ISO/IEC 27002:2022, 8.35.

8.35 ENR – Treatment of legacy systems

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

Control

The energy utility should ensure that all legacy systems are identified along with their potential information security vulnerabilities and that appropriate controls are implemented.

Purpose

To reduce the risks from the use of legacy systems.

Guidance

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.

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.

Other information

No other information.

8.36 ENR – Integrity and availability of safety functions

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

The integrity and availability of information, assets, systems, components and functions that are required to ensure safety functions should be protected according to applicable safety standards.

NOTE Legal requirements can apply.

Purpose

To protect the integrity and availability of safety functions against failure, interference and manipulation.

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.

Other information

No other information.

8.37 ENR – Securing process control data communication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

Control

Security measures to ensure the security requirements of internal and external process control data communication should be designed, developed and implemented.

Purpose

To protect information transmitted via process control data communication from compromise.

Guidance

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

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);[13]

— IEC 61850;

— IEC 61400-25;

— Modbus.[23]

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. according to 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 8.37 does not only apply to routed network-based communication but also to serial communication.

Other information

No other information.

8.38 ENR – Logical connection of external process control systems

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

Control

The energy utility organization should ensure that risks resulting from process control systems' connection to external parties are assessed and that only authorized communications and information flows can be exchanged.

Purpose

To protect control systems from interference, manipulation and compromise over logical connections with external parties.

Guidance

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

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.

Other information

No other information.

8.39 ENR – Least functionality

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

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

Purpose

To reduce the risks originating from unnecessary functionalities.

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.

Other information

No other information.

8.40 ENR – Emergency communication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Availability	#Protect #Detect	#System_and_network_security	#Protection

Control

Essential communication links should be maintained in case of emergencies.

Purpose

To ensure essential communication is possible even under adverse conditions.

Guidance

If major disturbances, natural disasters, accidents or any other emergencies occur, or if there is a risk thereof, energy utility organizations should ensure that essential communication links are maintained with their own emergency staff and 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.

Essential communication links can 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;

— gas and oil production, and heat generation;

— energy storage sites;

— 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 can 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 required for system restoration can in turn rely on the electric power supply.

Other information

No other information.

Annex A
(informative)

Energy utility industry specific controls reference

In addition to the security controls in ISO/IEC 27001:2022, Annex A, the specific security controls related to energy in Table A.1 can be considered when implementing ISO/IEC 27001:2022.

Table A.1 — Energy utility industry specific security controls

5	**Organizational controls**	
5.38	ENR – Identification of risks related to external business partners	The risks to the organization's information and information processing facilities resulting from relationships with external business partners should be identified and appropriate controls implemented before granting access.
5.39	ENR – Addressing security when dealing with customers	All identified security requirements should be addressed before giving customers access to the organization's information or assets.
7	**Physical controls**	
7.15	ENR – Securing control centres	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.
7.16	ENR – Securing equipment rooms	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.
7.17	ENR – Securing peripheral sites	To protect peripheral sites, physical security controls should be designed, developed and implemented or appropriate countermeasures applied.
7.18	ENR – Interconnected control and communication systems	For interconnected control and communication systems, responsibilities and interfaces with external parties should be clearly defined to allow organizations to disconnect and to be isolated within an appropriate period of time in case of security incidents.
8	**Technological controls**	
8.35	ENR – Treatment of legacy systems	The energy utility should ensure that all legacy systems are identified along with their potential information security vulnerabilities and that appropriate controls are implemented.
8.36	ENR – Integrity and availability of safety functions	The integrity and availability of information, assets, systems, components and functions that are required to ensure safety functions should be protected according to applicable safety standards.
8.37	ENR – Securing process control data communication	Security measures to ensure the security requirements of internal and external process control data communication should be designed, developed and implemented.
8.38	ENR – Logical connection of external process control systems	The energy utility organization should ensure that risks resulting from process control systems' connection to external parties are assessed and that only authorized communications and information flows can be exchanged.
8.39	ENR – Least functionality	Process controls systems should be designed, configured, operated and maintained to provide only required functions.
8.40	ENR – Emergency communication	Essential communication links should be maintained in case of emergencies.

Annex B
(informative)

Correspondence between this document and the first edition (ISO/IEC 27019:2017)

The purpose of this annex is to provide backwards compatibility with the first edition of this document (ISO/IEC 27019:2017) for organizations currently using it and wanting to transition to this edition. Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27019:2017.

Table B.1 — Correspondence between the controls in this document and controls in ISO/IEC 27019:2017

ISO/IEC 27019:2024 control identifier	ISO/IEC 27019:2017 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	Non-existent in ISO/IEC 27019:2017 and derived from ISO/IEC 27002:2022	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	Non-existent in ISO/IEC 27019:2017 and derived from ISO/IEC 27002:2022	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents