TECHNICAL REPORT

ISO/IEC TR 27019

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

COPYRIGHT PROTECTED DOCUMENT

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.