



BSI Standards Publication

Industrial communication networks — Network and system security

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

National foreword

This Published Document is the UK implementation of IEC/TR 62443-3-1:2009.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 33564 4

ICS 25.040.40; 33.040.40; 35.040

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2024.

Amendments/corrigenda issued since publication

Date	Text affected



IEC/TR 62443-3-1

Edition 1.0 2009-07

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	20
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	29
5.4.1 Overview	29
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	37
5.8.7	Recommendations and guidance.....	37
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	41
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	44
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	46
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.....	49
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	51
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	53

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.....	62
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	66
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.....	68
8.5.1	Overview	68

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.....	73
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	74
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.....	75
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.....	76
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.....	79
9.2.6	Future directions	80
9.2.7	Recommendations and guidance.....	80
9.2.8	Information sources and reference material.....	80

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	81
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.....	82
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	83
9.4.7	Recommendations and guidance.....	83
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	85
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.....	87
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	89
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 cybersecurity

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>

3 Terms, definitions and acronyms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

access authority

entity responsible for monitoring and granting access privileges to IACSs and their associated industrial networks for other authorized entities [3]¹

3.1.2

access control

- a) protection of system resources against unauthorized access
- b) process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy [3]

3.1.3

accountability

property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions [3]

3.1.4

application layer protocol

layer 7 protocol specific to executing network applications such as email and file transfer [2]

¹ Numbers in square brackets refer to the Bibliography.

NOTE Many modern industrial control systems include fieldbus networks, which do not normally include seven distinct layers, but have an application layer.

3.1.5

asymmetric key algorithm

public key cryptographic algorithm

NOTE By asymmetric, the key for encoding the digital data to be transmitted is entirely different from the code for decrypting the data at the receiving end. This is in contrast to symmetric key encryption, whereby the same key is used to encrypt and decrypt the data. Asymmetric is logistically more secure because it avoids transfer of the key between transmitter and receiver, whereby it could be intercepted. It is important to note that cryptographic methods to protect the confidential data are more critical for IT networks than for control networks. For IACSs, confidentiality is most critical for the authenticating and authorization stages during access control into a given IACS. Usually cryptography adds undesired latency to the IACS network, which is very undesirable for open and closed loop systems that must receive, manipulate, and send control data at a rate commensurate to an asset's process dynamics. Consequently, availability and integrity are usually higher IACS cyber security objectives than is confidentiality. [3]

3.1.6

authentication

security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information [4]

3.1.7

authorization

right or a permission that is granted to a system entity to access a system resource [3]

3.1.8

availability

probability that an asset, under the combined influence of its reliability, maintainability and security will be able to fulfil its required function over a stated period of time or at a given point in time

3.1.9

bandwidth

capacity of a communication channel to pass data through the channel in a given amount of time

NOTE 1 Bandwidth, in the sense of channel capacity, usually is expressed in bits per second.

NOTE 2 Control and SCADA data are usually of smaller, yet consistent, bit sizes than IT networks, which traditionally carry higher levels. Nonetheless, the move to fieldbus systems requires higher band widths due to their inherent nature of requiring less wiring and performing control algorithms without the use of a master station or PLC. [3]

3.1.10

certificate

public key certificate [3]

3.1.11

certification authority

entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy [3]

3.1.12

ciphertext

data that have been transformed by encryption so that the semantic information content (i.e., meaning) is no longer intelligible or directly available

3.1.13**cleartext**

data in which the semantic information content (i.e., meaning) is intelligible or is directly available [3]

3.1.14**client**

device or application receiving or requesting services or information from a server application [1]

3.1.15**confidentiality**

assurance that information is not disclosed to unauthorized individuals, processes or devices [4]

3.1.16**cryptographic key**

input parameter that varies the transformation performed by a cryptographic algorithm [3]

NOTE This is usually shortened to “key”.

3.1.17**cyberattack**

successful exploitation of the software, hardware or firmware vulnerabilities of IACS components and/or the IT network components connected to the industrial network

3.1.18**data-link layer protocol**

layer 2 protocol for point-to-point communications of data, conducting error checking, performing physical addressing and conducting media access control [2]

NOTE These protocols exist in most IT enterprise systems connected to control LANs and in some cases exist in the protocols of industrial networks.

3.1.19**decryption**

process of changing ciphertext into plaintext using a cryptographic algorithm and key (see 3.1.24 “encryption”) [3]

3.1.20**defence in depth**

security architecture based on the idea that any one point of protection may, and probably will, be defeated

NOTE Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be protected by capabilities in other layers;
- system security becomes a set of layers within the overall network security.

3.1.21**denial of service****DoS**

prevention or interruption of authorized access to a system resource or the delaying of system operations and functions [3]

3.1.22

digital signature

result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation [1]

3.1.23

distribution

key distribution [3]

3.1.24

encryption

cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used (see 3.1.19 "decryption") [3]

NOTE If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

3.1.25

integrity

quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data [4]

NOTE In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

3.1.26

interception

capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission and other communication attributes

3.1.27

interface

logical entry or exit point that provides access to the module for logical information flows

3.1.28

key

cryptographic key

3.1.29

key distribution

transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key [3]

3.1.30

key pair

public key and its corresponding private key used with a public key algorithm [3]

3.1.31

local area network

LAN

communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 km) [5]

3.1.32

latency

time interval between when a message is sent by one device and received by a second device

NOTE Latency, along with jitter, are two key parameters that define the performance of a control system. Increased latency for a control loop can be detrimental since the dynamics of the asset under control dictates the amount of latency to keep the control process safe and productive.

3.1.33

man-in-the-middle

active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association

NOTE This is also defined as snooping and can be effectively misleading and destructive in an IACS cyber attack since a control room operator's screen may be indicating safe and normal routine operation, while havoc is conducted on the automated processes and assets in the field. [3]

3.1.34

network layer protocol

layer 3 protocol for routing of messages through a complex network [2]

NOTE Most modern industrial fieldbus protocols and SCADA protocols usually contain a network layer.

3.1.35

non-repudiation

security service that provides protection against false denial of involvement in a communication [3]

3.1.36

password

string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization [1]

3.1.37

personal identification number

PIN

alphanumeric code or password used to authenticate an identity [1]

3.1.38

physical layer protocol

layer 1 protocol for transmitting raw physical (e.g. electro-magnetic) signals over a communications channel

NOTE Layer 1 deals with transmission physics such as cabling, modulation, and transmission rates. [2]

3.1.39

plaintext

unencoded data that is input to and transformed by an encryption process or that is output by a decryption process [3]

3.1.40

point-to-point protocol

PPP

protocol defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g., Internet Protocol (IP) packets) over serial point-to-point links, which is occasionally deployed in certain types of SCADA networks

3.1.41

protection profile

implementation-independent set of security requirements for a category of targets of evaluation that meet specific consumer needs [1]

3.1.42

pseudorandom number generator

PRNG

algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed

NOTE The output of a PRNG should appear to be uniform random, i.e., the output is statistically indistinguishable from uniform random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [3]

3.1.43

public key

cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public [1]

3.1.44

public key certificate

dataset that uniquely identifies an entity, contains the entity's public key and is digitally signed by a trusted party, thereby binding the public key to the entity [1]

3.1.45

public key (asymmetric) cryptographic algorithm

cryptographic algorithm that uses two related keys, a public key and a private key, such that deriving the private key from the public key is computationally infeasible

3.1.46

public key infrastructure

PKI

framework that is established to issue, maintain and revoke public key certificates [3]

3.1.47

repudiation

denial by one of the entities involved in a communication of having participated in all or part of the communication [3]

3.1.48

risk

expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [3]

3.1.49

secret key

cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public [1]

3.1.50

secret key (symmetric) cryptographic algorithm

cryptographic algorithm that uses a single secret key for both encryption and decryption [1]

3.1.51

security domain

system or subsystem of a control LAN or enterprise LAN that is under the authority of a single trusted authority

NOTE Security domains may be organized (e.g. hierarchically) to form larger domains. [3]

3.1.52**security services**

mechanisms used to provide confidentiality, data integrity, authentication or non repudiation of information [3]

3.1.53**server**

device or application that provides information or services to client applications and devices [3]

3.1.54**sniffing**

interception

3.1.55**spoof**

pretending to be an authorized user and performing an unauthorized action [3]

3.1.56**symmetric key**

single cryptographic key that is used with a secret (symmetric) key algorithm

NOTE A system whereby the encrypting key from plain text to cipher text is identical to the key to convert the cipher text back to plain text. [3]

3.1.57**symmetric key algorithm**

secret key cryptographic algorithm [3]

3.1.58**system software**

special software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs and data [1]

3.1.59**threat**

potentially damaging action (intended or unintended) or capability (internal or external) to adversely impact through a vulnerability [6]

3.1.60**throughput**

maximum continuous traffic rate that an IT or IACS device can handle without dropping a single packet [2]

3.1.61**vulnerability**

flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [3]

3.1.62**wide area network****WAN**

communications network designed to connect computers over a large distance, such as across a country or the world [1]

3.2 Acronyms

All trade names and trademarks used in this document are listed in Annex A.

3DES	Triple Digital Encryption Standard
AES	Advanced Encryption Standard
AGA	American Gas Association
ASM	Automated Software Management
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
CIP®	Common Industrial Protocol (formerly Control and Information Protocol)
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CS	Control System
DAC	Discretionary Access Control
DC	Domain Controller
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DPA	Differential Power Analysis
EC	Elliptic Curve
ECC	Elliptic Curve Cryptosystem
FAN	Field Area Network
FAQ	Frequently Asked Questions
FAT	Forensics and Analysis Tool
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GPS	Global Positioning System
HCM	Host Configuration Management
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IACS	Industrial Automation and Control System
IAONA	Industrial Automation Open Networking Association
IATF	Information Assurance Technical Framework
ID	Identification
IDS	Intrusion Detection System
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSS	Location Signature Sensor

MAC	Media Access Control
MIT	Massachusetts Institute of Technology
NAT	Network Address Translation
NFA	Network Forensics and Analysis
NIDS	Network Intrusion Detection System
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Administration
OLE [®]	Object Linking and Embedding
OPC [®]	OLE for Process Control
OS	Operating System
PC	Personal Computer
PCN	Process Control Network
PDA	Personal Digital Assistant
PGP [®]	Pretty Good Privacy [®]
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PPP	Point-to-Point Protocol
PRNG	Pseudorandom Number Generator
RBAC	Role-Based Access Control
RFC	Request For Comment
RSA [®]	Rivest, Shamir and Adleman
RTOS	Real-time Operating System
RTU	Remote Terminal Unit
SAM	Security Accounts Manager
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
Sysdiff	System Difference Packages
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VDS	Virus Detection System
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

4 Overview

Many industries and critical infrastructures have reported an increase in the number of unauthorized attempts to access electronic information, or even more ominous, hack into IACSS that monitor and regulate assets crucial for a nation (e.g. energy pipelines, transportation systems, water systems, the power grid). Over the last several years, the number of joint ventures, alliance partners and outsourced services in the industrial sector has

increased dramatically. During that same period, IACSs have evolved from isolated networks based on proprietary technologies and protocols to standards-based networks connected to the rest of the enterprise—including the IT business enterprise usually connected to the Internet and to other enterprises such as partners and corporate WANs.

Consequently, it is now very challenging to know *who* is authorized to have access to electronic IACSs information, *when* they are to have access to the information and *what* data they should be able to access. Partners in one business venture may also be competitors in another business. However, because IACS equipment is directly connected to a process, loss of trade secrets or interruptions in the flow of information are not the only potential consequences of a security breach and certainly not the ones with the greatest impact. Far more serious can be the potential loss of production, environmental damage, regulatory violation, or compromise to the safety of an operation. The latter may have ramifications beyond the targeted company; it may grievously damage the infrastructure of the host region or nation.

Worldwide, an increasing percentage of the population has become computer literate, and malicious hacking, in addition to being a nefarious hobby with high-profile news coverage, has become a means to profit financially. In fact, tools to automate malicious hacking are now publicly available on the Internet. Instances of computer virus attacks are increasing in frequency. External threats of terrorist, expert hackers and nation states are not the only concerns; knowledgeable insiders with malicious intent or even an innocent unintended act can pose a serious security risk to an industry or critical infrastructure. Combining all these factors, it is easy to see that the probability of someone gaining unauthorized or damaging access to a control system has increased.

While technology changes such as standardization, vertical connectivity, and remote access (both wire and wireless), as well as partner relationships may be good for the business, economics, efficiency and productivity ends of the critical infrastructure industries, they increase the potential risk for compromising the cyber security of IACSs. Likewise, as threats to industry increase, so does the need for cyber security.

The working group that authored this technical report determined that there were several categories of tools, countermeasures and technologies available for securing an IACS network. Major categories are covered in Clause 5 through Clause 10 of this technical report. The information in each clause provides an overview of each technology, tool and/or countermeasure category, a list of specific types of applications within that category and a discussion of how well that type of application fits the IACS environment and requirements.

IACS networks use many of the same computers and communication technologies as corporate IT/enterprise networks, because it is more economical to add to existing technologies than to start from scratch. However, unique technical and operating constraints shall be considered when applying security technologies. One of the major goals of this technical report is to highlight those areas that warrant special consideration of IACS factors.

5 Authentication and authorization technologies

5.1 General

The concept of authorization has existed for as long as humans have had assets worth protecting. Authorization is the initial step in protecting an IACS system and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system. Once this information is determined, defence-in-depth access control measures can be implemented to verify that only authorized people and devices can actually access an IACS system. The first measure is usually authentication of the person or device that is attempting access to an IACS system.

Authorization can be as granular as determining access to specific files in an application or as encompassing as access to an entire enterprise or IACS network. Authorization is usually implemented indirectly via configuration tools provided by the vendors of operating systems.

applications and networks. Authorization mechanisms show up in virtually all systems and impose great architectural and administrative challenges at all levels of enterprise and IACS computing.

Authorization and authentication are fundamental to access control for an IACS. They are distinct concepts but are often confused because of the close relationship between the two. Proper authorization is, in fact, dependent upon authentication.

Authentication describes the process of positively identifying potential network users, hosts, applications, services and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions. Based on the response received, the system may or may not allow the potential user access to its resources.

There are several possible factors for determining the authenticity of a person, device or system. For example, the test could be something known (e.g. PIN or password), something owned (e.g. key, dongle or smart card), something physical (e.g. biological characteristic such as a fingerprint or retinal signature), a location (e.g. global positioning system (GPS) location access), the time a request is made, or a combination of these attributes. In general, the more factors that are used in the authentication process, the more robust the cyber security process will be. When two or more factors are used, the process is known generically as multi-factor authentication.

There are two components to authentication:

- User authentication—traditional computer authentication such as “logging into a computer” or activating a human machine interface (HMI) to adjust a process.
- Network service authentication—the ability for networked devices to distinguish between authorized and unauthorized remote requests for IACS data or to perform actions on the IACS.

Computer systems in the IACS environment typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are often easy to guess or infrequently changed, and create additional security risk as a result. At the current time, protocols used in IACS environments generally have inadequate or no network service authentication.

NOTE Network service authentication should not be confused with “message authentication,” which is frequently used in security literature. Message authentication deals with protecting a message from modification during transmission and signing digital records for long-term electronic storage. This concept is included in Clause 7.

Listed below are several types of authentication and authorization technologies. Clause 9 on [operating systems](#) associated with IACS systems also includes a discussion of authorization issues.

5.2 Role-based authorization tools

5.2.1 Overview

Role-based access control (RBAC) is a technology and tool that is attracting a great deal of attention because of its potential for reducing the complexity and cost of security administration in networks with large numbers of intelligent devices like some IACS systems. Under RBAC, security administration is simplified by using roles, hierarchies, and constraints to organize user access levels. RBAC reduces costs within an organization because it accepts that control operation employees change more frequently than the duties within positions.

5.2.2 Security vulnerabilities addressed by this technology

RBAC systems are designed to minimize the potential for security violations by providing greater control over users' access to information and resources of multiple devices in an IACS network. The level of control room operator access can take several forms, including viewing,

using, and altering specific IACS data or device functions. The promise of RBAC is a uniform means to manage access to plant floor devices while reducing the cost of maintaining individual device access levels and minimizing errors.

The traditional approach to controlling access to IACS information and network resources is to establish specific permissions for each user. Permissions are then configured into the security level mechanisms supported by the individual intelligent devices. An industrial control system may have thousands of devices, such as DCSs, HMIs, process historians, PLCs, motor control centres, smart sensors and application-specific data concentrators. While effective in a static environment, this approach is difficult to manage in dynamic environments where users enter and leave employment and contractors, original equipment manufacturers, system integrators, and vendors come and go. The constant stream of changes requires frequent updates to access permissions, a time-consuming and error-prone process. A common security lapse with this approach is that timely permission updates are not made, enabling unauthorized users (such as terminated employees) to access restricted functions. Quite often, plants either do not use or simply disable individual device security access levels for this reason.

RBAC addresses this problem by basing access on a user's role or job responsibilities rather than customizing access for each individual. For example, machine operators may be able to view certain files, but not alter them.

On the surface, basing access control on job descriptions may seem a bit restricting, but RBAC can grant multiple access permissions to groups and has the ability to grant elevated access privileges to certain individuals. Using the previous example, the machine operators could view files on a number of devices, but the machine vendor's support engineers could access additional functions only on their specific machine. Roles can also be set up based on location, projects, schedule, and management level.

Although employee and contractor turnover make it difficult to maintain individual permissions, it is not a problem for roles because they usually do not change as often. Being able to add or remove users from role groups in a centralized database minimizes the effort to keep access levels current and reduces the potential for error.

5.2.3 Typical deployment

Access to computer system objects in an IACS is based on a user's role in an organization. Users are associated with roles and roles are associated with permissions. Users have permission to access an object only if the user has an authorized role associated with that permission.

RBAC tools provide graphical user interfaces that simplify the process of establishing roles, groups and permissions. These tools are often Web-based and can be operated over an enterprise's corporate Intranet. Most RBAC tools centralize the repository of authorizations, while delegating the actual role assignment to the functional department manager. A plant might use RBAC to centralize access control to the intelligent devices of the control system, but assigning personnel to roles becomes the separate responsibilities of the instrumentation, maintenance, and operations support departments.

RBAC tools can set, modify, or remove authorizations in applications, but they do not replace the authorization mechanism; they do not check and authenticate users every time a user wants to access an application.

5.2.4 Known issues and weaknesses

In order to provide uniform authorization management, RBAC tools shall be able to work with the tokens, digital certificates, directories, or other authorization mechanisms of the intelligent devices they are protecting. RBAC tools offer interfaces to authorization mechanisms for most current platforms in the IT arena. However, legacy IACS systems or specialized IACS equipment require development of specialized interface software. Software development can pose an enormous task for many systems, and is the single largest reason that prevents many

companies from implementing single-sign-on capabilities to enterprise networks. This issue is a large problem for industrial control systems that use a number of proprietary operating systems or customized operating system implementations and interfaces.

Centralized RBAC strategies have the potential for making access to the control systems dependent upon the health and availability of the corporate wide area network and some central RBAC server. Thus, centralized RBAC introduces additional points of failure that can impact the availability of the industrial automation and control system. Another issue with RBAC is that it is a relatively new methodology whose benefits and applications are not yet well understood. Also, some IACS architectures do not presently support the methodology.

5.2.5 Assessment of use in the industrial automation and control systems environment

At the time this technical report was released, the working group that authored it was not aware of any broad-based RBAC tools specifically developed for industrial control systems. In particular, tools that uniformly authorize control systems employing products from multiple vendors were not available. However, some equipment vendors did offer tools that centralize authorization of a portion of their products, such as access to the program development applications for controllers.

5.2.6 Future directions

Protocols used in industrial environments will need to accommodate access control mechanisms consistent with RBAC. While difficult to achieve in many legacy protocols, this is occurring in some more modern protocols. One example of this is the OLE[®] for Process Control (OPC[®]) standard, which has developed security specifications for access control to OPC[®] servers.

Products that perform some measure of uniform authorization management for industrial control devices were introduced as early as 2005, but are not widely deployed. The functionality in these products may be incorporated into security gateways that combine a number of security functions.

5.2.7 Recommendations and guidance

In the absence of uniform authorization tools, most designers of IACSs take precautions to minimize the amount of external traffic to and from the control system. While various architectural measures attempt to stop data flow into the control system from the enterprise systems, this cannot be achieved in total. While RBAC may increase the safety of spontaneous data requests to the control system, it is not a panacea for careless design of the data flows.

5.2.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [NIST02]
- [FKC]
- [KG]
- [bhold]

5.3 Password authentication

5.3.1 Overview

Password authentication technologies determine authenticity based on testing for something the device or the control operator that is requesting access to the IACS should know (i.e., a secret), such as a personal identification number (PIN) or password. Password authentication schemes are the simplest and most common.

There are three general types of passwords:

- passcode or PIN—a short sequence of numbers used as the secret (e.g., the digits 1234);
- password—a short character string used as the secret (e.g., “hat34slow”);
- passphrase—a long string used to generate the secret (e.g., the phrase “downtown 23 boats hit cars and blew smoke into cabbage” might generate the secret radix-64 value X34B3-By88e-P345s-56df0).

Each password type follows the same concept, but provides different levels of complexity for the user and therefore the security for the system.

- A passcode is simple enough for even the smallest embedded device to manage. It often represents a number from 0 to 9999 and can be stored as a simple 16-bit integer. It is also the least secure method. The two most common examples are a PIN for an automatic teller machine card or the keypad on a door access device.
- A password is a longer secret, often in the 6 to 14 character range. It takes more memory and processing to manage, and therefore provides a little more security.
- A passphrase is a longer secret that could be used to create a numeric key for a cipher system. While it takes some effort to remember a phrase like “downtown 23 boats hit cars and blew smoke into cabbage,” it is much easier for most people to remember than the code “X34B3-By88e-P345s-56df0.” This method also provides more security because it is the hardest for a hacker to guess and is less probable for a password/code-breaking program to break.

5.3.2 Security vulnerabilities addressed by this technology

In the IACS environment, passwords can be used to limit requests for services and functions to authorized users.

5.3.3 Typical deployment

Passwords are commonly employed in one of two ways:

- The password is submitted with the request for authorization. Network service requests usually include the password with the request. A common example is a Simple Network Management Protocol (SNMP) request that includes a community name.
- After the request, the system requests the password to confirm authorization. User authentication generally requests the password after a user attempts access.

5.3.4 Known issues and weaknesses

The strength of a password is directly related to its length and entropy (randomness). The importance of length is fairly obvious. A two-digit passcode has only 100 possible values from 00 to 99, while an 8-character password has billions of possible values.

Entropy is a measure of the randomness in the password and is equally important. Passwords that use predictable sequences of digits (e.g., “1234”) or common English language words (e.g., “password” or “operator”) are far easier to predict than more random passwords. Unfortunately, the greatest weakness in the use of passwords is that control system users tend to pick passwords that are easy to remember and thereby have very low entropy and are easy to predict.

Most passcodes on a 12-key keypad end up as a simple physical pattern, like 1254 or 1478, while many computer passwords are birth-dates or a spouse or pet name. Cracking schemes use human preferences for pattern recognition and familiarization to allow attackers to guess the correct password in far fewer than the theoretical number of tries. Password vulnerability can be reduced if the vendor implements an active password checker that prohibit weak, recently used, or commonly used passwords.

Another weakness is the ease of third party eavesdropping. Passwords typed at a keypad or keyboard are easily observed or recorded, especially in areas where attackers could plant tiny wireless cameras or hardware keystroke sniffers. Network service authentication often transmits passwords as plaintext (unencrypted), allowing any network capture tool to expose the actual password.

An improvement over plaintext passwords is hashed passwords. A one-way algorithm is used to cryptographically convert passwords into a hash code, which is extremely computationally expensive to decrypt back to the original password. However, not all hashed passwords are safe. It is possible to determine another password that hashes to the same value, but it is also computationally expensive to do so. More seriously, even if passwords are sent as cryptographic hashes, network capture tools often allow the message to be modified and “replayed,” easily creating a new message complete with valid encrypted password without ever knowing the original password.

Password files shall be protected from read or copy access. One common method for password cracking is to copy the password file and run off-line programs against the file. These programs generate a large number of possible passwords and hashes, each with the same one-way algorithm, to build a password versus hash list. The program then compares the captured password files to the list until a match is found. This method of attack limits the exposure of the attacker and may result in a fully compromised system.

5.3.5 Assessment of use in the industrial automation and control systems environment

One problem with passwords unique to IACS environments is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required, an operator may panic and have difficulty remembering the password and either be locked out completely or delayed in being able to respond to the event. If the password has been entered wrong and the system has a limit on allowed wrong password entries, the operator may be locked out permanently until an authorized employee can reset the account.

Special consideration shall be made when using IT policies based on login password authentication within the IACS environment. Without an exclusion list based on machine identification (ID), non-operator logon can result in policies being implemented such as auto-logout timeout and administrator password replacement that can be detrimental to the operation of the system. Some controller operating systems make setting secure passwords difficult, as the password size is very small and the system usually allows only group passwords at each level of access, not individual passwords.

Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted systems.

5.3.6 Future directions

Industrial automation and control systems equipment should be sophisticated enough to allow high-level password security. IACS equipment needs to have protocols that allow passwords to be transmitted in secure ways (i.e., not plaintext). One method of password use for the future may well be a common method noted as RBA, or role-based authentication, where several operators have, in some cases, the same password and therefore are equally authorized since they all have the same authorities in relation to what they can or cannot do once they enter the control system through authorization. Such role-based methods associate the person with his or her job role as opposed to his or her individuality and are useful for administration in an environment where job roles change more frequently than in a common IT enterprise.

Future IACS password equipment and protocols shall be able to provide flexibility to an operator for various emergency situations. For instance, in an emergency situation, a password

operator may attempt to log in unsuccessfully several times. Not allowing the operator access to the system in an emergency situation could create severe problems with disastrous results. Therefore, there shall be provisions for the password algorithm to recognize the unsuccessful attempts of someone who has knowledge of the password through the use of the similarities of each of the unsuccessful attempts. The algorithm should then allow a simple emergency password to be used by the operator for logon purposes.

5.3.7 Recommendations and guidance

The following are general recommendations and considerations with regards to the use of passwords. Specific recommendations will be presented in IEC 62443-2-1².

- Passwords should have appropriate length and entropy characterization for the security required. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
- Initial passwords and passwords that have been reset should be securely transmitted to the intended receiver. User authentication not subject to social engineering methods shall be employed. These can include face-to-face ID authentication and voice-mail delivery.
- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out during critical events.
- The keeper of master passwords should be a trusted employee, available during emergencies. Authority to change higher-level passwords should be limited to trusted employees. A password log, especially for master passwords, should be maintained separately from the control systems, possibly in a notebook locked in a vault or safe.
- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), users should consider supplementing password authentication with other forms of authentication such as challenge/response or two-factor authentication using biometric or physical tokens.
- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of strong encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
- For network service authentication purposes, passwords should be avoided if possible. There are more secure alternatives available, such as challenge/response or public-key authentication.

5.3.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [AGA-12]
- [NIST03], [NIST04], [NIST07], [NIST07A], [NIST07B], [NIST09], [NIST10]
- [IAONA]
- [Mix]
- [Zur]
- [Har1]

² To be published.

5.4 Challenge/response authentication

5.4.1 Overview

Challenge/response authentication requires that the service requester, the IACS operator, and service provider know a “secret” code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the “secret” without ever exposing the secret on the network.

5.4.2 Security vulnerabilities addressed by this technology

Challenge/response authentication addresses the security vulnerabilities of traditional password authentication. When passwords (hashed or plain) are sent across a network, a portion of the actual “secret” itself is being sent. Giving the secret to the remote device performs authentication. Therefore, traditional password exchange always suffers the risk of discovery or replay. Because the secret is known in advance and never sent in challenge/response systems, the risk of discovery is eliminated. If the service provider can never send the same challenge twice, and the receiver can detect all duplications, the risks of network capture and replay attacks are eliminated.

5.4.3 Typical deployment

Common challenge/response systems are:

- PPP-CHAP Internet Engineering Task Force (IETF)/RFC1994—PPP-CHAP allows a remote client to connect over a serial or dial-up link to a server. The client shall still know the password, but CHAP uses a challenge/response system to verify the password without sending it across the serial line where an attacker may see or replay it.
- Kerberos IETF/RFC1510—Kerberos is a centralized server system designed for small, single-authority networks. It allows servers to provide service to clients based on a simple, secure “ticket” concept. A theoretical example is an Object Linking and Embedding (OLE[®]) OPC[®] server that obtains a data read ticket from a central Kerberos server and submits it to a PLC before the PLC will answer data requests. Both Windows[®] and UNIX[®]/Linux[®] have options for Kerberos support.

5.4.4 Known issues and weaknesses

- Challenge/response authentication cannot be used directly for user authentication because users are not willing to manually combine their passwords and a challenge to calculate a suitable response. Protocols like PPP-CHAP get around this problem by directly accepting the user’s password and managing the challenge/response authentication indirectly without direct user awareness. However, this hybrid approach still provides a way for determined attackers to observe keystrokes as the user enters them.
- A theoretical weakness in challenge/response authentication is that an attacker is provided with both the challenge and the response to examine off-line. If a known algorithm and key are used to create the response, an attacker can use this knowledge to calculate the “secret.” This vulnerability is easily avoided by using strong cryptographic algorithms that make reverse calculation difficult and time-consuming.
- The greatest weakness in challenge/response authentication for network service authentication lies in any system that allows a “roll-back attack” during some form of authentication negotiation. In a rollback attack, the attacker causes the service provider to agree to use a weaker legacy authentication method, such as plain text passwords or no authentication at all. This vulnerability can be avoided if the vendor provides methods to prevent rollback, such as a setting in the service device to restrict network service authentication to use only secure versions of the protocol, and the user enables those methods.
- Passwords, keys, or secrets used by challenge/response authentication shall be distributed somehow, either physically or by a network, which risks exposing them and compromising

the system. Distribution methods require special care in design and implementation to avoid becoming the weak link in the security system.

5.4.5 Assessment of use in the industrial automation and control systems environment

For user authentication the direct use of challenge/response authentication is not feasible for control systems due to the possible latency that may be introduced in the necessary fast dynamics required for access to a control system or industrial network.

For network service authentication, the use of challenge/response authentication is preferable to more traditional password or source identity authentication schemes.

5.4.6 Future directions

Industrial automation and control systems equipment and their protocols should be sophisticated enough to allow challenge/response authentication in order to provide for proper security in the future. When ordering these systems, one should look for a good and timely challenge/response authentication protocol such as the Challenge Handshake Authentication Protocol (CHAP), which authenticates using a challenge/response method. CHAP is used the same way as is Password Authentication Protocol, but CHAP provides a higher degree security. CHAP can be used by remote users, routers, and network access servers to provide authentication before providing connectivity.

5.4.7 Recommendations and guidance

Challenge/response authentication provides more security than encrypted passwords for user authentication across a network.

Managing master encryption algorithms and master passwords becomes increasingly more complex as more parties are involved in the security processes, and is an important consideration in the robustness of the security scheme.

5.4.8 Information sources and reference material

The references in square brackets listed below refer to the Bibliography.

- [Sim]
- [ZC]

5.5 Physical/token authentication

5.5.1 Overview

Physical or token authentication is similar to “password authentication,” except that these technologies determine authenticity by testing for a device or token the person requesting access should have in his or her possession, such as security tokens or smart cards. Increasingly, PKI keys are being embedded in physical devices such as the universal serial bus (USB).

Some tokens support single-factor authentication only, so that simply having possession of the token is sufficient to be authenticated. Others support dual-factor authentication that require knowledge of a PIN or password in addition to possessing the token in order to be authenticated.

5.5.2 Security vulnerabilities addressed by this technology

The primary vulnerability that token authentication addresses is the ability to prevent the secret from being easily duplicated or shared with others. It eliminates the all-too-common scenario of a password to a “secure” system being left on the wall next to the personal computer.