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.

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).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition cancels and replaces the first edition of ISO/IEC TR 27019:2013, which has been technically revised.

The main changes compared to the previous edition are as follows:

— the scope has changed to include the energy oil sector;

— this document has been changed from a Technical Report to an International Standard;

— the previous edition was aligned with ISO/IEC 27002:2005. The new structure has been aligned with ISO/IEC 27002:2013;

— the title has been changed.

— where appropriate the technical content has been revised and updated to reflect current technological developments in the energy sector.

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.

This corrected version of ISO 27019:2017 corrects "should" into "shall" in Table A.1, 11.1.7

0 Introduction

0.1 Background and context

This document provides guiding principles based on ISO/IEC 27002:2013 "Code of practice for information security controls" 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 contents of ISO/IEC 27002:2013 to the domain of process control systems and automation technology, thus allowing the energy utility industry to implement a standardized and specific information security management system (ISMS) that is in accordance with ISO/IEC 27001:2013 and extends from the business to the process control level.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2013, the process control systems used by energy utilities and energy suppliers are subject to further special requirements. In comparison with conventional ICT environments (e.g. office IT, 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 need to be taken into due consideration by the management processes for process control systems and justify separate consideration within the ISO/IEC 27000 family of standards.

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 processes 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 it is important that appropriate protection measures 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 sector are increasingly interconnected to form complex systems. Risks arising from this trend need to 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. 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 27001:2013.

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 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 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 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 the 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 results of an organization's risk assessment, taking into account the organization's general business strategies and objectives. Through a risk assessment, risk sources and events are identified; potential consequences and likelihood of the occurrence of the risks are assessed.

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 external parties.

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

NOTE It is important that the energy utility organization 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, e.g.

— 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.

The necessary security measures or controls are determined by the methodical assessment of security risks. It is necessary that the cost of controls be balanced against the economic losses that can 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; and

— 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 can affect the results assessed.

Requirements for the risk assessment and control selection are given in ISO/IEC 27001:2013.

0.4 Selecting controls

Once the security objectives 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 sector, taking into consideration the special requirements in these environments. 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.

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, it details the fundamental measures in accordance with the objectives of ISO/IEC 27002:2013 and defines specific measures for process control systems of the energy utility industry, their supporting systems and the associated infrastructure.

Information technology — Security techniques — Information security controls for the energy utility industry

1 Scope

This document provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry 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. of Distributed Energy Resources (DER), electric charging infrastructures, in 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. DMS (Distribution Management System) applications or OMS (Outage Management System);

— any premises housing the above-mentioned equipment and systems;

— remote maintenance systems for above-mentioned systems.

This document does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 62645.

This document also includes a requirement to adapt the risk assessment and treatment processes described in ISO/IEC 27001:2013 to the energy utility industry-sector–specific guidance provided in this document.

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.