

TECHNICAL REFERENCE

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

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

Confirmed 2024

TR IEC/TR 62443-3-1:2018(2024)

IEC/TR 62443-3-1:2009, IDT
(ICS 25.040.40; 33.040.40; 35.040)

TECHNICAL REFERENCE

Industrial communication networks – Network and system security

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

Published by Enterprise Singapore



**THIS PUBLICATION IS COPYRIGHT
PROTECTED**

**Copyright © 2018 Enterprise Singapore
Copyright © 2009 IEC, Geneva, Switzerland**

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from Enterprise Singapore, representing the IEC National Committee of Singapore, or the IEC. If you have any questions about the copyrights of Enterprise Singapore or the IEC or have an enquiry about obtaining additional rights to this publication, please contact Enterprise Singapore at: standards@enterprisesg.gov.sg for further information.

ISBN 978-981-48-3524-4

National Foreword

This Technical Reference (TR) was prepared by the Working Group on Cyber Security for Industrial Automation set up by the Technical Committee on Smart Manufacturing under the purview of the Manufacturing Standards Committee.

This TR is an identical adoption of 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.

Attention is drawn to the possibility that some of the elements of this TR 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. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “mature standards”. Mature standards will not be subject to further review, unless there are requests to review such standards.*
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 and the Singapore Standards Council 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. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
3. *Compliance with a SS or TR does not exempt users from any legal obligations.*



TECHNICAL REPORT



Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 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.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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

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



TECHNICAL REPORT



Industrial communication networks – Network and system security – Part 3 1: Security technologies for industrial automation and control systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XD**

ICS 25.040.40; 33.040.040; 35.040

ISBN 978-2-88910-711-7

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	12
2 Normative references	13
3 Terms, definitions and acronyms	13
3.1 Terms and definitions	13
3.2 Acronyms	19
4 Overview	21
5 Authentication and authorization technologies	22
5.1 General	22
5.2 Role-based authorization tools	23
5.2.1 Overview	23
5.2.2 Security vulnerabilities addressed by this technology	23
5.2.3 Typical deployment.....	24
5.2.4 Known issues and weaknesses.....	24
5.2.5 Assessment of use in the industrial automation and control systems environment	25
5.2.6 Future directions	25
5.2.7 Recommendations and guidance	25
5.2.8 Information sources and reference material	25
5.3 Password authentication	25
5.3.1 Overview	25
5.3.2 Security vulnerabilities addressed by this technology	26
5.3.3 Typical deployment.....	26
5.3.4 Known issues and weaknesses.....	26
5.3.5 Assessment of use in the industrial automation and control systems environment	27
5.3.6 Future directions	27
5.3.7 Recommendations and guidance	28
5.3.8 Information sources and reference material	28
5.4 Challenge/response authentication.....	28
5.4.1 Overview	28
5.4.2 Security vulnerabilities addressed by this technology	29
5.4.3 Typical deployment.....	29
5.4.4 Known issues and weaknesses.....	29
5.4.5 Assessment of use in the industrial automation and control systems environment	30
5.4.6 Future directions	30
5.4.7 Recommendations and guidance	30
5.4.8 Information sources and reference material	30
5.5 Physical/token authentication	30
5.5.1 Overview	30
5.5.2 Security vulnerabilities addressed by this technology	30
5.5.3 Typical deployment.....	31
5.5.4 Known issues and weaknesses.....	31
5.5.5 Assessment of use in the industrial automation and control systems environment	31

5.5.6	Future directions	31
5.5.7	Recommendations and guidance	31
5.5.8	Information sources and reference material	32
5.6	Smart card authentication	32
5.6.1	Overview	32
5.6.2	Security vulnerabilities addressed by this technology	32
5.6.3	Typical deployment.....	32
5.6.4	Known issues and weaknesses.....	33
5.6.5	Assessment of use in the industrial automation and control systems environment	33
5.6.6	Future directions	33
5.6.7	Recommendations and guidance	33
5.6.8	Information sources and reference material	34
5.7	Biometric authentication	34
5.7.1	Overview	34
5.7.2	Security vulnerabilities addressed by this technology	34
5.7.3	Typical deployment.....	34
5.7.4	Known issues and weaknesses.....	34
5.7.5	Assessment of use in the industrial automation and control systems environment	35
5.7.6	Future directions	35
5.7.7	Recommendations and guidance	35
5.7.8	Information sources and reference material	35
5.8	Location-based authentication	35
5.8.1	Overview	35
5.8.2	Security vulnerabilities addressed by this technology	36
5.8.3	Typical deployment.....	36
5.8.4	Known issues and weaknesses.....	36
5.8.5	Assessment of use in the industrial automation and control systems environment	36
5.8.6	Future directions	36
5.8.7	Recommendations and guidance	36
5.8.8	Information sources and reference material	37
5.9	Password distribution and management technologies	37
5.9.1	Overview	37
5.9.2	Security vulnerabilities addressed by this technology	37
5.9.3	Typical deployment.....	37
5.9.4	Known issues and weaknesses.....	37
5.9.5	Assessment of use in the industrial automation and control systems environment	38
5.9.6	Future directions	38
5.9.7	Recommendations and guidance	39
5.9.8	Information sources and reference material	39
5.10	Device-to-device authentication.....	39
5.10.1	Overview	39
5.10.2	Security vulnerabilities addressed by this technology	40
5.10.3	Typical deployment.....	40
5.10.4	Known issues and weaknesses.....	40
5.10.5	Assessment of use in the industrial automation and control systems environment	40

5.10.6	Future directions	40
5.10.7	Recommendations and guidance	41
5.10.8	Information sources and reference material	41
6	Filtering/blocking/access control technologies	41
6.1	General	41
6.2	Network firewalls	41
6.2.1	Overview	41
6.2.2	Security vulnerabilities addressed by this technology	42
6.2.3	Typical deployment.....	43
6.2.4	Known issues and weaknesses.....	43
6.2.5	Assessment of use in the industrial automation and control systems environment	43
6.2.6	Future directions	43
6.2.7	Recommendations and guidance	44
6.2.8	Information sources and reference material	44
6.3	Host-based firewalls	45
6.3.1	Overview	45
6.3.2	Security vulnerabilities addressed by this technology	45
6.3.3	Typical deployment.....	45
6.3.4	Known issues and weaknesses.....	45
6.3.5	Assessment of use in the industrial automation and control systems environment	46
6.3.6	Future directions	46
6.3.7	Recommendations and guidance	46
6.3.8	Information sources and reference material	47
6.4	Virtual Networks	47
6.4.1	Overview	47
6.4.2	Security vulnerabilities addressed by this technology	48
6.4.3	Known issues and weaknesses.....	48
6.4.4	Assessment of use in the industrial automation and control systems environment	48
6.4.5	Future directions	48
6.4.6	Recommendations and guidance	48
6.4.7	Information sources and reference material	48
7	Encryption technologies and data validation	49
7.1	General.....	49
7.2	Symmetric (secret) key encryption.....	49
7.2.1	Overview	49
7.2.2	Security vulnerabilities addressed by this technology	50
7.2.3	Typical deployment.....	50
7.2.4	Known issues and weaknesses.....	50
7.2.5	Assessment of use in the industrial automation and control systems environment	51
7.2.6	Future directions	51
7.2.7	Recommendations and guidance	52
7.2.8	Information sources and reference material	52
7.3	Public key encryption and key distribution	53
7.3.1	Overview	53
7.3.2	Security vulnerabilities addressed by this technology	53
7.3.3	Typical deployment.....	54

7.3.4	Known issues and weaknesses.....	54
7.3.5	Assessment of use in the industrial automation and control systems environment	54
7.3.6	Future directions	55
7.3.7	Problems of encryption usage.....	55
7.3.8	Information sources and reference material	56
7.4	Virtual private networks (VPNs).....	56
7.4.1	Overview	56
7.4.2	Security vulnerabilities addressed by this technology	56
7.4.3	Typical deployment.....	57
7.4.4	Known issues and weaknesses.....	59
7.4.5	Assessment of use in the industrial automation and control systems environment	59
7.4.6	Future directions	60
7.4.7	Recommendations and guidance	60
7.4.8	Information sources and reference material	60
8	Management, audit, measurement, monitoring, and detection tools	60
8.1	General	60
8.2	Log auditing utilities	60
8.2.1	Overview	60
8.2.2	Security vulnerabilities addressed by this technology	61
8.2.3	Typical deployment.....	62
8.2.4	Known issues and weaknesses.....	62
8.2.5	Assessment of use in the industrial automation and control systems environment	62
8.2.6	Future directions	63
8.2.7	Recommendations and guidance	63
8.2.8	Information sources and reference material	63
8.3	Virus and malicious code detection systems.....	63
8.3.1	Security vulnerabilities addressed by this technology	64
8.3.2	Typical deployment.....	64
8.3.3	Known issues and weaknesses.....	64
8.3.4	Assessment of use in the industrial automation and control systems environment	64
8.3.5	Cost range.....	65
8.3.6	Future directions	65
8.3.7	Recommendations and guidance	65
8.3.8	Information sources and reference material	65
8.4	Intrusion detection systems (IDS).....	65
8.4.1	Overview	65
8.4.2	Security vulnerabilities addressed by this technology	66
8.4.3	Typical deployment.....	66
8.4.4	Known issues and weaknesses.....	67
8.4.5	Assessment of use in the industrial automation and control systems environment	67
8.4.6	Future directions	68
8.4.7	Recommendations and guidance	68
8.4.8	Information sources and reference material	68
8.5	Vulnerability scanners	69
8.5.1	Overview	69

8.5.2	Security vulnerabilities addressed by this technology	69
8.5.3	Typical deployment.....	70
8.5.4	Known issues and weaknesses.....	70
8.5.5	Assessment of use in the industrial automation and control systems environment	70
8.5.6	Future directions	71
8.5.7	Recommendations and guidance	71
8.5.8	Information sources and reference material	71
8.6	Forensics and analysis tools (FAT).....	71
8.6.1	Overview	71
8.6.2	Security vulnerabilities addressed by this technology	72
8.6.3	Typical deployment.....	72
8.6.4	Known issues and weaknesses.....	72
8.6.5	Assessment of use in the industrial automation and control systems environment	73
8.6.6	Future directions	73
8.6.7	Recommendations and guidance	74
8.6.8	Information sources and reference material	74
8.7	Host configuration management tools (HCM).....	74
8.7.1	Overview	74
8.7.2	Security vulnerabilities addressed by this technology	74
8.7.3	Typical deployment.....	75
8.7.4	Known issues and weaknesses.....	75
8.7.5	Assessment of use in the industrial automation and control systems environment	75
8.7.6	Future directions	75
8.7.7	Recommendations and guidance	76
8.7.8	Information sources and reference material	76
8.8	Automated software management tools (ASM)	76
8.8.1	Overview	76
8.8.2	Security vulnerabilities addressed by this technology	77
8.8.3	Typical deployment.....	77
8.8.4	Known issues and weaknesses.....	77
8.8.5	Assessment of use in the industrial automation and control systems environment	77
8.8.6	Future directions	78
8.8.7	Recommendations and guidance	78
8.8.8	Information sources and reference material	78
9	Industrial automation and control systems computer software	78
9.1	General	78
9.2	Server and workstation operating systems.....	79
9.2.1	Overview	79
9.2.2	Security vulnerabilities addressed by this technology	79
9.2.3	Typical deployment.....	79
9.2.4	Known issues and weaknesses.....	79
9.2.5	Assessment of use in the industrial automation and control systems environment	80
9.2.6	Future directions	80
9.2.7	Recommendations and guidance	80
9.2.8	Information sources and reference material	81

9.3	Real-time and embedded operating systems	81
9.3.1	Overview	81
9.3.2	Security vulnerabilities addressed by this technology	81
9.3.3	Typical deployment.....	81
9.3.4	Known issues and weaknesses.....	82
9.3.5	Assessment of use in the industrial automation and control systems environment	82
9.3.6	Future directions	82
9.3.7	Recommendations and guidance	82
9.3.8	Information sources and reference material	83
9.4	Web technologies.....	83
9.4.1	Overview	83
9.4.2	Security vulnerabilities addressed by this technology	83
9.4.3	Typical deployment.....	83
9.4.4	Known issues and weaknesses.....	83
9.4.5	Assessment of use in the industrial automation and control systems environment	83
9.4.6	Future directions	84
9.4.7	Recommendations and guidance	84
9.4.8	Information sources and reference material	84
10	Physical security controls	84
10.1	General	84
10.2	Physical protection	85
10.2.1	Security vulnerabilities addressed by this technology	85
10.2.2	Typical deployment.....	86
10.2.3	Known issues and weaknesses.....	86
10.2.4	Assessment of use in the industrial automation and control systems environment	86
10.2.5	Future directions	87
10.2.6	Recommendations and guidance	87
10.2.7	Information sources and reference material	88
10.3	Personnel security.....	88
10.3.1	Overview	88
10.3.2	Security vulnerabilities addressed by this technology	88
10.3.3	Typical deployment.....	89
10.3.4	Known issues and weaknesses.....	90
10.3.5	Assessment of use in the industrial automation and control systems environment	90
10.3.6	Future directions	90
10.3.7	Recommendations and guidance	90
10.3.8	Information sources and reference material	91
Annex A	(informative) Trade name declarations	92
Bibliography	96
Figure 1	– Firewall zone separation	42
Figure 2	– Security gateway to security gateway VPN.....	57
Figure 3	– Host to security gateway VPN	57
Figure 4	– Host to host gateway VPN.....	58

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