PD ISO/IEC TR 27019:2013

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/IEC TR 27019:2013.

As described in its International Foreword, ISO/IEC TR 27019:2013 was adopted by Joint Technical Committee ISO/IEC JTC 1, Information technology, using the "fast track procedure". In consequence it has been published as an ISO/IEC Technical Report, and adopted by BSI as a Published Document.

However, IST/33 considers its content to be analogous to other sector-specific interpretations of ISO/IEC 27002, *Code of practice for information security management*, that have been published as International and British Standards.

The content of this Published Document is based on the 2005 edition of ISO/IEC 27002 and may need to be updated when ISO/IEC 27002 is republished.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT – Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2013

ISBN 978 0 580 80270 6

ICS 35.040; 35.240.99

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2013.

Amendments/corrigenda issued since publication

Date	Text affected

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)

COPYRIGHT PROTECTED DOCUMENT

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*