ISO/IEC 27019

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27019:2024 — Information security, cybersecurity and privacy protection — **Information security controls for the energy utility industry** *(second edition)*

Abstract

"[ISO/IEC 27019:2024] 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;*

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

- *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."*

[Source: ISO/IEC 27019:2024]

Introduction

This standard is intended to help organisations in "the energy utility industry" (such as conventional/non-nuclear electricity generators) to interpret and apply ISO/IEC 27002 in order to secure their industrial process control systems *i.e.* their **O**perational **T**echnology as opposed to **I**nformation **T**echnology.

Scope and purpose

Information security management presents fundamentally the same risk management challenges in all contexts, but the real-time nature of process control systems plus their associated safety and environmental criticality make some aspects particularly challenging for energy utilities. The standard therefore provides additional, more specific guidance on information security controls than the generic advice provided by ISO/IEC 27002, tailored to the specific context of process control systems used by energy utilities 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.

Note: given its unique risks, the scope of ISO/IEC 27019 explicitly *excludes* process control in nuclear facilities. See instead (for example) IEC 63096 *"Nuclear power plants - Instrumentation, control and electrical power systems - Security controls"*.

Structure and content

ISO/IEC 27019 complements and must be read in conjunction with ISO/IEC 27002. It is aligned with ISO/IEC 27002:2022 but does *not* incorporate the content of ISO/IEC 27002.

A dozen additional controls are offered for the energy sector, such as:

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

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 in accordance with 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.

The standard notes in clause 0.4:

> *"In addition to the controls provided by a comprehensive information security management system, [ISO/IEC 27019] provides additional assistance and sector-specific measures for the process control systems used by the energy utility sector, taking into consideration the special requirements in these environments. If necessary, further 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."*

Other ISO27k standards are also recommended to fill-in the broader context *e.g.* ISO/IEC 27001 for an overarching **I**nformation **S**ecurity **M**anagement **S**ystem that encompasses process control/OT as well as general commercial systems, networks and processes, plus ISO/IEC 27005 concerning the management of information risk.

Status of the standard

A *preliminary* edition was published as a **T**echnical **R**eport in **2013** by fast-tracking the German standard DIN SPEC 27009:2012-04 based on ISO/IEC 27002:2005.

The *first* International Standard was published in **2017,** based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013, plus IEC TC 57 standards, IEC TC 65 standards (IEC 62443-2-1) and IEC SC45A standards (IEC 62645). A corrigendum to replace a stray "should" with a "shall" in the annex was published to critical acclaim in 2019. Hurrah! Crisis averted!

The corrected standard was confirmed unchanged in 2022 ... but then was revised anyway to reflect the organisational/people/physical/technological themed structure and controls sequence of ISO/IEC 27002:2022 adding 12 suggested "ENR" controls to ISO/IEC 27022's 96.

The *second* edition was published in October **2024**.

Personal comments

The global energy industry has long had a strong safety culture since the devastating physical impacts caused by explosions, oil and chemical spills, radioactive releases *etc.* are painfully apparent (Bhopal, Three Mile Island, Chernobyl, Exxon Valdiz, Deepwater Horizon, Fukoshima ... need we say more?). The industry also has a strong awareness of its environmental obligations both in terms of its own operations, the upstream primary industries (*e.g.* mining) and the downstream impacts of some of its products. Furthermore, the industry has a strong culture of physical and information security due to the substantial risks arising from:

- **Threats** such as natural disasters and deliberate attacks (sabotage) from hackers, **A**dvanced **P**ersistent **T**hreats, spies and spooks, terrorists, insiders, pressure groups and foreign states, as well as more mundane threats from accidents, competitors, electromechanical failures, malware/ransomware, social engineers *etc*.;
- **Vulnerabilities** inherent in their systems and processes. Process control systems that are (in some manner) connected to, exposed to or accessible from the Internet and other networks are vulnerable to a panopoly of cyber-threats, including those resulting from design flaws and bugs in software especially if they are not well designed, managed and maintained (*e.g*. security patching is distinctly challenging on safety-critical systems, given the need for assurance that patches do not harm safety); and
- **Impacts**, particularly limited availability and/or integrity of business- or safety-critical information leading to supply interruptions (power cuts), out-of-specification supplies (*e.g*. over/under-voltage supplies), safety incidents (*e.g*. the catastrophic release of vast amounts of energy) and environmental incidents (*e.g.* oil/gas/chemical leaks). Energy utilities, both public and private, are generally classed as part of the critical national infrastructures (*e.g.* under NIS 2 in Europe) due to their obvious strategic significance.

With an extremely high level of automation, the energy industry relies heavily on OT, principally electronic process control systems such as **P**rogrammable **L**ogic **C**ontrollers, **I**ndustrial **I**nternet **o**f **T**hings, **I**ndustrial **C**ontrol **S**ystems and **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition, plus the associated networks and procedures, to monitor, direct and control its production activities in real time. Most of the safety-related operations, for example, in a modern plant depend heavily on networked computer systems with electronic monitoring and electrically-operated valves, switches and actuators, while manually-operated controls are often limited to specific backup or emergency override functions. Many of the monitored and controlled systems are located in physically stressful locations subject to extreme heat, pressure, corrosion and/or vibration, and some are distributed remotely, sometimes *very* remotely, making physical access, monitoring and access control challenging and costly.

In short, the industry cannot function normally and safely without its electronic process control systems and networks, while serious, widespread or extended incidents cause severe national if not international repercussions.

< Previous standard ^ Up a level ^ Next standard >