SLOVENSKI STANDARD
oSIST prEN IEC 62443-2-1:2019

01-november-2019

Zaščita industrijske avtomatizacije in kontrolnih sistemov - 2-1. del: Zahteve za program varnosti zaščite za lastnike sredstev IACS

Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners

Réseaux industriels de communication - Sécurité dans les réseaux et les systèmes - Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

Ta slovenski standard je istoveten z: **prEN IEC 62443-2-1:2019**

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

oSIST prEN IEC 62443-2-1:2019 **en,fr,de**

65/756/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62443-2-1 ED2**	
DATE OF CIRCULATION: **2019-08-23**	CLOSING DATE FOR VOTING: **2019-11-15**
SUPERSEDES DOCUMENTS: **65/692A/RR**	

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

SECRETARIAT: France	SECRETARY: Mr Rudy BELLIARDI
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 44, SC 45A, TC 57, SC 62A; ISO/IEC/JTC1/SC 27	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY

☒ SUBMITTED FOR CENELEC PARALLEL VOTING ☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

Security for industrial automation and control systems –

Part 2-1: Security program requirements for IACS asset owners

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard IEC 62443-2-1 has been prepared by subcommittee TC65: Industrial process measurement, control and automation, in cooperation with the ISA99 liaison.

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title Security for industrial automation and control systems, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updates at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The National Committees are requested to note that for this document the stability date is ....

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

Edition	Year	Changes
1	2010	Original Document
2	2019	Reformatted and revised document to create a set of requirements for asset owners to apply to their IACS.

INTRODUCTION

NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2. [13][1] The ISO/IEC Directives specify the format of this document as well as the use of terms like “shall”, “should” and “may”. The use of those terms for the requirements specified in the numbered clauses of this document use the conventions discussed in the ISO/IEC Directives, Appendix H.

This document is the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. It has been developed by Working Group 02 of the International Society of Automation (ISA) committee on Security for industrial automation and control systems, ISA99, in collaboration with Working Group 10 of the International Electrotechnical Commission (IEC) Technical Committee 65. Its requirements focus on cyber security and allow security capabilities that meet them to be provided as a combination of technical, physical and procedural measures and compensating capabilities.

Figure 1 illustrates the relationship of the different parts of IEC 62443 that have been or are being developed. Those that are normatively referenced are included in the list of normative references in clause 2. All the parts are referenced in the Bibliography for informational purposes.

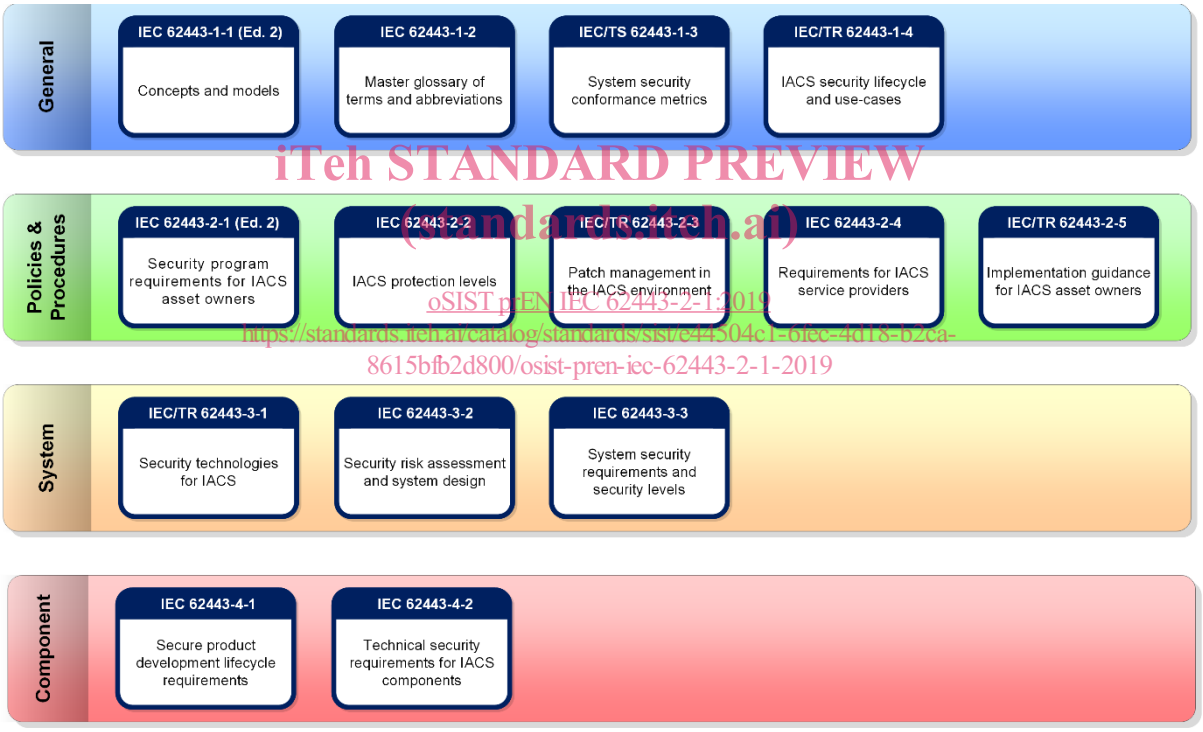

Figure 1 – Parts of the IEC 62443 Series

Cyber security is an increasingly important topic in modern organizations. The term cyber security is generally used to describe the set of countermeasures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the concern is that unwanted access or attack may result in the IACS not performing the critical functions in the required timeframe.

Industrial organizations have begun using commercial-off-the-shelf (COTS) technology developed for business systems in their IACS. Such products are often not ruggedized or

[1] Numbers in square brackets refer to the Bibliography.

rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the health, safety and environment (HSE) of the plant and the minimization of the operational and business impact on plant operation.

Some organizations may attempt to use pre-existing IT and business cyber security solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent and undesired consequences.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cyber security risks with IACS. However, a frequent mistake is to deal with cyber security one system at a time. Cyber security is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system may require a cultural change within the organization.

Addressing cyber security on an organization-wide basis may seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

All situations will be different. In some situations, the risk may be related to HSE factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cyber security for an IACS by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [9] describes a standard methodology for addressing cyber security risks in an IACS system design and can assist in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Asset owners may wish to apply their IACS SP across the organization to address the organization's needs and objectives, security requirements, business and work processes, as well as the organization's size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization's supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

1 Scope

IEC 62443-2-1 specifies asset owner security program (SP) requirements for an industrial automation and control system (IACS). This document uses the broad definition and scope of what constitutes an IACS as described in IEC 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for a legacy system may address only a subset of the requirements defined in this document. For example, if its software is no longer supported, security patching requirements cannot be met. Similarly, backup software for older systems may not be available for all components of the IACS. As a result, this document recognizes that not all requirements can be met by legacy systems. In situations where specific requirements or subsets of requirements are applicable but unable to be implemented in legacy systems, then compensating countermeasures should be implemented where possible.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with wireless technology or safety systems will not apply to IACSs that do not include wireless technology or safety systems technology. Similarly, malware protection requirements may not all apply to systems for which anti-malware software is not available for any of their devices. Therefore, the asset owner should identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

Figure 2 illustrates the security capabilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the functional capabilities necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [6] and technical security capabilities defined in IEC 62443-3-3 [10] and IEC 62443-4-2 [12].