International Standard

ISO/IEC 27019

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

Second edition
2024-10

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*