TECHNICAL REPORT

ISO/IEC TR 27019

First edition
2013-07-15

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Technologies de l'information — Techniques de sécurité — Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie des opérateurs énergétiques

Reference number
ISO/IEC TR 27019:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 27019 was prepared by DIN Deutsches Institut für Normung e. V. (as DIN SPEC 27009:2012-04 [4]) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by the national bodies of ISO and IEC.

Introduction

This Technical Report provides guiding principles based on ISO/IEC 27002 “Code of practice for information security management” for information security management applied to process control systems as used in the energy utility industry. The aim of this document is to extend the ISO/IEC 27000 standards to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

At the focus of application of this document are the systems and networks for controlling and supervising the generation, transmission and distribution of electric power, gas and heat in combination with the control of facilitating processes. This includes control and automation systems, protection and safety systems and measurement systems, including their associated communications and telecontrol applications. For purposes of simplification, these systems will be collectively referred to in the following as “process control systems”.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2005, the process control systems used by energy utilities and energy suppliers are subject to further, special requirements. In comparison with conventional IT environments (e.g. office IT) 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 may represent integral components of critical infrastructures which means they are therefore essential for the secure and reliable operation of such infrastructures. These distinctions and characteristics need to be taken into due consideration by the management processes for process control systems and justify separate consideration within the ISO/IEC 27000 series of standards.

In particular, the following fundamental differences exist compared with conventional IT systems:

Security features

In comparison with conventional IT systems, process control systems exhibit increased requirements with regard to their availability and integrity. In some operational environments failure of the process monitoring and control systems cannot be tolerated. Also, the integrity of the data processed is frequently of crucial importance. Incorrect data can lead to incorrect control inputs, resulting in failure of protection or safety systems or trigger incorrect decisions by operating personnel, as a result of an erroneous representation of current process conditions. These requirements therefore need to be taken into consideration during the system design stage as well as in normal operation.

System architecture

Besides the central IT installations within control centers for grid operation or conventional power plants there are several systems which are typically distributed over larger areas, e.g.:

— process control and monitoring systems within substations and gas pressure regulating and metering stations;

— process control and monitoring systems for distributed generation, like wind-farms or photovoltaic generation units;

— digital metering and measurement devices.

Often, these remote systems cannot be physically protected at the same level as centrally located systems. Therefore, the system architecture needs to take these differences into consideration and it may be necessary to provide additional safeguards at the interface between distributed and central systems.

Also, the operating and management processes for distributed systems may vary in comparison with centralized IT architectures. It is for instance, not normal procedure to apply changes to essential systems in critical substations or at other important sites via remote access, unless the corresponding field service personnel are present on-site.

Furthermore, in many process control environments the architecture should allow for autonomous (local) operation of each distributed site – without network access to central installations. In case of outages it has to be possible to restart selected sites without an external energy source, e.g. for grid restoration ("black start capable" systems).

Maintenance

Process control systems are often designed for a service life of 20 or more years. If standard operating systems or software packages are used, special measures to handle outdated and no-longer supported software are needed.

Frequent shutdowns of process control components, e.g. to install software patches or updates, are normally not possible. System restarts after software installation may also not be acceptable due to the availability requirements. Maintenance periods have to be planned and scheduled in advance. Particularly thorough and careful pre-deployment testing is required in order to ensure that the integrity of the process control system is maintained.

Equipment resources

The in-process components (e.g. field control elements) of process control systems are generally designed to support only the intended process data applications and frequently do not have sufficient system resources to support additional security features such as encryption or authentication.

Audience

This guideline is targeted at the persons responsible for the operation of process control systems used by energy utilities, information security managers, vendors, system integrators and auditors. For this target group it details the fundamental measures in accordance with the objectives of the ISO/IEC 27002:2005 standard and defines specific measures for process control systems, their supporting systems and the associated infrastructure.

Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

1 Scope

The scope of this guideline covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes in particular the following systems, applications and components:

— the overall IT-supported central and distributed process control, monitoring and automation technology as well as IT systems used for their operation, such as programming and parameterization devices;

— digital controllers and automation components such as control and field devices or PLCs, including digital sensor and actuator elements;

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

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

— digital metering and measurement devices, e.g. for measuring energy consumption, generation or emission values;

— digital protection and safety systems, e.g. protection relays or safety PLCs;

— distributed components of future smart grid environments;

— all software, firmware and applications installed on above mentioned systems.

Outside the scope of this guideline is the conventional or classic control equipment that is non-digital, i.e. purely electro-mechanical or electronic monitoring and process control systems. Furthermore, energy process control systems in private households and other, comparable residential building installations are outside the scope of this guideline.

Telecommunication systems and components used in the process control environment are also not directly part of the scope of this guideline. These are covered by the standard “ISO/IEC 27011:2008 *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*”. It is recommended that users of this guideline should implement the measures defined in that standard for the telecommunication systems and components used in the process control environment.

2 Normative references

The documents referred to below are required for the purposes of this document. When such references are made only the version stated shall be applicable. If references are made without stating dates then the latest version of the document in question shall be applicable (including all changes).

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the definitions in accordance with ISO/IEC 27001:2005 and ISO/IEC 27002:2005 shall apply, together with the following definitions.

3.1
blackout
widespread electrical power outage

3.2
Computer Emergency Response Team
CERT
team of security experts to support the handling of information security incidents

3.3
critical infrastructure
organizations and facilities that are essential for the functioning of society and the economy as a whole

NOTE A failure or malfunction of such organizations and facilities would result in sustained supply shortfalls, make a significant impact on public security and have other wide ranging impacts.

3.4
debugging
analysing malfunctions in computer systems

3.5
distribution
the transport of electrical energy of high, medium or low voltage over a distribution grid or the transport of gas or heat over local or regional distribution networks

3.6
energy equipment installation
equipment or plant for the generation, conversion, storage, transfer or supply of energy

3.7
energy supply
the process of generation, production or storage of energy for delivery to customers and the operation of an energy supply network

3.8
energy utility
legal body or a person that supplies energy in form of electricity, gas or heat to other parties, to an energy distribution network or to a storage complex

3.9
human-machine interface
HMI
user interface for operating and monitoring of a process control systems and/or a plant

3.10
maintenance
all measures used in the field of energy supply that are normally related to inspection, maintenance, fault clearance and improvement

3.11
PLC
programmable logic controller

3.12
process control system
system that serves to control and monitor the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes

3.13
safety
functional safety

3.14
safety systems
systems and components that are required to ensure functional safety

3.15
smart grid
electric grid system, which is characterized by the use of communication networks and the control of grid components and loads

3.16
statement of applicability
SOA
Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS

3.17
transmission system
transmission grid for the transport of electrical energy using a high voltage or ultra-high voltage grid or a gas transmission network for the transport of natural gas using a high pressure pipeline network

4 Overview

4.1 Structure of this guideline

This guideline has been structured in a format compatible with ISO/IEC 27002:2005. Where no additional detailed information is necessary direct reference is made here to the specifications applicable to the objectives and measures set forth in ISO/IEC 27002:2005. In cases where the measures set forth in ISO/IEC 27002:2005 require a method of implementation that is specific to the energy supply sector or some form of expanded implementation this is provided in the form of implementation guidelines for the energy supply sector or as further information. A list of the new control objectives and/or measures for the energy supply sector is set forth in Annex A. Supplementary comments and notes are set forth in Annex B.

Further recommendations for implementation and information specific to energy utilities are included in the following clauses:

- Organization of information security (clause 6);
- Asset management (clause 7);
- Human resources security (clause 8);
- Physical and environmental security (clause 9);
- Communications and operations management (clause 10);
- Access control (clause 11);

- Information systems acquisition, development and maintenance (clause 12);
- Business continuity management (clause 14);
- Compliance (clause 15).

4.2 Information security management systems for energy supply utilities

4.2.1 Objectives

From the viewpoint of design and function, process control systems used by the energy utility sector are in fact information processing systems. They collect process data and monitor the status of the physical process using sensors. The systems then process this data and generate control outputs that regulate actions using actuators. The control and regulation is automatic but manual intervention by operating personnel is also possible. Information and information processing systems are therefore an essential part of operational processes within energy utilities. This means that appropriate protection measures should be applied in the same manner as for other organizational units.

Software and hardware components based on standard IT technology are being utilized increasingly in process control environments.

Nowadays, the information and information processing systems in process control environments are consequently also exposed to an increasing number of threats and vulnerabilities. It is therefore essential that, in the process control domain of the energy utility industry, adequate information security is achieved through the implementation and continuous improvement of an ISMS in accordance with ISO/IEC 27001.

Effective information security in the process control domain of the energy utility sector can be achieved by establishing, implementing, monitoring, reviewing and if necessary improving the applicable measures set forth in this guideline, in order to attain the specific security and business objectives of the organization. Particular consideration should be given here to the special role of the energy utilities in society and to the economic necessity of a secure and reliable energy supply.

4.2.2 Security considerations for process control systems used by the energy utilities

The requirement for a general and overall information security framework for the process control domain of the energy utility industry is based on several basic requirements:

a) Customers expect a secure and reliable energy supply.

b) Legal and regulatory requirements demand secure and reliable operation of energy supply systems.

c) In their own interests energy providers themselves require information security in order to safeguard their business interests and to fulfil customer needs and comply with the legal regulations.

4.2.3 Information assets to be protected

In order to establish an information security management system, it is necessary for the organization to identify all of its organizational assets. The identification of organizational assets and the clarification of their importance enable the application of appropriate controls.

Further advice regarding the type of organizational assets that should be protected by an energy supply organization can be found in 7.1.1, Inventory of assets.

4.2.4 Establishment of information security management

4.2.4.1 How to establish security requirements

It is essential that energy utility organizations identify their security requirements. There are three main sources of security requirements:

a) The results of an organization's risk assessment, taking into account the organization's general business strategies and objectives. Through a risk assessment, threats to the organization's own assets will be identified; vulnerabilities and likelihood of occurrence will be evaluated and potential impact estimated.

b) The requirements which result from legislation and bye-laws, regulations and contracts which have to be fulfilled by an organization, and sociocultural requirements. Particular examples include safeguarding a reliable, effective and secure energy supply as well as the reliable fulfilment of the requirements of a deregulated energy market, in particular the reliable and secure transfer of data with third parties.

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

4.2.4.2 Assessing security risks

The necessary security measures or controls are determined by the methodical assessment of security risks. The cost of controls has to be balanced against the economic losses that may be incurred due to security issues. The results of the risk assessment facilitate the definition of adequate management actions and priorities for the management of information security risks as well as the implementation of the controls chosen to protect against these risks. The risk assessment should be repeated periodically in order to take all changes into account, which could affect the results assessed.

4.2.4.3 Selecting controls

Once the security requirements and risks have been identified and decisions taken on how to deal with the risks, appropriate controls should then be 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 management system this guideline 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. It is therefore recommended that energy utilities implement the measures set forth in this guideline. If necessary, further measures can be developed to fulfil particular requirements. The selection of security measures depends upon the decisions taken by the organization on the basis of its own risk acceptance criteria, the options for dealing with the risk and the general risk management approach of the organization. The selection of measures should also take relevant national and international law, legal ordinances and regulations into consideration.

4.2.5 Critical success factors

The contents from ISO/IEC 27002:2005 clause 0.7 apply.

5 Security policy

No additional information specific to the energy utility domain.