SS IEC 62443-2-1 : 2018
IEC 62443-2-1:2010, IDT
(ICS 25.040.40; 35.100.05)

SINGAPORE STANDARD

Industrial communication networks – Network and system security –

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

Published by
Enterprise Singapore

SS IEC 62443-2-1 : 2018
IEC 62443-2-1:2010, IDT
(ICS 25.040.40; 35.100.05)

SINGAPORE STANDARD

Industrial communication networks – Network and system security –

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

ISBN 978-981-48-3536-7

This Singapore Standard was approved on 15 November 2018 by the Manufacturing Standards Committee under the purview of the Singapore Standards Council.

First published, 2019.

The Manufacturing Standards Committee, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Dr John Yong	*Individual Capacity*
Deputy Chairman	:	Mr Brandon Lee	*Individual Capacity*
Secretary	:	Mr Lee Weiguo	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Ms Fong Pin Fen	*Singapore Economic Development Board*
		Mr Goh Wee Hong	*TÜV SÜD PSB Pte Ltd*
		Mr Ho Chi Bao	*Enterprise Singapore*
		Mr Steven Koh	*Singapore Precision Engineering and Technology Association*
		Ms Lee Wan Sie	*Info-comm Media Development Authority*
		Dr Jim Li Hui Hong	*Individual Capacity*
		Dr Lim Ee Meng	*National Metrology Centre*
		Mr Loh Wai Mun	*Science and Engineering Research Council*
		Er. Prof Seeram Ramakrishan	*The Institution of Engineers, Singapore*

The Technical Committee on Smart Manufacturing, appointed by the Manufacturing Standards Committee, consists of representatives from the following organisations:

		Name	Organisation
Co-Chairmen	:	Mr Yeoh Pit Wee	*Individual Capacity*
		Dr Tan Puay Siew	*Individual Capacity*
Secretary	:	Mr Louis Lauw	*Singapore Manufacturing Federation – Standards Development Organisation*
Members	:	Dr Ian Chan Hian Leng	*Singapore Institute of Manufacturing Technology*
		Mr Cheong Siah Chong	*Singapore Industrial Automation Association*
		Mr David Chia	*Beckhoff Automation Pte Ltd (Southeast Asia)*
		Dr Andreas Hauser	*TÜV SÜD Asia Pacific Pte Ltd*
		Mr Phil Kay	*SP Manufacturing Pte Ltd*
		Mr Sunny Khoo	*Toshiba Tec Singapore Pte Ltd*
		Dr Lai Weng Hong	*Singapore Semiconductor Industry Association*
		Mr Brandon Lee	*Singapore Manufacturing Federation*
		Mr Francis Lee	*TRUMPF Pte Ltd*

	Name	Organisation
Members :	Prof Lee Loo Hay	*National University of Singapore*
	Mr Zach Lee	*Siemens*
	Mr Gerry Ong	*SMT Technology Pte Ltd*
	Prof John Pang	*Nanyang Technological University*
	Er. Prof Seeram Ramakrishan	*The Institution of Engineers, Singapore*
	Mr Sim Bak Chor	*Infocomm Media Development Authority*
	Mr Brian Teo	*PBA Systems Pte Ltd*
	Mr Stuart Wong	*Advanced Remanufacturing and Technology Centre*

The Working Group on Cyber Security for Industrial Automation, appointed by the Technical Committee on Smart Manufacturing to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

	Name
Co-Convenors :	Dr Andreas Hauser
	Mr Lim Thian Chin
Secretary :	Mr Louis Lauw
Members :	Mr Willie Lui Tien Heong
	Mr Thomas Quek
	Mr Sherkar Suhas Laxman
	Mr Henry Tan
	Mr William Temple
	Dr Vrizlynn Thing
	Mr Vishram Mishra
	Mr Timothy Yong
	Mr Bobby Zhou WenBo

The organisations in which experts of the Working Group are involved are:

Advanced Digital Sciences Center
Cyber Security Agency of Singapore
Huawei International Pte Ltd
Infineon Technologies Asia Pacific Pte Ltd
Institute for Infocomm Research
MicroSec Pte Ltd
REDCON Security Advisors LLP
Temasek Polytechnic
TÜV SÜD Asia Pacific Pte Ltd

(blank page)

CONTENTS

National Foreword

This Singapore Standard was prepared by the Working Group on Cyber Security for Industrial Automation appointed by the Technical Committee on Smart Manufacturing under the purview of the Manufacturing Standards Committee.

This standard is identical with IEC 62443-2-1:2010, “Industrial communication network – Network and system security – Part 2-1 : Establishing an industrial automation and control system security program”, published by the International Electrotechnical Commission.

Where reference to a particular part of IEC 62443 is made, the appropriate Singapore Standard (which is an identical adoption of that part of IEC 62443) shall apply.

This standard is expected to be used by asset owners who can provide references to product suppliers and system integrators.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

`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.

This bilingual version (2012-04) corresponds to the monolingual English version, published in 2010-11.

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.

The French version of this standard has not been voted upon.

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.

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.

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

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 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 62443‑1‑1[2] – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[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.