IEC TR 63283-3

Edition 1.0 2022-03

TECHNICAL REPORT

colour inside

Industrial-process measurement, control and automation – Smart manufacturing –
Part 3: Challenges for cybersecurity

IEC TR 63283-3:2022-03(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 63283-3

Edition 1.0 2022-03

TECHNICAL REPORT

colour inside

Industrial-process measurement, control and automation – Smart manufacturing –
Part 3: Challenges for cybersecurity

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40

ISBN 978-2-8322-1085-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – SMART MANUFACTURING –

Part 3: Challenges for cybersecurity

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.

IEC TR 63283-3 has been prepared by Technical Committee 65: Industrial-process measurement, control and automation. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
65/865/DTR	65/906/RVDTR

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

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts in the IEC 63283 series, published under the general title *Industrial-process measurement, control and automation – Smart Manufacturing*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

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

Smart Manufacturing comes with many new challenges to cybersecurity. It starts from architectural paradigm shifts combining many valuable assets (design, production planning, engineering, supply chain management, etc.) currently enclosed into dedicated systems into one system. Many stakeholders need to cooperate and exchange information. This is enabled by the application of new information technologies such as industrial internet-of-things (IIoT), edge technology, machine learning, wireless communications and new production technologies as additive manufacturing, exposure of data belonging to contracting parties.

From the point of view of cybersecurity increasing digitalization, tight networking and interconnectivity, usage of standard IT technologies, etc., increase the attack surface and could enable new types of attack. This puts the protection goals integrity and availability of the production system, as well as confidentiality of data involved in the production process at risk. Examples are counterfeiting, loss of know-how or intellectual property, leaking of key performance indicators.

This Technical Report contains smart manufacturing challenges for cybersecurity, i.e., it identifies issues that need to be addressed/fulfilled by smart manufacturing systems in order to ensure their security.

Cybersecurity is a concern for any kind of production method such as:

- discrete manufacturing;
- continuous production;
- batch production.

The tasks of the IEC 65 WG 23 taskforce cybersecurity are:

- review smart manufacturing use cases to find cybersecurity relevant scenarios and requirements;
- if necessary, propose additional smart manufacturing use cases showing potential cybersecurity issues;
- develop a list of smart manufacturing requirements that are necessary to provide cybersecurity in smart manufacturing components, systems, design, integration, and operation and maintenance;
- propose possibilities for smart manufacturing specific profiling in order to simplify application of IEC 62443 (all parts).

This report is limited to cybersecurity related impacts of smart manufacturing. Other requirements for smart manufacturing systems such as safety and reliability are left to be addressed in future reports. However, cybersecurity needs to consider and address safety issues triggered by security attacks.

The initial use case analysis constitutes a bottom-up approach intended to gain a better understanding of the topic. The provided use cases are not necessarily exhaustive. A top-down approach for a generic smart manufacturing model is aimed for in the future.

INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – SMART MANUFACTURING –

Part 3: Challenges for cybersecurity

1 Scope

This part of IEC 63283 identifies challenges which apply to the engineering of a smart manufacturing facility related to cybersecurity.

NOTE Cybersecurity challenges and how to deal with them can impose constraints on the engineering of the smart manufacturing system.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443 (all parts), *Security for industrial automation and control systems*

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

NOTE The definitions are fully aligned with IEC TR 63283-1 [1] (65/683/DTR).

3.1.1
access
ability and means to communicate with or otherwise interact with a system in order to use system resources

Note 1 to entry: Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log in to a system and application, through a combination of logical and physical means).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.1]

[1] Under preparation. Stage at the time of publication: IEC/DECPUB 63283-1:2022.

3.1.2
access control
protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy

[SOURCE: IEC TS 62443-1-1:2009, 3.2.2]

3.1.3
administrator
user role whose responsibilities include controlling access to and implementing security policies for a system

3.1.4
asset
entity owned by or under the custodial duties of an organization, which has either a perceived or actual value to the organization

3.1.5
attack
assault on a system that derives from an intelligent threat – i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Note 1 to entry: There are different commonly recognized classes of attack:

a) An "active attack" attempts to alter system resources or affect their operation.

b) A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.

c) An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

d) An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.9]

3.1.6
attribute
property or characteristic of an entity

[SOURCE: IEC TR 62390:2005, 3.1.3]

3.1.7
audit log
traceable record that requires a higher level of integrity protection than provided by typical event logs

Note 1 to entry: Audit logs are used to protect against claims that repudiate responsibility for an action.

3.1.8
authenticate
verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

[SOURCE: IEC TS 62443-1-1:2009, 3.2.12]

3.1.9
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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.13]

3.1.10
authorization
right or permission that is granted to a system entity to access a system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14]

3.1.11
availability
ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided

Note 1 to entry: This ability depends on the combined aspects of the reliability performance, the maintainability performance and the maintenance support performance.

Note 2 to entry: Required external resources, other than maintenance resources do not affect the availability performance of the item.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.16, modified – (performance) removed after the term.]

3.1.12
batch production
production process where products or components are produced in batches and where each separate batch consists of a number of the same products or components

[SOURCE: EN 14943:2005]

3.1.13
conduit
logical grouping of communication assets that protects the security of the channels it contains

Note 1 to entry: This is analogous to the way that a physical conduit protects cables from physical damage.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.27]

3.1.14
confidentiality
assurance that information is not disclosed to unauthorized individuals, processes, or devices

[SOURCE: IEC TS 62443-1-1:2009, 3.2.28]

3.1.15
continuous production
production that is running at a steady rate

[SOURCE: ISO 2859-3:2005, 3.1.1, modified – The word "running" has been added and the Note has been deleted.]

3.1.16
cybersecurity
actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.36]

3.1.17
data confidentiality
property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes

[SOURCE: IEC TS 62443-1-1:2009, 3.2.37]

3.1.18
data integrity
property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.38]

3.1.19
denial of service
prevention or interruption of authorized access to a system resource or the delaying of system operations and functions

Note 1 to entry: In the context of industrial automation and control systems, denial of service can refer to loss of process function, not just loss of data communications.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.42]

3.1.20
device
independent physical entity capable of performing one or more specified functions in a particular context and delimited by its interfaces

[SOURCE: IEC 61804-2:2018, 3.1.18]

3.1.21
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

[SOURCE: IEC TS 62443-1-1:2009, 3.2.43]

3.1.22
discrete manufacturing
method of manufacturing where products are manufactured in a non-continuous manner, e.g. automobiles, appliances, computers

[SOURCE: EN 14943:2005]

3.1.23
entity
thing (physical or non-physical) having a distinct existence

[SOURCE: ISO/IEC 20924:2021, 3.1.18]

3.1.24
functional requirement
specification of a behaviour that a solution or part of a solution shall perform

3.1.25
host
computer that is attached to a communication sub-network or inter-network and can use services provided by the network to exchange data with other attached systems

[SOURCE: IEC TS 62443-1-1:2009, 3.2.56]

3.1.26
Identifier
ID
information that unambiguously distinguishes one entity from other entities in a given identity context

[SOURCE: IEC 60050-741: 2020, 741-01-21]

3.1.27
impact
evaluated consequence of a particular event

Note 1 to entry: Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss, and recovery costs.

3.1.28
incident
event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

3.1.29
industrial automation and control systems
IACS
collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process

Note 1 to entry: These systems include, but are not limited to:

– industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (SIS) functions, whether they are physically separate or integrated.)

– associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.

– associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.57]

3.1.30
manufacturing
all life cycle activities and procedures involved in the design, production, and support of manufacturing systems and of manufactured products

3.1.31
nonrepudiation
security service that provides protection against false denial of involvement in a communication

[SOURCE: IEC TS 62443-1-1:2009, 3.2.72]

3.1.32
privilege
authorization or set of authorizations to perform specific functions, especially in the context of a computer operating system

EXAMPLE Functions that are controlled through the use of privilege include acknowledging alarms, changing setpoints, modifying control algorithms.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.78]

3.1.33
process
set of activities performed with a set of resources to realize an objective within a specified timeline

[SOURCE: ISO 22400-1:2014, 2.1.8]

3.1.34
product
result of labour or of a natural or industrial process

[SOURCE: IEC 61360-1:2017, 3.1.23]

3.1.35
public key certificate
set of data 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

3.1.36
resilience
ability of an IACS organization, process entity or system, to resist being affected by disruptions

3.1.37
risk
combination of the probability of occurrence of harm and the severity of that harm

3.1.38
risk assessment
process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure

Note 1 to entry: Types of resources include physical, logical and human.

Note 2 to entry: Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and quantify the associated risk. They are carried out initially and periodically to reflect changes in the organization's risk tolerance, vulnerabilities, procedures, personnel and technological changes.