Singapore Standards Council

TR IEC/TS 62443-1-1 : 2018

IEC/TS 62443-1-1:2009, IDT

(ICS 25.040.40; 33.040.040; 35.040.01)

TECHNICAL REFERENCE

Industrial communication networks – Network and system security –

Part 1-1 : Terminology, concepts and models

Published by

Enterprise Singapore

TR IEC/TS 62443-1-1 : 2018
IEC/TS 62443-1-1:2009, IDT
(ICS 25.040.40; 33.040.040; 35.040.01)

TECHNICAL REFERENCE

Industrial communication networks – Network and system security –

Part 1-1 : Terminology, concepts and models

ISBN 978-981-48-3522-0

This Technical Reference was approved on 15 October 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 Technical Reference 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 TS 62443-1-1:2009, “Industrial communication networks – Network and system security – Part 1-1 : Terminology, concepts and models”, published by the International Electrotechnical Commission.

This Technical Reference is expected to be used by asset owners, product suppliers and system integrators.

Attention is drawn to the possibility that some of the elements of this Technical Reference 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 1-1: Terminology, concepts and models

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62443-1-1, which is a technical specification, has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This technical specification is derived from the corresponding US ANSI/S99.01.01 standard.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
65/423/DTS	65/432A/RVC

Full information on the voting for the approval of this technical specification 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 parts of the IEC 62433 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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

- transformed into an International standard,
- 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 technical specification will be synchronized with the other parts of the IEC 62443 series.

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 publication using a colour printer.

INTRODUCTION

The subject of this technical specification is security for industrial automation and control systems. In order to address a range of applications (i.e., industry types), each of the terms in this description have been interpreted very broadly.

The term “Industrial Automation and Control Systems” (IACS), includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

The term “security” is considered here to mean the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in IACS. Cybersecurity which is the particular focus of this technical specification, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

The audience for this technical specification includes all users of IACS (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, government organizations involved with, or affected by, control system cybersecurity, control system practitioners, and security practitioners. Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this technical specification is also a reference for those responsible for the integration of IACS and enterprise networks.

Typical questions addressed by this technical specification include:

a) What is the general scope of application for IACS security?

b) How can the needs and requirements of a security system be defined using consistent terminology?

c) What are the basic concepts that form the foundation for further analysis of the activities, system attributes, and actions that are important to provide electronically secure control systems?

d) How can the components of an IACS be grouped or classified for the purpose of defining and managing security?

e) What are the different cybersecurity objectives for control system applications?

f) How can these objectives be established and codified?

Each of these questions is addressed in detail in subsequent clauses of this technical specification.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 1-1: Terminology, concepts and models

1 Scope

1.1 General

This part of the IEC 62443 series is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.

To fully articulate the systems and components the IEC 62443 series address, the range of coverage may be defined and understood from several perspectives, including the following:

a) range of included functionality;

b) specific systems and interfaces;

c) criteria for selecting included activities;

d) criteria for selecting included assets.

Each of these is described in the following subclauses:

1.2 Included functionality

The scope of this technical specification can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

This technical specification focuses primarily on industrial automation and control, as described in a reference model (see Clause 6). Business planning and logistics systems are not explicitly addressed within the scope of this technical specification, although the integrity of data exchanged between business and industrial systems is considered.

Industrial automation and control includes the supervisory control components typically found in process industries. It also includes SCADA (Supervisory Control and Data Acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include the following:

a) electricity transmission and distribution;

b) gas and water distribution networks;

c) oil and gas production operations;

d) gas and liquid transmission pipelines.

This is not an exclusive list. SCADA systems may also be found in other critical and non-critical infrastructure industries.

1.3 Systems and interfaces

In encompassing all IACS, this technical specification covers systems that can affect or influence the safe, secure, and reliable operation of industrial processes. They include, but are not limited to:

a) Industrial control systems and their associated communications networks[1], including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. (In this context, industrial control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.)

b) Associated systems at level 3 or below of the reference model described in Clause 6. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, pipeline leak detection systems, work management, outage management, and electricity energy management systems.

c) Associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

1.4 Activity-based criteria

IEC 62443-2-1[2] provides criteria for defining activities associated with manufacturing operations. A similar list has been developed for determining the scope of this technical specification. A system should be considered to be within the range of coverage of the IEC 62443 series if the activity it performs is necessary for any of the following:

a) predictable operation of the process;

b) process or personnel safety;

c) process reliability or availability;

d) process efficiency;

e) process operability;

f) product quality;

g) environmental protection;

h) regulatory compliance;

i) product sales or custody transfer.

1.5 Asset-based criteria

The coverage of this technical specification includes those systems in assets that meet any of the following criteria, or whose security is essential to the protection of other assets that meet these criteria:

a) The asset has economic value to a manufacturing or operating process.

---

[1] The term “communications networks” includes all types of communications media, including various types of wireless communications. A detailed description of the use of wireless communications in industrial automation systems is beyond the scope of this technical specification. Wireless communication techniques are specifically mentioned only in situations where their use or application may change the nature of the security applied or required.

[2] To be published.

b) The asset performs a function necessary to operation of a manufacturing or operating process.

c) The asset represents intellectual property of a manufacturing or operating process.

d) The asset is necessary to operate and maintain security for a manufacturing or operating process.

e) The asset is necessary to protect personnel, contractors, and visitors involved in a manufacturing or operating process.

f) The asset is necessary to protect the environment.

g) The asset is necessary to protect the public from events caused by a manufacturing or operating process.

h) The asset is a legal requirement, especially for security purposes of a manufacturing or operating process.

i) The asset is needed for disaster recovery.

j) The asset is needed for logging security events.

This range of coverage includes systems whose compromise could result in the endangerment of public or employees health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, environmental contamination, and/or economic loss or impact on an entity or on local or national security.

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 62264-1, *Enterprise-control system integration – Part 1: Models and terminology*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*