

TECHNICAL REFERENCE**Industrial communication networks – Network
and system security –**

Part 3-1 : Security technologies for industrial automation
and control systems

Published by

 **Enterprise
Singapore**

TR IEC/TR 62443-3-1 : 2018
IEC/TR 62443-3-1:2009, IDT
(ICS 25.040.40; 35.040.40; 35.100.05)

TECHNICAL REFERENCE

**Industrial communication networks – Network and
system security –**

Part 3-1 : Security technologies for industrial automation and control systems

All rights reserved. Unless otherwise specified, no part of this Technical Reference may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: standards@enterprisesg.gov.sg.

© IEC 2009 – All rights reserved
© Enterprise Singapore 2018

ISBN 978-981-48-3524-4

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

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

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

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

CONTENTS

NATIONAL FOREWORD	12
FOREWORD	13
INTRODUCTION	15
1 Scope	17
2 Normative references	18
3 Terms, definitions and acronyms	18
3.1 Terms and definitions	18
3.2 Acronyms	25
4 Overview	27
5 Authentication and authorization technologies	28
5.1 General	28
5.2 Role-based authorization tools	29
5.2.1 Overview	29
5.2.2 Security vulnerabilities addressed by this technology	29
5.2.3 Typical deployment	30
5.2.4 Known issues and weaknesses	30
5.2.5 Assessment of use in the industrial automation and control systems environment	31
5.2.6 Future directions	31
5.2.7 Recommendations and guidance	31
5.2.8 Information sources and reference material	31
5.3 Password authentication	31
5.3.1 Overview	31
5.3.2 Security vulnerabilities addressed by this technology	32
5.3.3 Typical deployment	32
5.3.4 Known issues and weaknesses	32
5.3.5 Assessment of use in the industrial automation and control systems environment	33
5.3.6 Future directions	33
5.3.7 Recommendations and guidance	34
5.3.8 Information sources and reference material	34
5.4 Challenge/response authentication	35
5.4.1 Overview	35
5.4.2 Security vulnerabilities addressed by this technology	35
5.4.3 Typical deployment	35
5.4.4 Known issues and weaknesses	35
5.4.5 Assessment of use in the industrial automation and control systems environment	36
5.4.6 Future directions	36
5.4.7 Recommendations and guidance	36
5.4.8 Information sources and reference material	36
5.5 Physical/token authentication	36
5.5.1 Overview	36
5.5.2 Security vulnerabilities addressed by this technology	37

5.5.3	Typical deployment	37
5.5.4	Known issues and weaknesses	37
5.5.5	Assessment of use in the industrial automation and control systems environment	37
5.5.6	Future directions	37
5.5.7	Recommendations and guidance	38
5.5.8	Information sources and reference material	38
5.6	Smart card authentication	38
5.6.1	Overview	38
5.6.2	Security vulnerabilities addressed by this technology	38
5.6.3	Typical deployment	39
5.6.4	Known issues and weaknesses	39
5.6.5	Assessment of use in the industrial automation and control systems environment	40
5.6.6	Future directions	40
5.6.7	Recommendations and guidance	40
5.6.8	Information sources and reference material	40
5.7	Biometric authentication	40
5.7.1	Overview	40
5.7.2	Security vulnerabilities addressed by this technology	40
5.7.3	Typical deployment	41
5.7.4	Known issues and weaknesses	41
5.7.5	Assessment of use in the industrial automation and control systems environment	41
5.7.6	Future directions	41
5.7.7	Recommendations and guidance	42
5.7.8	Information sources and reference material	42
5.8	Location-based authentication	42
5.8.1	Overview	42
5.8.2	Security vulnerabilities addressed by this technology	42
5.8.3	Typical deployment	43
5.8.4	Known issues and weaknesses	43
5.8.5	Assessment of use in the industrial automation and control systems environment	43
5.8.6	Future directions	43
5.8.7	Recommendations and guidance	43
5.8.8	Information sources and reference material	43
5.9	Password distribution and management technologies	44
5.9.1	Overview	44
5.9.2	Security vulnerabilities addressed by this technology	44
5.9.3	Typical deployment	44
5.9.4	Known issues and weaknesses	44
5.9.5	Assessment of use in the industrial automation and control systems environment	45
5.9.6	Future directions	45
5.9.7	Recommendations and guidance	46
5.9.8	Information sources and reference material	46

5.10	Device-to-device authentication	46
5.10.1	Overview	46
5.10.2	Security vulnerabilities addressed by this technology.....	47
5.10.3	Typical deployment.....	47
5.10.4	Known issues and weaknesses	47
5.10.5	Assessment of use in the industrial automation and control systems environment	47
5.10.6	Future directions	48
5.10.7	Recommendations and guidance	48
5.10.8	Information sources and reference material	48
6	Filtering/blocking/access control technologies	48
6.1	General.....	48
6.2	Network firewalls	48
6.2.1	Overview	48
6.2.2	Security vulnerabilities addressed by this technology.....	49
6.2.3	Typical deployment.....	50
6.2.4	Known issues and weaknesses	50
6.2.5	Assessment of use in the industrial automation and control systems environment	50
6.2.6	Future directions	51
6.2.7	Recommendations and guidance	51
6.2.8	Information sources and reference material	51
6.3	Host-based firewalls	52
6.3.1	Overview	52
6.3.2	Security vulnerabilities addressed by this technology.....	52
6.3.3	Typical deployment.....	53
6.3.4	Known issues and weaknesses	53
6.3.5	Assessment of use in the industrial automation and control systems environment	53
6.3.6	Future directions	54
6.3.7	Recommendations and guidance	54
6.3.8	Information sources and reference material	54
6.4	Virtual Networks	55
6.4.1	Overview	55
6.4.2	Security vulnerabilities addressed by this technology.....	55
6.4.3	Known issues and weaknesses	55
6.4.4	Assessment of use in the industrial automation and control systems environment	55
6.4.5	Future directions	56
6.4.6	Recommendations and guidance	56
6.4.7	Information sources and reference material	56
7	Encryption technologies and data validation	56
7.1	General.....	56
7.2	Symmetric (secret) key encryption	56
7.2.1	Overview	56
7.2.2	Security vulnerabilities addressed by this technology.....	58
7.2.3	Typical deployment.....	58

7.2.4	Known issues and weaknesses	58
7.2.5	Assessment of use in the industrial automation and control systems environment	59
7.2.6	Future directions	59
7.2.7	Recommendations and guidance	59
7.2.8	Information sources and reference material	60
7.3	Public key encryption and key distribution	61
7.3.1	Overview	61
7.3.2	Security vulnerabilities addressed by this technology.....	61
7.3.3	Typical deployment.....	62
7.3.4	Known issues and weaknesses	62
7.3.5	Assessment of use in the industrial automation and control systems environment	62
7.3.6	Future directions	63
7.3.7	Problems of encryption usage	63
7.3.8	Information sources and reference material	64
7.4	Virtual private networks (VPNs)	64
7.4.1	Overview	64
7.4.2	Security vulnerabilities addressed by this technology.....	64
7.4.3	Typical deployment.....	65
7.4.4	Known issues and weaknesses	67
7.4.5	Assessment of use in the industrial automation and control systems environment	68
7.4.6	Future directions	68
7.4.7	Recommendations and guidance	68
7.4.8	Information sources and reference material	68
8	Management, audit, measurement, monitoring, and detection tools	69
8.1	General.....	69
8.2	Log auditing utilities.....	69
8.2.1	Overview	69
8.2.2	Security vulnerabilities addressed by this technology.....	70
8.2.3	Typical deployment.....	71
8.2.4	Known issues and weaknesses	71
8.2.5	Assessment of use in the industrial automation and control systems environment	71
8.2.6	Future directions	71
8.2.7	Recommendations and guidance	71
8.2.8	Information sources and reference material	72
8.3	Virus and malicious code detection systems	72
8.3.1	Security vulnerabilities addressed by this technology.....	73
8.3.2	Typical deployment.....	73
8.3.3	Known issues and weaknesses	73
8.3.4	Assessment of use in the industrial automation and control systems environment	73
8.3.5	Cost range	74
8.3.6	Future directions	74
8.3.7	Recommendations and guidance	74

8.3.8	Information sources and reference material	74
8.4	Intrusion detection systems (IDS)	74
8.4.1	Overview	74
8.4.2	Security vulnerabilities addressed by this technology.....	75
8.4.3	Typical deployment.....	75
8.4.4	Known issues and weaknesses	76
8.4.5	Assessment of use in the industrial automation and control systems environment	76
8.4.6	Future directions	77
8.4.7	Recommendations and guidance	77
8.4.8	Information sources and reference material	77
8.5	Vulnerability scanners	78
8.5.1	Overview	78
8.5.2	Security vulnerabilities addressed by this technology.....	79
8.5.3	Typical deployment.....	79
8.5.4	Known issues and weaknesses	79
8.5.5	Assessment of use in the industrial automation and control systems environment	80
8.5.6	Future directions	80
8.5.7	Recommendations and guidance	80
8.5.8	Information sources and reference material	81
8.6	Forensics and analysis tools (FAT)	81
8.6.1	Overview	81
8.6.2	Security vulnerabilities addressed by this technology.....	81
8.6.3	Typical deployment.....	82
8.6.4	Known issues and weaknesses	82
8.6.5	Assessment of use in the industrial automation and control systems environment	83
8.6.6	Future directions	83
8.6.7	Recommendations and guidance	83
8.6.8	Information sources and reference material	83
8.7	Host configuration management tools (HCM)	84
8.7.1	Overview	84
8.7.2	Security vulnerabilities addressed by this technology.....	84
8.7.3	Typical deployment.....	84
8.7.4	Known issues and weaknesses	84
8.7.5	Assessment of use in the industrial automation and control systems environment	85
8.7.6	Future directions	85
8.7.7	Recommendations and guidance	85
8.7.8	Information sources and reference material	85
8.8	Automated software management tools (ASM).....	86
8.8.1	Overview	86
8.8.2	Security vulnerabilities addressed by this technology.....	86
8.8.3	Typical deployment.....	87
8.8.4	Known issues and weaknesses	87

8.8.5	Assessment of use in the industrial automation and control systems environment	87
8.8.6	Future directions	88
8.8.7	Recommendations and guidance	88
8.8.8	Information sources and reference material	88
9	Industrial automation and control systems computer software	88
9.1	General.....	88
9.2	Server and workstation operating systems	89
9.2.1	Overview	89
9.2.2	Security vulnerabilities addressed by this technology.....	89
9.2.3	Typical deployment.....	89
9.2.4	Known issues and weaknesses	89
9.2.5	Assessment of use in the industrial automation and control systems environment	90
9.2.6	Future directions	90
9.2.7	Recommendations and guidance	90
9.2.8	Information sources and reference material	91
9.3	Real-time and embedded operating systems.....	91
9.3.1	Overview	91
9.3.2	Security vulnerabilities addressed by this technology.....	91
9.3.3	Typical deployment.....	91
9.3.4	Known issues and weaknesses	92
9.3.5	Assessment of use in the industrial automation and control systems environment	92
9.3.6	Future directions	92
9.3.7	Recommendations and guidance	93
9.3.8	Information sources and reference material	93
9.4	Web technologies.....	93
9.4.1	Overview	93
9.4.2	Security vulnerabilities addressed by this technology.....	93
9.4.3	Typical deployment.....	93
9.4.4	Known issues and weaknesses	93
9.4.5	Assessment of use in the industrial automation and control systems environment	94
9.4.6	Future directions	94
9.4.7	Recommendations and guidance	94
9.4.8	Information sources and reference material	94
10	Physical security controls	94
10.1	General.....	94
10.2	Physical protection	95
10.2.1	Security vulnerabilities addressed by this technology.....	95
10.2.2	Typical deployment.....	96
10.2.3	Known issues and weaknesses	96
10.2.4	Assessment of use in the industrial automation and control systems environment	97
10.2.5	Future directions	97
10.2.6	Recommendations and guidance	97

10.2.7	Information sources and reference material	98
10.3	Personnel security.....	98
10.3.1	Overview	98
10.3.2	Security vulnerabilities addressed by this technology.....	99
10.3.3	Typical deployment.....	99
10.3.4	Known issues and weaknesses	100
10.3.5	Assessment of use in the industrial automation and control systems environment	100
10.3.6	Future directions	101
10.3.7	Recommendations and guidance	101
10.3.8	Information sources and reference material	102
Annex A (informative)	Trade name declarations	103
Bibliography.....		107
Figure 1 – Firewall zone separation		49
Figure 2 – Security gateway to security gateway VPN		65
Figure 3 – Host to security gateway VPN.....		66
Figure 4 – Host to host gateway VPN		66

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 TR 62443-3-1:2009, "Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems", 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 3-1: Security technologies for industrial automation
and control systems**

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. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62443-3-1, which is a technical report, has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This technical report is closely related to ANSI/ISA-TR99.03.01-2007.

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

Enquiry draft	Report on voting
65/424/DTR	65/431A/RVC

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

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

A list of all 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 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:

- 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 report 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 need for protecting Industrial Automation and Control System (IACS) computer environments from malicious cyberintrusions has grown significantly over the last decade. The combination of the increased use of open systems, platforms, and protocols in the IACS environment, along with an increase in joint ventures, alliance partners and outsourcing, has lead to increased threats and a higher probability of cyberattacks. As these threats and vulnerabilities increase, the risk of a cyberattack on an industrial communication network correspondingly increases, as well as the need for protection of computer and networked-based information sharing and analysis centres. Additionally, the growth in intelligent equipment and embedded systems; increased connectivity to computer and networked equipment and software; and enhanced external connectivity coupled with rapidly increasing incidents of network intrusion, more intelligent hackers, and malicious yet easily accessible software, all add to the risk as well.

There are numerous electronic security technologies and cyberintrusion countermeasures potentially available to the IACS environment. This technical report addresses several categories of cybersecurity technologies and countermeasure techniques and discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for their deployment, and their known strengths and weaknesses. Additionally, guidance is provided for using the various categories of security technologies and countermeasure techniques for mitigation of the above-mentioned increased risks.

This technical report does not make recommendations of one cybersecurity technology or mitigation method over others, but provides suggestions and guidance for using the technologies and methods, as well as information to consider when developing a site or corporate cybersecurity policy, program and procedures for the IACS environment.

The responsible standards development working group intends to update this technical report periodically to reflect new information, cybersecurity technologies, countermeasures, and cyberrisk mitigation methods. The committee cautions the reader that following the recommended guidance in this report will not necessarily ensure that optimized cybersecurity is attained for the reader's industrial automation or control systems environment. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired cyberintrusions that could compromise confidential information or, even worse, cause human and environmental harm, as well as disruption or failure of the industrial network or control systems and the industry and infrastructure critical assets they monitor and regulate.

This technical report provides an evaluation and assessment of many current types of electronic-based cybersecurity technologies, mitigation methods and tools that may apply to protecting the IACS environment from detrimental cyberintrusions and attacks. For the various technologies, methods and tools introduced in this report, a discussion of their development, implementation, operations, maintenance, engineering and other user services is provided. The report also provides guidance to manufacturers, vendors, and security practitioners at end-user companies, facilities, and industries on the technological options and countermeasures for securing automated IACSs (and their associated industrial networks) against electronic (cyber) attack.

Following the recommended guidance given in this technical report will not necessarily ensure that optimized cybersecurity is attained for IACSs. It will, however, help to identify and address vulnerabilities, and to reduce the risk of undesired intrusions that could compromise confidential information or cause disruption or failure of control systems and the critical infrastructure assets they automate and control. Of more concern, use of the recommendations may aid in reducing the risk of any human or environmental harm that may result after the cyber compromise of an automated control system or its associated industrial network.

The cybersecurity guidance presented in this document is general in nature, and should be applied to each control system or network as appropriate by personnel knowledgeable in those specific industrial automation or control systems to which it is being applied. The guidance identifies those activities and actions that are typically important to provide cybersecure control systems, but whose application is not always compatible with effective operation or maintenance of a system's functions. The guidance includes suggestions and recommendations on appropriate cybersecurity applications to specific control systems. However, selection and deployment of particular cybersecurity activities and practices for a given control system and its related industrial network is the responsibility of the system's owner.

It is intended that this guidance will mature and be modified over time, as experience is gained with control system vulnerabilities, as specific cybersecurity implementations mature, and as new control-based cybersecurity technologies become available. As such, while the general format of this guidance is expected to remain relatively stable, the specifics of its application and solutions are expected to evolve.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-1: Security technologies for industrial automation and control systems

1 Scope

This part of IEC 62443 provides a current assessment of various cybersecurity tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.

The concept of IACS cybersecurity as applied in this technical report is in the broadest possible sense, encompassing all types of components, plants, facilities, and systems in all industries and critical infrastructures. IACSs include, but are not limited to:

- Hardware (e.g., data historian servers) and software systems (e.g., operating platforms, configurations, applications) such as Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing systems, and monitoring, diagnostic, and assessment systems. Inclusive in this hardware and software domain is the essential industrial network and any connected or related information technology (IT) devices and links critical to the successful operation to the control system at large. As such, this domain also includes, but is not limited to: firewalls, servers, routers, switches, gateways, fieldbus systems, intrusion detection systems, intelligent electronic/end devices, remote terminal units (RTUs), and both wired and wireless remote modems.
- Associated internal, human, network, or machine interfaces used to provide control, data logging, diagnostics, safety, monitoring, maintenance, quality assurance, regulatory compliance, auditing and other types of operational functionality for either continuous, batch, discrete, and combined processes.

Similarly, the concept of cybersecurity technologies and countermeasures is also broadly applied in this technical report and includes, but is not limited to, the following technologies:

- authentication and authorization;
- filtering, blocking, and access control;
- encryption;
- data validation;
- auditing;
- measurement;
- monitoring and detection tools;
- operating systems.

In addition, a non-cyber technology —physical security control— is an essential requirement for some aspects of cybersecurity and is discussed in this technical report.

The purpose of this technical report is to categorize and define cybersecurity technologies, countermeasures, and tools currently available to provide a common basis for later technical reports and standards to be produced by the ISA99 committee. Each technology in this technical report is discussed in terms of:

- security vulnerabilities addressed by the technology, tool, and/or countermeasure;
- typical deployment;
- known issues and weaknesses;
- assessment of use in the IACS environment;
- future directions;
- recommendations and guidance;
- information sources and reference material.

The intent of this technical report is to document the known state of the art of cybersecurity technologies, tools, and countermeasures applicable to the IACS environment, clearly define which technologies can reasonably be deployed today, and define areas where more research may be needed.

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.

<none>

¹ Numbers in square brackets refer to the Bibliography.