SLOVENSKI STANDARD
oSIST prEN 62443-2-4:2019

01-januar-2019

Zaščita industrijske avtomatizacije in nadzornih sistemov - 2-4. del: Zahteve za program varnosti za ponudnike storitev IACS

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

Sécurité des automatismes industriels et des systèmes de commande □ Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

Ta slovenski standard je istoveten z: prEN 62443-2-4

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

oSIST prEN 62443-2-4:2019 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 62443-2-4

November 2018

ICS

English Version

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015)

Sécurité des automatismes industriels et des systèmes de commande ¿ Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS
(IEC 62443-2-4:2015)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme
(IEC 62443-2-4:2015)

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2019-02-08.

The text of this draft consists of the text of IEC 62443-2-4:2015.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German).
A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (prEN 62443-2-4:2018) consists of the text of IEC 62443-2-4:2015 prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

IEC 62443-2-4

Edition 1.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.040; 35.100 ISBN 978-2-8322-2767-1

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-2-4 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This publication contains an attached file in the form of an Excel 97-2003 spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

The text of this standard is based on the following documents:

CDV	Report on voting
65/545/CDV	65/561A/RVC

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

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

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The contents of the corrigendum of August 2015 have been included in this copy.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS). It has been developed by IEC Technical Committee 65 in collaboration with the International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name, and ISA 99 committee members.

Figure 1 illustrates the relationship of the different parts of IEC 62443 being developed. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

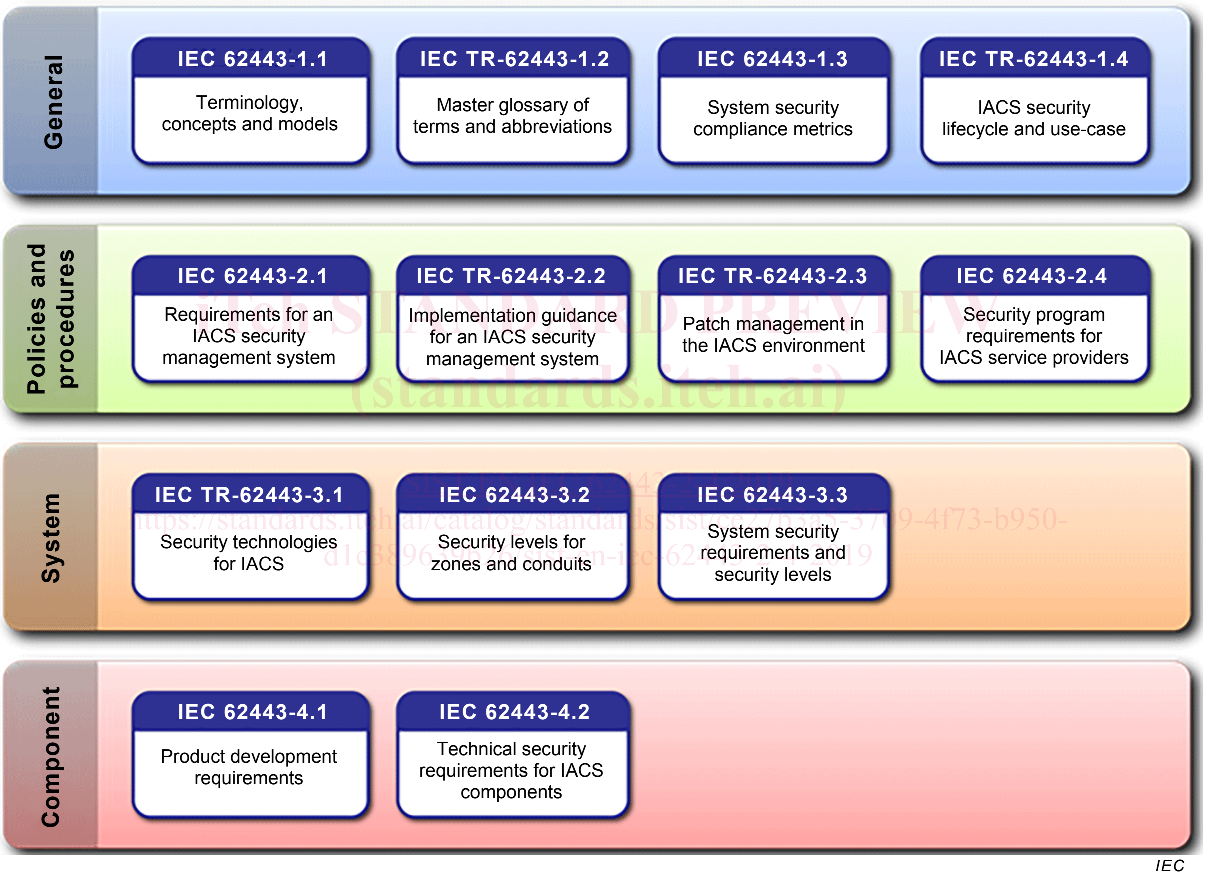
General
IEC 62443-1.1
Terminology, concepts and models
IEC TR-62443-1.2
Master glossary of terms and abbreviations
IEC 62443-1.3
System security compliance metrics
IEC TR-62443-1.4
IACS security lifecycle and use-case
Policies and procedures
IEC 62443-2.1
Requirements for an IACS security management system
IEC TR-62443-2.2
Implementation guidance for an IACS security management system
IEC TR-62443-2.3
Patch management in the IACS environment
IEC 62443-2.4
Security program requirements for IACS service providers
System
IEC TR-62443-3.1
Security technologies for IACS
IEC 62443-3.2
Security levels for zones and conduits
IEC 62443-3.3
System security requirements and security levels
Component
IEC 62443-4.1
Product development requirements
IEC 62443-4.2
Technical security requirements for IACS components
IEC

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

1 Scope

This part of IEC 62443-2-4 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 2 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

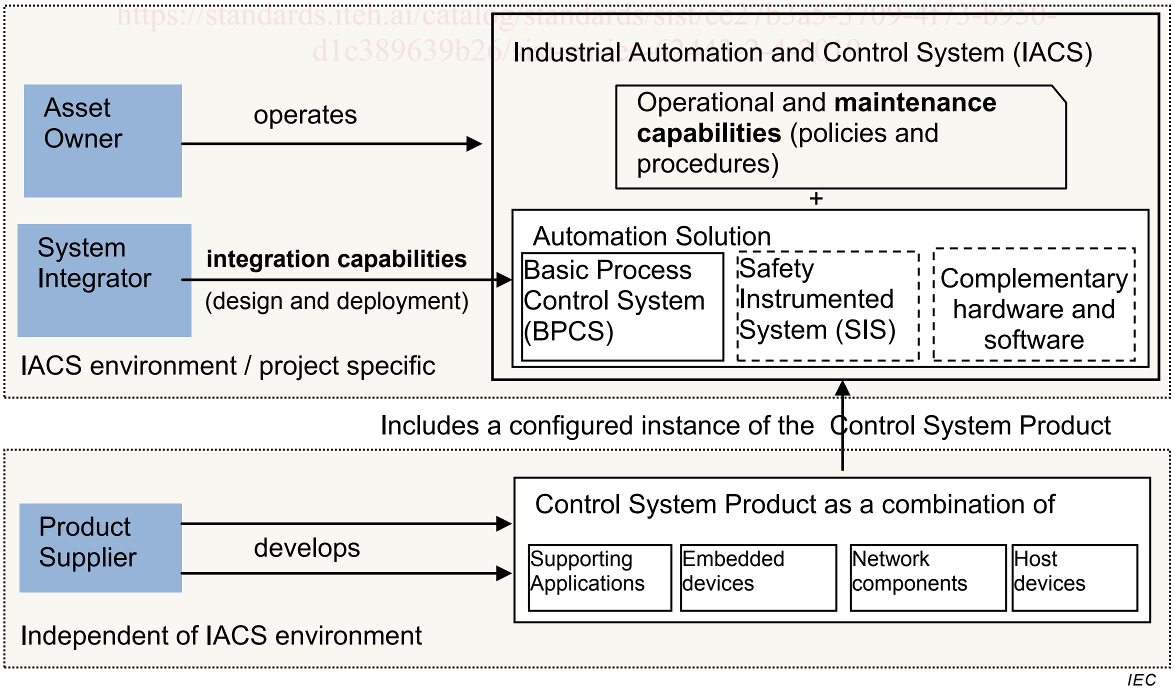
Industrial Automation and Control System (IACS)
Asset Owner
operates
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
integration capabilities
(design and deployment)
Automation Solution
Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary hardware and software
IACS environment / project specific
Includes a configured instance of the Control System Product
Product Supplier
develops
Control System Product as a combination of
Supporting Applications
Embedded devices
Network components
Host devices
Independent of IACS environment
IEC

Figure 2 – Scope of service provider capabilities

In Figure 2, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 3 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

NOTE 4 Clause 4.1.4 describes profiles and how they can be used by industry groups and other organizations to adapt this International Standard to their specific environments, including environments not based on an IACS.

NOTE 5 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

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, abbreviated terms and acronyms

3.1 Terms and definitions

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

3.1.1
asset owner
individual or organization responsible for one or more IACSs

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: This definition includes the components that are part of the IACS.

Note 3 to entry: In the context of this standard, asset owner also includes the operator of the IACS.

3.1.2
attack surface
physical and functional interfaces of a system that can be accessed and through which the system can be potentially exploited

Note 1 to entry: The size of the attack surface for a software interface is proportional to the number of methods and parameters defined for the interface. Simple interfaces, therefore, have smaller attack surfaces than complex interfaces.

Note 2 to entry: The size of the attack surface and the number of vulnerabilities are not necessarily related to each other.

3.1.3
Automation Solution
control system and any complementary hardware and software components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this part of IEC 62443.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (e.g. a specific number of workstations, controllers, and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution may be comprised of components from multiple suppliers, including the product supplier of the control system.

3.1.4
basic process control system

system that responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety integrated functions (SIF)

Note 1 to entry: Safety instrumented functions are specified in the IEC 61508 series.

Note 2 to entry: The term “process” in this definition may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

3.1.5
consultant

subcontractor that provides expert advice or guidance to the integration or maintenance service provider

3.1.6
control system

hardware and software components used in the design and implementation of an IACS

Note 1 to entry: As shown in Figure 2, control systems are composed of field devices, embedded control devices, network devices, and host devices (including workstations and servers.

Note 2 to entry: As shown in Figure 2, control systems are represented in the Automation Solution by a BPCS and an optional SIS.

3.1.7
handover

act of turning an Automation Solution over to the asset owner

Note 1 to entry: Handover effectively transfers responsibility for operations and maintenance of an Automation Solution from the integration service provider to the asset owner and generally occurs after successful completion of system test, often referred to as Site Acceptance Test (SAT).

3.1.8
industrial automation and control system

collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

Note 1 to entry: The IACS may include components that are not installed at the asset owner’s site.

Note 2 to entry: The definition of IACS was taken from in IEC-62443-3-3 and is illustrated in Figure 2. Examples of IACSs include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. IEC 62443-2-4 also defines the proper noun “Solution” to mean the specific instance of the control system product and possibly additional components that are designed into the IACS. The Automation Solution, therefore, differs from the control system since it represents a specific implementation (design and configuration) of the control system hardware and software components for a specific asset owner.

3.1.9
integration service provider

service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover

Note 1 to entry: Integration service providers are often referred to as integrators or Main Automation Contractors (MAC).

3.1.10
maintenance service provider

service provider that provides support activities for an Automation Solution after handover

Note 1 to entry: Maintenance is often considered to be distinguished from operation (e.g. in common colloquial language it is often assumed that an Automation Solution is either in operation or under maintenance). Maintenance service providers can perform support activities during operations, e.g. managing user accounts, security monitoring, and security assessments.

3.1.11
portable media
portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to: CD / DVD / BluRay Media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds, and portable computers.

3.1.12
product supplier
manufacturer of hardware and/or software product

Note 1 to entry: Used in place of the generic word vendor to provide differentiation.

3.1.13
remote access
access to a control system through an external interface of the control system

Note 1 to entry: Examples of applications that support remote access include RDP, OPC, and Syslog.

Note 2 to entry: In general, remote access applications and the Automation Solution will reside in different security zones as determined by the asset owner. See IEC 62443-3-2 for the application of zones and conduits to the Automation Solution by the asset owner.

3.1.14
safety instrumented system
system used to implement functional safety

Note 1 to entry: See IEC 61508 and IEC 61511 for more information on functional safety.

3.1.15
security compromise
violation of the security of a system such that an unauthorized (1) disclosure or modification of information or (2) denial of service may have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

3.1.16
security incident
security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term “of some significance’ is relative to the environment in which the security compromise is detected. For example, the same compromise may be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

3.1.17
security patch
software patch that is relevant to the security of a software component

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches may address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

3.1.18
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS

Note 1 to entry: The security program for IACS service providers refers to the policies and procedures defined by them to address security concerns of the IACS.

3.1.19
service provider
individual or organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.20
subcontractor
service provider under contract to the integration or maintenance service provider or to another subcontractor that is directly or indirectly under contract to the integration or maintenance service provider

3.1.21
system
interacting, interrelated, or interdependent elements forming a complex whole

Note 1 to entry: A system may be packaged as a product.

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by the use of an adjective, such as control system. In the context of a control system, the elements are largely hardware and software elements.

3.1.22
verify
check that the specified requirement was met

3.1.23
vulnerability
flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise

Note 1 to entry: Security policies typically include policies to protect confidentiality, integrity, and availability of system assets.

3.2 Abbreviations

AES_GCM	Advanced Encryption Standard Galois/Counter Mode
BPCS	Basic Process Control System
BR	Base Requirement
CEF	Common Event Format
DCOM	Distributed Common Object Model
DCS	Distributed Control System
EWS	Engineering Workstation
IACS	Industrial Automation and Control System
RE	Requirement Enhancement
RDP	Remote Desktop Protocol
RFC	Request For Comment
RFQ	Request For Quote
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level