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)

COPYRIGHT PROTECTED DOCUMENT

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.

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。

国际标准

ISO/IEC 27019

2024 年 10 月
第二版

信息安全、网络安全和隐私保护——公用能源行业的信息安全控制措施

信息安全、网络安全与隐私保护——能源运营商行业的信息安全措施

奥邦检验认证集团有限公司翻译
内部资料 严谨外泄

Reference number ISO/IEC 27019:2024(en)

受版权保护的文件

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了全球标准化的专门体系。作为 ISO 或 IEC 成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定技术活动领域的事务。ISO 和 IEC 的技术委员会在共同感兴趣的领域进行合作。与 ISO 和 IEC 有联系的其他政府和非政府国际组织也参与了这项工作。

用于制定本文件及其后续维护的程序在《ISO/IEC 指令》第 1 部分中描述。尤其应注意不同类型的文件所需的不同批准标准。本文件依据《ISO/IEC 指令》第 2 部分的编辑规则起草（参见 www.iso.org/directives 或 www.iec.ch/members_experts/refdocs）。

ISO 和 IEC 提请注意，实施本文件可能涉及（一项或多项）专利的使用。ISO 和 IEC 不对任何声称的专利权的证据、有效性或适用性持任何立场。截至本文件发布之日，ISO 和 IEC 未收到可能实施本文件所需的（一项或多项）专利的通知。然而，提醒实施者注意，这可能不是最新信息，最新信息可从 www.iso.org/patents 和 https://patents.iec.ch 提供的专利数据库中获取。ISO 和 IEC 不承担识别任何或所有此类专利权的责任。

本文件中使用的任何商品名称均是为方便用户而提供的信息，并不构成认可。

关于标准的自愿性、与符合性评估相关的 ISO 特定术语和表达的含义，以及 ISO 遵守世界贸易组织（WTO）《技术性贸易壁垒（TBT）》原则的信息，请参见 www.iso.org/iso/foreword.html。在 IEC，请参见 www.iec.ch/understanding-standards。

本文件由联合技术委员会 ISO/IEC JTC 1（信息技术）的分技术委员会 SC 27（信息安全、网络安全和隐私保护）编制。

本第二版取消并取代了第一版（ISO/IEC 27019:2017），第一版已进行了技术修订。

主要变化如下：
— 将控制措施与 ISO/IEC 27002:2022 涵盖的组织、人员、物理和技术主题保持一致；
— 更新了第 5 至第 8 章中的“指南”和“其他信息”，以避免与 ISO/IEC 27002:2022 重复；
— 为本文件特定的控制措施添加了属性。

对本文件的任何反馈或问题应直接发送给用户的国家标准机构。这些机构的完整列表可在 www.iso.org/members.html 和 www.iec.ch/national-committees 找到。

引言

0.1 背景和环境

本文件基于 ISO/IEC 27002:2022，为应用于能源公用事业行业使用的过程控制系统的信息安全管理提供了指南。本文件旨在将 ISO/IEC 27002:2022 的内容扩展到能源行业的过程控制系统和自动化技术领域。

除了 ISO/IEC 27002:2022 中阐述的安全目标和措施外，能源公用事业和能源供应商使用的过程控制系统还受到进一步的特殊要求。与常规的信息和通信技术（ICT）环境（例如，办公信息技术、能源交易系统）相比，过程控制系统在开发、运行、修复、维护和运行环境方面存在根本性的显著差异。此外，本文件中提及的过程技术可以代表关键基础设施的组成部分。这意味着它们因此对此类基础设施的安全可靠运行至关重要。过程控制系统的管理过程应充分考虑这些区别和特征，并证明在 ISO/IEC 27001 及相关标准内单独考虑是合理的。

从设计和功能的角度来看，能源公用事业行业使用的过程控制系统实际上是信息处理系统。它们使用传感器收集过程数据并监控物理过程的状态。然后，系统处理这些数据并生成控制输出，通过执行器调节操作。控制和调节是自动的，但操作人员也可以进行手动干预。因此，信息和信息处理系统是能源公用事业内部运营过程的重要组成部分。重要的是，应以与其他组织单元相同的方式应用适当的控制措施。

基于标准 ICT 技术的软件和硬件（例如，可编程逻辑）组件越来越多地用于过程控制环境，并且也涵盖在本文件中。此外，能源公用事业行业的过程控制系统日益互连形成复杂系统。应在风险评估中考虑由此趋势产生的风险。

过程控制环境中的信息和信息处理系统也面临越来越多的威胁和脆弱性。

能源公用事业行业过程控制领域的有效信息安全可以通过建立、实施、监视、评审并在必要时改进本文件中阐述的适用控制措施来实现，以达到组织特定的安全和业务目标。在此，特别重要的是要充分考虑能源公用事业在社会中的特殊作用以及安全可靠能源供应的经济必要性。最终，能源行业网络安全的整体成功基于所有利益相关者（供应商、客户等）的协作努力。

0.2 能源公用事业使用的过程控制系统的安全考虑

对能源公用事业行业过程控制领域制定一个通用且全面的信息安全框架的要求基于若干基本要求：

a) 客户期望安全可靠的能源供应。
b) 法律要求能源供应系统安全、可靠且安全地运行。
c) 能源提供商需要信息安全以保障其商业利益、满足客户需求并遵守法律法规。

0.3 信息安全要求

能源公用事业组织识别其安全要求至关重要。安全要求主要有三个来源：

a）对组织风险的评估，需考虑组织的整体业务战略和目标。这可以通过信息安全特定的风险评估来促进或支持。这应导致确定必要的控制措施，以确保组织的剩余风险满足其风险接受准则；
b）组织及其利益相关方（贸易伙伴、服务提供商等）预期需要遵守的法律、法规、规章和合同要求及其社会文化环境；
c）组织为支持其运营而制定的信息生命周期所有步骤的一套原则、目标和业务要求。

注：能源公用事业组织确保过程控制系统的安全要求得到分析并在信息安全方针中得到充分覆盖，这一点很重要。信息安全要求和目标的分析包括考虑安全能源供应和交付的所有相关标准，例如：
— 能源供应安全性的损害；
— 能源流动的限制；
— 受影响的人口份额；
— 人身伤害的危险；
— 对其他关键基础设施的影响；
— 对信息隐私的影响；
— 财务影响。

0.4 确定控制措施

一旦识别了安全要求和风险，并决定了如何处理风险，随后便选择并实施适当的控制措施，以确保将风险降低到可接受的水平。

除了全面的信息安全管理体系所提供的控制措施外，本文件还考虑了这些环境中的特殊要求，为能源公用事业行业使用的过程控制系统提供了额外的帮助和特定行业的措施。如有必要，可以制定进一步的控制措施以满足特定要求。控制措施的选择取决于组织基于其自身风险接受准则、处理风险的选择以及组织整体风险管理方法所作出的决策。

注：可能适用国家和国际法律、法令和法规。

0.5 受众

本文件的目标受众是负责能源公用事业使用的过程控制系统运行的人员、信息安全经理、供应商、系统集成商和审计员。针对该目标群体，本文件根据 ISO/IEC 27002:2022 的目标详细说明了基本控制措施，并为能源公用事业行业的过程控制系统、其支持系统和相关基础设施定义了具体措施。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。