

INTERNATIONAL STANDARD



**Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security
program**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

INTERNATIONAL STANDARD



**Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security
program**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XG**

ICS 25.040.40; 33.040

ISBN 978-2-88912-206-6

CONTENTS

| | |
|---|-----|
| FOREWORD..... | 5 |
| 0 INTRODUCTION | 7 |
| 0.1 Overview..... | 7 |
| 0.2 A cyber security management system for IACS | 7 |
| 0.3 Relationship between this document and ISO/IEC 17799 and ISO/IEC 27001..... | 7 |
| 1 Scope..... | 9 |
| 2 Normative references..... | 9 |
| 3 Terms, definitions, abbreviated terms, acronyms, and conventions | 9 |
| 3.1 Terms and definitions | 9 |
| 3.2 Abbreviated terms and acronyms..... | 14 |
| 3.3 Conventions | 16 |
| 4 Elements of a cyber security management system | 16 |
| 4.1 Overview..... | 16 |
| 4.2 Category: Risk analysis | 18 |
| 4.2.1 Description of category | 18 |
| 4.2.2 Element: Business rationale | 18 |
| 4.2.3 Element: Risk identification, classification and assessment | 18 |
| 4.3 Category: Addressing risk with the CSMS..... | 20 |
| 4.3.1 Description of category | 20 |
| 4.3.2 Element group: Security policy, organization and awareness | 20 |
| 4.3.3 Element group: Selected security countermeasures | 25 |
| 4.3.4 Element group: Implementation | 32 |
| 4.4 Category: Monitoring and improving the CSMS | 36 |
| 4.4.1 Description of category | 36 |
| 4.4.2 Element: Conformance | 36 |
| 4.4.3 Element: Review, improve and maintain the CSMS..... | 37 |
| Annex A (informative) Guidance for developing the elements of a CSMS..... | 39 |
| Annex B (informative) Process to develop a CSMS | 140 |
| Annex C (informative) Mapping of requirements to ISO/IEC 27001 | 148 |
| Bibliography..... | 156 |
| Figure 1 – Graphical view of elements of a cyber security management system | 17 |
| Figure 2 – Graphical view of category: Risk analysis..... | 18 |
| Figure 3 – Graphical view of element group: Security policy, organization and awareness | 20 |
| Figure 4 – Graphical view of element group: Selected security countermeasures | 25 |
| Figure 5 – Graphical view of element group: Implementation..... | 32 |
| Figure 6 – Graphical view of category: Monitoring and improving the CSMS | 36 |
| Figure A.1 – Graphical view of elements of a cyber security management system | 40 |
| Figure A.2 – Graphical view of category: Risk analysis..... | 40 |
| Figure A.3 – Reported attacks on computer systems through 2004 (source: CERT)..... | 44 |
| Figure A.4 – Sample logical IACS data collection sheet..... | 57 |
| Figure A.5 – Example of a graphically rich logical network diagram | 59 |

| | |
|--|-----|
| Figure A.6 – Graphical view of element group: Security policy, organization, and awareness | 66 |
| Figure A.7 – Graphical view of element group: Selected security countermeasures | 82 |
| Figure A.8 – Reference architecture alignment with an example segmented architecture | 90 |
| Figure A.9 – Reference SCADA architecture alignment with an example segmented architecture | 93 |
| Figure A.10 – Access control: Account administration | 95 |
| Figure A.11 – Access control: Authentication..... | 98 |
| Figure A.12 – Access control: Authorization | 103 |
| Figure A.13 – Graphical view of element group: Implementation..... | 106 |
| Figure A.14 – Security level lifecycle model: Assess phase..... | 109 |
| Figure A.15 – Corporate security zone template architecture..... | 112 |
| Figure A.16 – Security zones for an example IACS | 113 |
| Figure A.17 – Security level lifecycle model: Develop and implement phase | 116 |
| Figure A.18 – Security level lifecycle model: Maintain phase..... | 120 |
| Figure A.19 – Graphical view of category: Monitoring and improving the CSMS | 133 |
| Figure B.1 – Top level activities for establishing a CSMS..... | 140 |
| Figure B.2 – Activities and dependencies for activity: Initiate CSMS program..... | 142 |
| Figure B.3 – Activities and dependencies for activity: High-level risk assessment..... | 143 |
| Figure B.4 – Activities and dependencies for activity: Detailed risk assessment | 144 |
| Figure B.5 – Activities and dependencies for activity: Establish security policy, organization and awareness | 144 |
| Figure B.6 – Training and assignment of organization responsibilities..... | 145 |
| Figure B.7 – Activities and dependencies for activity: Select and implement countermeasures..... | 146 |
| Figure B.8 – Activities and dependencies for activity: Maintain the CSMS | 147 |
| Table 1 – Business rationale: Requirements..... | 18 |
| Table 2 – Risk identification, classification and assessment: Requirements | 19 |
| Table 3 – CSMS scope: Requirements..... | 21 |
| Table 4 – Organizing for security: Requirements..... | 22 |
| Table 5 – Staff training and security awareness: Requirements | 22 |
| Table 6 – Business continuity plan: Requirements | 23 |
| Table 7 – Security policies and procedures: Requirements | 24 |
| Table 8 – Personnel security: Requirements..... | 26 |
| Table 9 – Physical and environmental security: Requirements..... | 27 |
| Table 10 – Network segmentation: Requirements | 28 |
| Table 11 – Access control – Account administration: Requirements | 29 |
| Table 12 – Access control – Authentication: Requirements | 30 |
| Table 13 – Access control – Authorization: Requirements..... | 31 |
| Table 14 – Risk management and implementation: Requirements..... | 33 |
| Table 15 – System development and maintenance: Requirements..... | 33 |
| Table 16 – Information and document management: Requirements | 34 |
| Table 17 – Incident planning and response: Requirements | 35 |

| | |
|---|-----|
| Table 18 – Conformance: Requirements | 37 |
| Table 19 – Review, improve and maintain the CSMS: Requirements..... | 38 |
| Table A.1 – Typical likelihood scale..... | 52 |
| Table A.2 – Typical consequence scale | 54 |
| Table A.3 – Typical risk level matrix | 55 |
| Table A.4 – Example countermeasures and practices based on IACS risk levels..... | 107 |
| Table A.5 – Example IACS asset table with assessment results | 110 |
| Table A.6 – Example IACS asset table with assessment results and risk levels..... | 110 |
| Table A.7 – Target security levels for an example IACS..... | 114 |
| Table C.1 – Mapping of requirements in this standard to ISO/IEC 27001 references..... | 148 |
| Table C.2 – Mapping of ISO/IEC 27001 requirements to this standard | 152 |

This document is a preview generated by EVS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
NETWORK AND SYSTEM SECURITY –****Part 2-1: Establishing an industrial automation
and control system security program**

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 IEC technical committee 65: Industrial-process measurement, control and automation.

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

| FDIS | Report on voting |
|-------------|------------------|
| 65/457/FDIS | 65/461/RVD |

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

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

A list of all existing parts of IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website. The full list of existing and intended parts can also be found in the Bibliography of this standard.

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

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

A bilingual version of this publication may be issued at a later date.

NOTE The revision of this international standard will be initiated shortly after this standard is published. The next revision will be aligned more closely with ISO/IEC 27001, which addresses many of the same issues but without consideration of the specialized requirements for continuous operation and safety that are common in the industrial automation and control systems environment.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

0 INTRODUCTION

0.1 Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established cyber security management systems (CSMS) in place as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (see ISO/IEC 17799 [23]¹ and ISO/IEC 27001 [24]). These management systems provide an organization with a well-established method for protecting its assets from cyber attacks.

Industrial automation and control system (IACS) organizations have begun using commercial off the shelf (COTS) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the IACS equipment. These systems are not usually as robust, in the IACS environment, as are systems designed specifically as IACS at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the 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 consequences.

0.2 A cyber security management system for IACS

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. This standard addresses the aspects of the elements included in a CSMS for IACS and also provides guidance on how to go about developing the CSMS for IACS.

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 made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that needs to address the entire set of IACS 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 can seem like a daunting task. Unfortunately there is no simple cookbook for security. There is good reason for this. There is not 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 really 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 cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799 [23] and ISO/IEC 27001 [24] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to IACS as well. This standard emphasizes the need

1 Numbers in square brackets refer to the Bibliography.

for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this standard are encouraged to read ISO/IEC 17799 and ISO/IEC 27001 for additional supporting information. This standard builds on the guidance in these ISO/IEC standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS may have HSE implications and should be integrated with other existing risk management practices addressing these risks.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 2-1: Establishing an industrial automation and control system security program

1 Scope

This part of IEC 62443 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1.

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

NOTE 1 Other documents in the IEC 62443 series and in the Bibliography discuss specific technologies and/or solutions for cyber security in more detail.

The guidance provided on how to develop a CSMS is an example. It represents the author's opinion on how an organization could go about developing the elements and may not work in all situations. The users of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning CSMS for an organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE 2 There may be cases where a pre-existing CSMS is in place and the IACS portion is being added or there may be some organizations that have never formally created a CSMS at all. The authors of this standard cannot anticipate all cases where an organization will be establishing a CSMS for the IACS environment, so this standard does not attempt to create a solution for all cases.

2 Normative references

The following referenced documents are indispensable for the application 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.

IEC/TS 62443-1-12 – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62443-1-1 and the following apply.

² This standard is derived from ANSI/ISA 99.02.01:2009 and wholly replaces it for international use. It is intended that the second edition of IEC/TS 62443-1-1 be an International Standard, not a TS, after inclusion of some normative requirements to which conformance is possible.