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 It also gives information on projects, replaced and withdrawn publications.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

Warning! Make sure that you obtained this publication from an authorized distributor.

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.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88]

3.1.39
security

a) measures taken to protect a system

b) condition of a system that results from the establishment and maintenance of measures to protect the system

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.99]

3.1.40
smart
capable of some independent action

3.1.41
system
set of interrelated elements considered in a defined context as a whole and separated from its environment

Note 1 to entry: Such elements may be both material objects and concepts as well as the results thereof (e.g. forms of organization, mathematical methods, and programming languages).

Note 2 to entry: The system is considered to be separated from the environment and other external systems by an imaginary surface, which can cut the links between them and the considered system.

[SOURCE: IEC 61804-2:2018, 3.1.65]

3.1.42
system of systems
set or arrangement of systems that results when independent systems are integrated into a larger system

3.1.43
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

3.1.44
use case
specification of a set of actions performed by a system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system

[SOURCE: ISO/IEC 19505-2:2012, 16.3.6]

3.1.45
zone
grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization

Note 1 to entry: All unqualified uses of the term “zone” in this document should be assumed to refer to a security zone.

[SOURCE: IEC 62443-3-2:2020, 3.1.25, modified – Note 1 to entry is different.]

3.2 Abbreviated terms and acronyms

AC	Identification and Authentication Control (Defined as a security functional requirement in IEC TS 62443-1-1)
ACS	Automation and Control System
CAD	Computer Aided Design
CAPP	Computer Aided Production Planning
DC	Data Confidentiality (Defined as a security functional requirement in IEC TS 62443-1-1)
FMEA	Failure Mode and Effects Analysis
FR	Foundational Requirement
IACS	Industrial Automation and Control System
IIoT	Industrial Internet-of-Things
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IP	Intellectual Property
ISMS	Information Security Management System
KPI	Key Performance Indicator
RA	Resource Availability (Defined as a security functional requirement in IEC TS 62443-1-1)
RDF	Restricted Data Flow (Defined as a security functional requirement in IEC TS 62443-1-1)
SI	System Integrity (Defined as a security functional requirement in IEC TS 62443-1-1)
SM	Smart Manufacturing
TRE	Timely Response to Events (Defined as a security functional requirement in IEC TS 62443-1-1)
UC	Use Control (Defined as a security functional requirement in IEC TS 62443-1-1)

4 Smart Manufacturing challenges for cybersecurity

Smart Manufacturing bears some new challenges with regard to automation control system (ACS) security. Compared to classic manufacturing systems the following characteristics of smart manufacturing systems have an impact on cybersecurity:

- **Multiple stakeholders**: The ACS is no longer under the control of a single stakeholder. Instead multiple stakeholders need to interact, e.g., product owner, owner of production equipment, production process owner, data analytics service providers. The security mechanisms used need to be able to support multiple stakeholders and to balance and protect their potentially opposing interests.

- **Continuous change**: A smart manufacturing system is subject to continuous change and reconfiguration, e.g., functional enhancements, changes of production equipment, change of the product being produced, process optimization. The boundaries between different lifecycle phases become blurred (especially product design, engineering, operation). The security of the system needs to accommodate these changes, including while in transition, and adjust accordingly.
- **Intensive use of digital data (digitalization)**: Smart Manufacturing systems produce and process a vast amount of control and other digital data. Product and process design data (e.g., Computer Aided Design (CAD), Computer Aided Production Planning (CAPP)), sensor data, engineering data, equipment self-descriptive data, simulation model data, which have formerly been kept on distinct systems are now an intrinsic part of the manufacturing system. This increases data exposure and makes it more susceptible to attack. Potential attackers either draw direct benefits from that data (e.g., product or process/algorithmic intellectual property (IP)), gain competitive advantages (key performance indicator (KPI) data), or use captured data to develop more sophisticated attacks (e.g., by working with simulation models, that themselves need to have restricted access).
- **Architecture**: The classic automation pyramid dissolves and it is transformed into a structured automation network relying on service-oriented paradigms. New architectural concepts arise from, e.g., IEC PAS 63088:2017 [3] (RAMI 4.0), ISO/IEC 30141:2018, IoT – Reference architecture [13], ISO/IEC 30166:2020, IoT – Industrial IoT [14]. This requires adjustments in the corresponding security architecture.
- **Application of new communication technologies in manufacturing**: The adaption of wireless networking such as Wi-Fi and 3GPP technologies (LTE, 5G) for smart manufacturing allows increased flexibility (e.g., easy relocation of production equipment). However, wireless networks need to provide well-defined performance. With new communication infrastructure paradigms, such as software defined networking (SDN) and 5G, enabling easy remote communications and in some cases communication across the IEC PAS 63088 [3] levels according to IEC 62264 (all parts) or IEC 61512 (all parts) [16]. For example, Field device sensors (level 1) are potentially allowed to directly communicate to the enterprise/connected world (level 4) bypassing traditional pyramid layers.

This report is mainly based on the evaluation of a subset of smart manufacturing use cases. Further work is required but not limited to, e.g., extending the evaluation on a larger set of use cases. Also, this work needs to be aligned with other work taking place in the rapid developing field of smart manufacturing cybersecurity.

5 Systems engineering

Smart Manufacturing facilities are complex integrated systems of systems. They are engineered by deploying the processes, activities and tasks defined in ISO/IEC/IEEE 15288:2015 [7]. Some System Engineering processes need a specific consideration from the cybersecurity point of view. This happens when activities of these processes will use cybersecurity related inputs or produce cybersecurity related outputs. Table 1 below identifies processes and activities concerned. It proposes specific aspects that have to be taken into consideration as far as cybersecurity is concerned.

Table 1 – ISO/IEC/IEEE 15288 System engineering process

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical management processes			
Project planning	The purpose of the Project Planning process is to produce and coordinate effective and workable plans. This process determines the scope of the project management and technical activities, identifies process outputs, tasks and deliverables, establishes schedules for task conduct, including achievement criteria, and required resources to accomplish tasks. This is an ongoing process that continues throughout a project, with regular revisions to plans.	Security objectives and plans are defined; Roles, responsibilities, accountabilities, authorities for security aspects are defined; Resources and services necessary to achieve the security objectives are formally requested and committed.	
Project Assessment and Control	The Project Assessment and Control process provides for monitoring the extent of achievement of the requirements and critical quality characteristics and communicating the results to stakeholders and managers.	Security performance measures or assessment results are available; Adequacy of roles, responsibilities, accountabilities and authorities for security aspects is assessed; Adequacy of security related resources is assessed; Technical progress reviews including security objectives achievement are performed; Deviations in security performance from plans are investigated and analysed; Affected stakeholders by security concerns are informed of project status; Corrective action is defined and directed, when security achievement is not meeting targets; Security objectives are achieved.	Define a Security Plan for describing the Security strategy in relation to the System Engineering management plan
Decision Management process	The Decision Management process provides assessment of alternative requirements, architecture characteristics and design characteristics against the decision criteria, including the critical quality characteristics. Results of these comparisons are ranked, via a suitable selection model, and are then used to decide on an optimal solution	Decisions requiring alternative security analysis are identified; A preferred security strategy is selected.	Trade off Security constraints and requirements in the concept and development stage to optimise the achievement of stakeholders needs.

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical management processes			
Risk Management	The Risk Management process, in its entirety, provides for identifying, evaluating, and handling risks of the system, including those related to meeting the critical quality characteristics.	Security vulnerabilities leading to risks are identified; Risk treatment options are identified, prioritised and selected for security vulnerabilities; Appropriate security measures as implemented.	Identify, assess, mitigate risk related to security, all along the system life cycle
Configuration Management	The purpose of the Configuration Management process is to manage and control system elements and configurations over the life cycle. Configuration Management also manages consistency between a product and its associated configuration definition.	Security related items requiring configuration management are defined; Changes to security related items under configuration management are controlled.	
Information Management	The Information Management process, in its entirety, provides for the specification, development and maintenance of information items for documenting and communicating the extent of achievement. Note that information items used for the purpose of critical quality characteristics are sometimes specialized in nature. Sources for the description of these information items include industry associations, regulators, and specific standards.	Security related information to be managed is identified; Security related information representations are defined. Security related information is obtained, developed, transformed, stored, validated, presented and disposed of. Security related information is available to designated stakeholders.	Document al the security outputs all along the system life cycle.
Measurement	The purpose of the Measurement process is to collect, analyze, and report objective data and information to support effective management and demonstrate the quality of the products, services, and processes.	An appropriate set of security metrics, based on the security related information needs are identified or developed; Required security data is collected, verified and stored; The security data is analysed and the results interpreted; Security related information items provide objective information that support decision.	

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical management processes			
Quality Assurance	The purpose of the Quality Assurance process is to help ensure the effective application of the organization's Quality Management process to the project. Quality assurance focuses on providing confidence that quality requirements will be fulfilled. Proactive analysis of the project cycle processes and outputs is performed to assure that the product being produced will be of the desired quality and that organization and project policies and procedures are followed.	Evaluations of the project's security related products, services, and processes are performed, consistent with quality management policies, procedures and requirements; Results of security evaluations are provided to relevant stakeholders; Security incidents are resolved.	

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical processes			
Business and Mission Analysis	The Business and Mission Analysis process provides for the definition of the problem space and characterization of the solution space, including the relevant trade-space factors and preliminary life cycle concepts. This includes developing an understanding of the context and any key parameters, such as the critical quality characteristics (e.g., security threats, safety hazards, human interfaces, operational characteristics, and system assurance context).	The security aspects of the problem or opportunity space are defined; The security solution space is characterised; Preliminary operational security concepts and other concepts in the life cycle stages are defined; Candidate alternative security solution classes are identified and analysed; The preferred candidate alternative security solution class(es) are selected; Traceability of security related business or mission problems and opportunities and the preferred alternative security solution classes is established.	Capture business and operational context, identify missions, and capabilities, operational scenarios. Define Preliminary stakeholder domain objectives (Business, safety, image, etc…) with regards to operational scenarios, perform preliminary cybersecurity vulnerability analysis

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
		Technical processes	
Stakeholder Needs and Requirements Definition	The Stakeholder Needs and Requirements Definition process provides for the selection and definition of characteristics, including critical quality characteristics, and associated information items. The activities and the documentation are useful in identifying, prioritizing, defining, and recording requirements for the critical quality characteristics.	Stakeholders of the system concerned by security are identified; Required security characteristics and context of use of capabilities and concepts in the life cycle stages, including operational concepts, are defined; Security constraints on a system are identified; Stakeholders security needs are defined; Stakeholders security needs are prioritized and transformed into clearly defined stakeholders requirements; Critical security performance metrics are defined; Stakeholder agreement that their security needs and expectations are reflected adequately in the requirements is achieved; Any enabling systems or services needed for stakeholders needs and requirements area available; Traceability of stakeholder requirements to stakeholders and their needs is established.	Preliminary analysis; define stakeholder domain objectives and preliminary requirements per domain. Initiate a System Security Plan (SSecP) in order to formalize the Security strategy in the context of the system.
System Requirements Definition	The System Requirements Definition process provides for the specification of parameters for the critical quality characteristics and the selection of measures for tracking the achievement of these requirements with respect to the specific system to be developed.	The system description, including system interfaces, security functions and boundaries, for a system solution is defined. Security related system requirements (functional, performance, process, non-functional, and interface) and design constraints are defined; Critical security performance metrics are defined; The security system requirements are analysed; Traceability of security system requirements to stakeholder security requirements is developed.	Define accurately Security objectives by a likelihood/severity matrix, for different undesirable behaviours of the system for different operational scenarios. Undesirable behaviours are to be identified for each operational scenario considering also undesired control actions. Validate the System Security Plan

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical processes			
Architecture Definition	The Architecture Definition process provides for the identification of stakeholder concerns from an architecture perspective. These concerns often translate into expectations or constraints across the life cycle stages that relate to the critical quality characteristics, such as utilization (e.g., availability, security, effectiveness, usability), support (e.g., repairability, obsolescence management), evolution of the system and of the environment (e.g., adaptability, scalability, survivability), production (e.g., manufacturability, testability), retirement (e.g., environmental impact, transportability), etc. This process further addresses those critical quality characteristic requirements that drive the architecture decisions, including the assessment of the architecture with respect to the concerns and associated characteristics.	Identified stakeholders security concerns are addressed by the architecture; A security architecture viewpoint is developed; A security architecture model is developed for the system; Concepts, properties, characteristics, behaviours, functions, or constraints that are significant to security architecture decisions of the system are allocated to architectural entities; Security related system elements and their interfaces are defines; Security architecture candidates are assessed; A security architectural basis for processes throughout the life cycle is achieved; Alignment of the security architecture with security requirements and design characteristics is achieved; Traceability of security related architecture elements to stakeholder and system security requirements is developed.	Perform Preliminary Security Countermeasures Analysis Validation of requirements that flow down in an engineered security architecture, considering not only what is required for the nominal countermeasures in each of the operational scenarios, but also what is required in case the countermeasure is not applied or applied too early, too late or not properly (failure mode and effects analysis (FMEA), Fault tree)
Design Definition	The Design Definition process provides for the determination of necessary design characteristics, which includes the critical quality characteristics, such as security of design criteria for the specialty characteristics and the evaluation of alternative designs with respect to those criteria.	Design characteristics of each security related system element are defined; Security system requirements are allocated to system elements; Interfaces between security related system elements composing the system are defined or refined; Design alternatives for security related system elements are assessed; Traceability of the design characteristics of security related elements to the architectural entities of the system architecture is established.	Perform security analysis at system and sub system level, including operational, functional and physical architecture point of view

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical processes			
System Analysis	The System Analysis process provides for the level of analysis needed to understand the trade space with respect to the critical quality characteristics through the conduct of mathematical analysis, modelling, simulation, experimentation, and other techniques. The analysis results are input to trade-offs made through the Decision Management process in support of other Technical processes.	System security analysis needed are identified; System security analysis assumptions and results are validated; System security analysis results are provided for decisions; Traceability of the system security analysis results is established.	Ensure confidence that system security critical failure likelihood is compliant with stakeholder objectives. Complete System security Analysis and Subsystem Security Analysis ensuring consistency through a Hazard Threat and Vulnerability Tracking System
Implementation	The Implementation process provides for recording the evidence that critical quality requirements have been met.	Implementation constraints that influence system security requirements, architecture, or design are identified.	In addition, for the development of complex components (i.e. not possible to be 100% tested), once countermeasures have been exhaustively defined, a bespoke level of process assurance can be added. Specific integrity or assurance level is assigned to complex components by reference to existing standards agreed during the agreement process
Integration	The Integration process provides for planning the integration, including the considerations for critical quality characteristics, and the assurance that the achievement of the characteristics is determined and recorded.	Integration constraints that influence system security requirements, architecture, or design, including interfaces are identified; Approach and checkpoints for the secure operation of the assembled interfaces and system functions are defined; The interfaces between the implemented system security related elements that compose the system are checked; Integration security results and anomalies are identified; Traceability of the integrated system security related elements is established.	Complete System security Analysis and Subsystem Security Analysis ensuring consistency through a Hazard Threat and Vulnerability Tracking System
Verification	The Verification process, provides for the planning and execution of a strategy to perform verification, including the critical quality characteristics. The selected verification strategy can introduce design constraints that could affect the achievement of the characteristics.	Constraints of verification that influence system security requirements, security architecture, or design are identified; The system or system security related element is verified; Objective evidence that the realized system fulfils the security requirements, architecture, and design is provided; Security aspects verification results and anomalies are identified.	Complete System security Analysis and Subsystem Security Analysis ensuring consistency through a Hazard Threat and Vulnerability Tracking System. Verify Security requirements and define a Security Assessment report

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical processes			
Transition	The Transition process provides for installing the system in its operational environment. Because some specialty properties involve a trade-off between design constraints and operational constraints, attention to installation is often important.	Transition constraints that influence system security requirements, architecture, or design, are identified; Operators, users and other stakeholders necessary to the system utilization and support are trained on security aspects; Security transition results and anomalies are identified; The installed system is activated and ready for secure operation.	Complete System security Analysis and Subsystem Security Analysis ensuring consistency through a Hazard Threat and Vulnerability Tracking System. Verify Security requirements and define a Security Assessment report
Validation	The Validation process provides evidence that the services provided by the system meet the stakeholders' needs, including the critical quality characteristics.	Validation criteria for stakeholder security requirements are defined; The availability of security services required by stakeholders is confirmed; Security constraints of validation that influence system requirements, architecture, or design are identified; The system or system security related element is validated; Security aspects validation results and anomalies are identified; Objective evidence that the realised system or system elements satisfies stakeholder security needs is provided.	Verify and Validate Security requirements and complete a Security Assessment Report
Operation	Use the system to deliver its services	Operations constraints that influence system security requirements, architecture, or design are identified; Security trained, qualified operators are available; System security services that meet stakeholder requirements are delivered; System security performance during operation is monitored.	Timely response to security events protecting confidentiality, integrity and availability of the system of the system.
Maintenance	Sustain the capability of the system to provide a service	Maintenance constraints that influence system security requirements, architecture, or design are identified; Replacement, repaired, or revised security related system elements are made available; The security need for changes to address corrective, perfective or adaptive maintenance is reported; Failure and lifetime security data, including associated costs, is recorded.	Test and implement security patches to address vulnerabilities

Processes ISO/IEC/IEEE 15288:2015	Purpose	Security aspects of engineering outcomes	Security activities considerations
Technical processes			
Disposal	Sustain the capability of the system to provide a service	Disposal security constraints are provided as inputs to requirements, architecture, design and implementation.	Purging sensitive information from decommissioned parts of the system and ensuring remaining parts will continue to meet their security requirements.

6 Applying IEC 62443 (all parts) to smart manufacturing

6.1 General

IEC 62443 is a series of standards for industrial cybersecurity.

While originating from the automation industry many domains (e.g., automation, power distribution, mobility, …) are now interested in using IEC 62443 (all parts).

IEC 62443 (all parts) extends over the entire life cycle of a production system and provides requirements for product suppliers, integrators, service providers, as well as system operators.

This approach makes IEC 62443 (all parts) an attractive standard to be used for the definition of security requirements for smart manufacturing systems that are either composed of or need to interface with components from different domains.

Figure 1 shows the published and the ballot approved parts of the IEC 62443 series, other parts and updates are in progress.

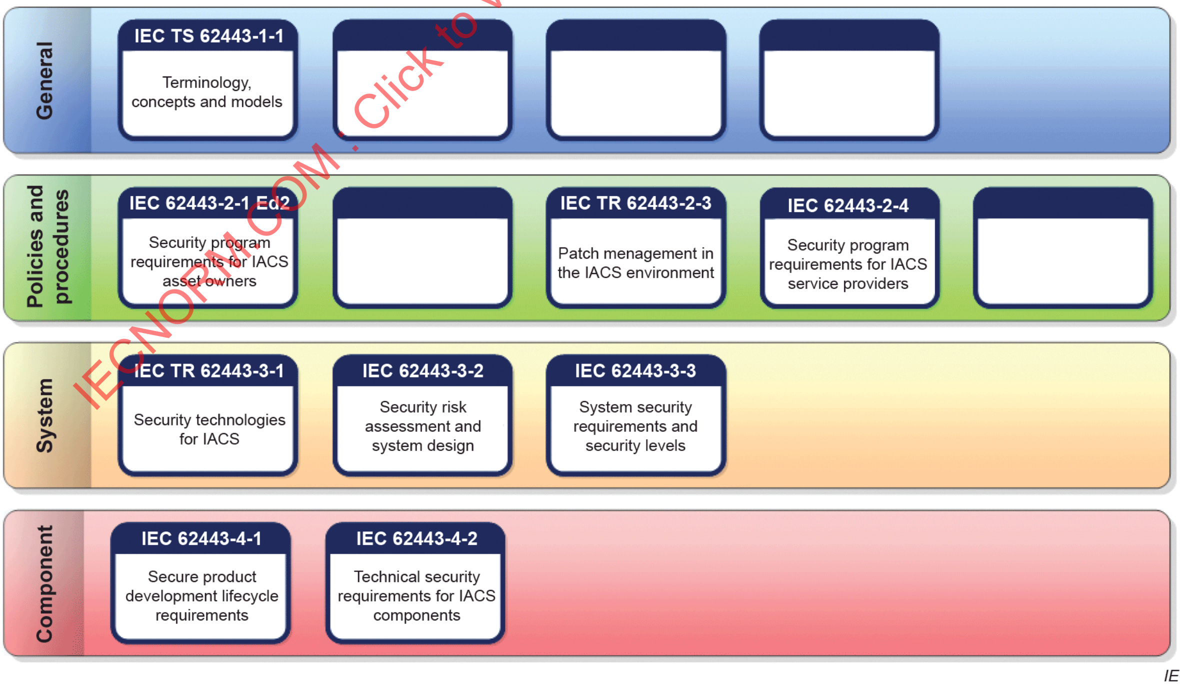

General
IEC TS 62443-1-1
Terminology, concepts and models
Policies and procedures
IEC 62443-2-1 Ed2
Security program requirements for IACS asset owners
IEC TR 62443-2-3
Patch menagement in the IACS environment
IEC 62443-2-4
Security program requirements for IACS service providers
System
IEC TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Secure product development lifecycle requirements
IEC 62443-4-2
Technical security requirements for IACS components
IEC

Figure 1 – The IEC 62443 series

The fundamental concepts outlined in IEC 62443 (all parts) also apply to the implementation of a security programme (IEC TS 62443-1-1, ISO/IEC 27000:2014 [20]) for a smart manufacturing system. This document provides guidance on the application of IEC 62443 (all parts) in smart manufacturing systems.

Within the scope of smart manufacturing, the standard could be applied to components, devices, systems, systems of systems, enterprises, and smart manufacturing artifacts (e.g., products).

Figure 2 shows how the individual parts of IEC 62443 (all parts) are applied in detail during the individual life cycles of automation assets (supply, integrate, operate).

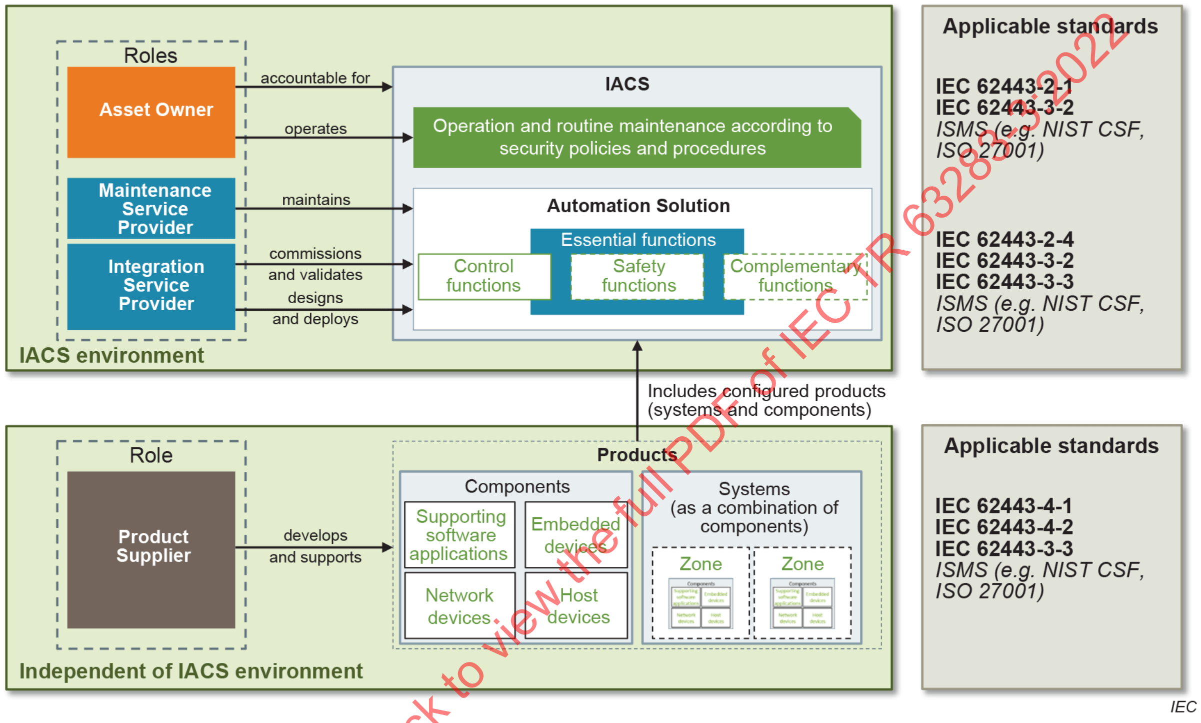


Figure 2 – Details of the application of individual parts of IEC 62443 by different roles during the individual life cycles of automation assets

Figure 2 illustrates how IEC 62443 (all parts) addresses different stakeholders such as product suppliers, integrators, service providers, as well as system operators. This holistic approach of IEC 62443 (all parts) also makes it well suited for smart manufacturing systems as boundaries between the individual phases (especially integration and operation) will blur.

6.2 Relation to ISO/IEC 27000 (all parts)

Security within an organization is very often deployed first from an ISMS (Information Security Management System) security perspective using ISO/IEC 27001 [21] and ISO/IEC 27002 [22] in addition with a sector specific document. The process is structured around a risk analysis and an implementation of a risk management program. In the case of industrial activity, the scope often includes an IACS (Industrial Automation and Control System) with some specific operational, safety and availability constraints. The cybersecurity approach of this ACS is very often dealt with independently from ISMS.

From a cybersecurity in depth perspective, the ACS and ISMS systems need to be considered as a system of systems in which the evaluation of the security takes place. From the point of cybersecurity the combined individual systems raise different requirements, restrictions, and risks (e.g., confidentiality, integrity). Indeed, there are many system functions that are often addressed by the ISMS part and directly impact the cybersecurity of the operational part. As the systems become more and more digital, the border between the two organizations (IT and OT) tends to become more and more blurred.

A first approach to this is addressed in the IEC 62443-2-1, which provides a mapping of the ISO/IEC 27001 and ISO/IEC 27002 controls to the IEC 62443 requirements, covering either the system, product, or the service provider aspects. In case of critical infrastructures a more in-depth analysis and risk assessment needs to be performed to also address the safety, availability and real time operational issues.

6.3 Reference model

While the general reference model given in IEC TS 62443-1-1:2009, Clause 6 provides a good framework to organize the different functional aspects of a smart manufacturing system, it would be supportive to address also examples for connected smart manufacturing system architectures different from the classic automation pyramid shown in IEC TS 62443-1-1:2009, Figure 16.

6.4 Foundational requirements

IEC 62443 (all parts) defines seven foundational requirements (FRs) that need to be addressed in order to implement cybersecurity for ACS. These foundational requirements do also apply to smart manufacturing systems. The foundational requirements as given in IEC TS 62443-1-1 are:

1) Access Control (AC): control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
2) Use Control (UC): control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
3) Data Integrity (DI): ensure the integrity of data on selected communication channels to protect against unauthorized changes.
4) Data Confidentiality (DC): ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
5) Restrict Data Flow (RDF): restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
6) Timely Response to Event (TRE): respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission-critical or safety-critical situations.
7) Resource Availability (RA): ensure the availability of all network resources to protect against denial of service attacks.

While in classic systems sensitive user data is typically not exposed to the automation system, this will change with smart manufacturing. The importance of protecting the privacy of user data will increase for smart manufacturing systems (e.g., lot-size-one in pharmaceutics). It is not required to have a completely new foundational requirement for privacy as this can be covered with FR4 (Data Confidentiality) and FR5 (Restricted Data Flow) for smart manufacturing systems. Other FR may need to be developed when new threats become apparent. Such other FR need to be developed in cooperation with TC 65/WG 10.

6.5 Zones and conduits in system of systems

Zones and conduits are an important concept of IEC 62443. The idea behind zones and conduits is to divide a complex automation system into several (nested) subsystems. A zone is a group/subsystem composed of automation assets (devices) based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization. Communication among devices within a zone or between zones takes place using so called conduits (see IEC TS 62443-1-1 for examples).

While zones can be defined according to different characteristics, typical implementations/installations attempt to group production system belonging to a zone into an enclosed physical location (e.g., several devices locally organized in a production line are organized within a zone). Smart production devices in smart automation systems are likely to be deployed more flexibly. For example, a robot participates in the production process of several production lines, automated intelligent vehicles moving all around the factory replace the fixed installation of conveyor belts, software services used in the automation system are deployed remotely (cloud).

Moreover, smart manufacturing systems may use changed architectural blueprints. New technologies such as wireless, 5G, and software defined networks allow reduction of the physical hierarchy and complexity and decoupling the physical network topology from the functional hierarchy as defined in IEC 62264 (all parts) [15]. Zones and conduits need to adapt for these kinds of architectures and communication infrastructures.

IEC TS 62443-1-1 mentions virtual zones and conduits. Virtual zones and conduits are not bound by physical location. Virtual zones and conduits are a potential concept to be used for smart manufacturing systems.

IEC 62443-3-2 does not yet elaborate on virtual zones and conduits or give any hints on how zones and conduits are applied to smart manufacturing systems.

The focus for system segmentation for smart manufacturing systems needs to be shifted from physical access and proximity towards logical separation which is based on access control and virtual network isolation supported by cryptographic means. There needs to be further guidance on the definition and implementation of virtual zones and conduits.

6.6 Security risk assessment and security levels

It is the goal of the security risk assessment to identify the scope and degree of required security activities and mechanisms to protect the essential functions of the manufacturing system (cf. Figure 2). Security risk assessment for a smart manufacturing system is no longer focused on a specific product and production process – security ratings and security requirements need to be dynamically adjusted depending on the actual use of the manufacturing system. A prerequisite for the envisioned flexible production is that the smart manufacturing system can provide and adjust to a requested security level. A smart manufacturing system constitutes a system-of-systems. Smart components are integrated to smart devices forming a smart system and so on. There needs to be an efficient and well-defined process to determine the security level of a composed system.

6.7 Security lifecycle

The **security lifecycle** of a smart manufacturing system needs to be aligned with the lifecycle model of a smart manufacturing system. As observed above, the boundaries between lifecycle phases will disappear. How the IEC 62443 security lifecycle model (see IEC TS 62443-1-1:2009, Figure 19) integrates with the flexible lifecycles of a smart manufacturing system undergoing continuous reconfigurations needs to be defined. The complete path throughout those transitions needs to be secure.

6.8 Auditing and logging

Auditing and logging for smart manufacturing scenarios needs further investigation. Components (including products) are dynamically added and removed from the manufacturing system and/or move between different manufacturing systems. Audit and logging needs to keep track of these operations. In addition, it needs to be assured that audit and logging data stored on these components stays available when a component is no longer accessible. At least IEC 62443-2-4 and IEC 62443-4-2 need to be considered. Applicability of other standards needs further evaluation.

6.9 Conclusion

The following items summarize the recommendations with regards to the further improvement of the existing IEC 62443 series of standards for smart manufacturing:

1) Align on use of specific terms and definitions, esp. as far as components, products, and systems are concerned to avoid misunderstandings (cf. IEC 63283-1).
2) Extension of virtual zones and conduits concept of IEC 62443 to adopt to logical/virtual topologies which are equivalent to that of the physical manufacturing system.
3) Adjustment of Risk Assessment and Security Levels of IEC 62443, e.g., a manufacturing system is enable to switch between different (predefined) security levels depending on the actual production context (e.g., product being produced).
4) Aligning Security management activities of IEC 62443 (IEC 62443-2-1:2010, 4.3.4.1 Figure 5) with lifecycle of Smart Manufacturing systems, esp. giving guidance to what extent flexible reconfiguration is to be considered in the initial system design and can be handled within the maintenance process.
5) Considering the product and its data being an integral part of the production system (e.g., carrying production data, providing feedback data), hence the product being manufactured takes part in the manufacturing process.
6) Extension of Auditing and Logging of IEC 62443 (all parts) (cf. 6.8).

7 Smart Manufacturing security threats

7.1 General

This section identifies potential security risks of smart manufacturing systems. The analysis takes a threat-based approach. A threat describes an action performed by an attacker that will result in the violation of one of the following IACS protection goals:

- Availability – the automation system is able to execute its intended function. The production not disturbed by (intentional) attacks
- Integrity – the automation system behaves as intended and all data used in the production system is not tampered with or modified by unauthorized entities
- Confidentiality – certain data, e.g., product, processing, or machine intellectual property, customer private data, KPIs, is not disclosed to unauthorized entities

To capture a wide coverage of potential threats this document makes use of the following viewpoints:

- Use Case View – Discusses potential threats relevant for several Use Cases described in IEC TR 63283-2 [2][2].
- Lifecycle View – Discusses potential threats caused by additional life-cycle interdependencies of smart manufacturing systems.

[2] Numbers in square brackets refer to the Bibliography.

The threats turning up in different views are not mutually exclusive, e.g., a threat relevant to a specific use case also occurs for life-cycles or features related to that use case.

7.2 Use case view on cybersecurity

7.2.1 General

Clause 7 analyses a set of selected use cases with respect to cybersecurity. The analyzed use cases originate from IEC TR 63283-2 [2]. Additional use cases have been defined by the taskforce to illustrate a specific security issue. The selection of use cases is intended to provide an overview on smart manufacturing specific security threats and challenges. The challenges are categorized according to the foundational requirements given in IEC 62443 (all parts) as described in 6.4.

Where applicable the figures from IEC TR 63283-2 [2] showing the technical perspective of the use case have been reused and annotated to illustrate to which interactions and/or assets the identified threats apply. Note that the location of these assets and occurrence of interactions within the system heavily depends on the implementation and deployment of the actual smart manufacturing system. So does the analysis of security threats and risks. The following 7.2.2 to 7.2.13 cannot replace a threat and risk analysis for a real system. The intention is to provide some security guidance when turning these abstract use cases into an actual system.

Further use cases will be added as the understanding of smart manufacturing and smart manufacturing security advances. Annex A provides an overview of the analysed use cases and foundational requirements being addressed.

7.2.2 Use case "Manufacturing of individualized products"

Manufacturer wants to offer individualized products requested by customer based on an adaptable production system to better address customer respective market needs.

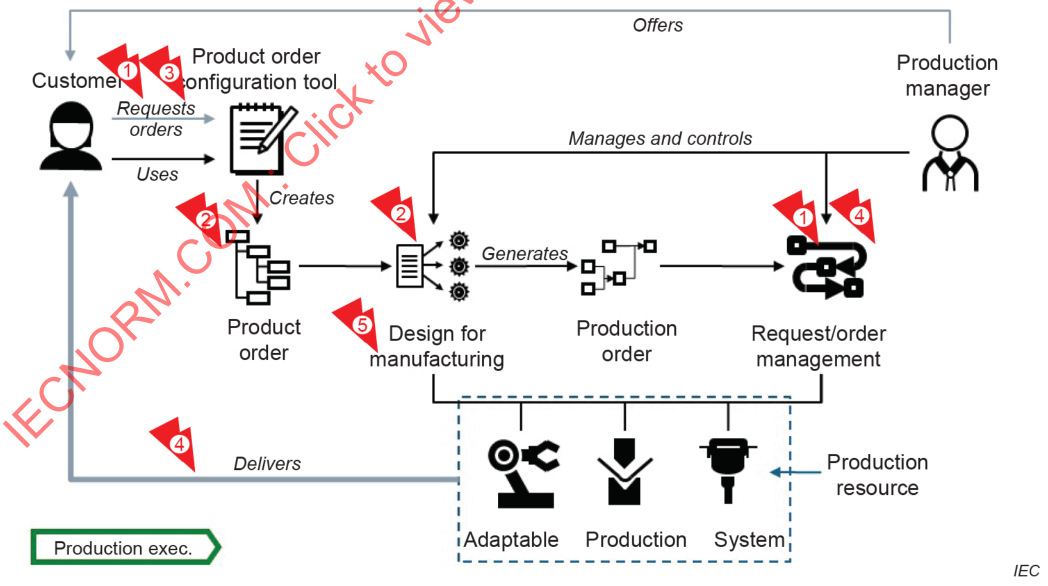


Figure 3 – Use case "Manufacturing of individualized products"

Figure 3 shows possible points of attack. The potential threats and security challenges are detailed in Table 2.

Table 2 – Use case “Manufacturing of individualized products”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker gets access to confidential customer data (e.g., individual recipes, customer specific preferences, address data, …)	Confidentiality	DC01 Privacy of customer data – ensure confidentiality of sensible customer data (privacy) RDF01 Need-to-know flow of customer data – ensure that customer data is only made available on a need-to-know basis	Customer individual product data
2	Attacker/manufacturer gets access to confidential product data (esp. in the scenario “offering manufacturing services; e.g., BoM, PoP). The data can be used to extract IP or produce extra/counterfeit products.	Confidentiality	DC05 Confidentiality of product intellectual property DI11 Ensure genuineness of semi-finished and finished products	Increased level of detail of product data being exposed within the manufacturing system.
3	Attacker repudiates the individual order. Product has to be disposed/sold at a lower price.	Integrity	AC01 Authentication of the customer – ensure authenticity of the order.	Orders are exchanged between different security domains (e.g., sub-suppliers). Customer specific orders are less likely to find alternative demand.
4	Attacker manipulates delivery process – e.g., to get hold of a higher value product instead the one actually ordered. Someone else receives the wrong product.	Integrity	AC01 Authentication of the customer DI01 Data integrity of exchanged data – ensure authenticity and integrity of the order. Appropriate concepts need to be found or developed in cooperation with the logistics domain.	Orders are exchanged between different security domains (e.g., sub-suppliers)

Ref	Threat	Protection Goal	Challenge	SM Specific?
5	Attacker comes up with a product order exploiting a (known) error/shortcoming in the design of the manufacturing process to impair production system (e.g., exceeding actual limitations of the production system)	Availability	DI12 Data integrity with respect to known boundary conditions – implement input validation, do only accept product orders within a well-defined range of variations TRE03 Audit logging for security monitoring and forensics – keep full record of product orders	The customer order directly impacts the production process (e.g., passing a recipe, digital product model)

7.2.3 Use case "Standardization of production technologies"

Manufacturer requests for production resources complying to semantically defined production capabilities in order to improve the efficiency and flexibility of the production (for example by outsourcing or insourcing of production orders).

Production resource supplier wants to offer production resources complying to semantically defined production capabilities, but also wants to be able to offer unique selling propositions.

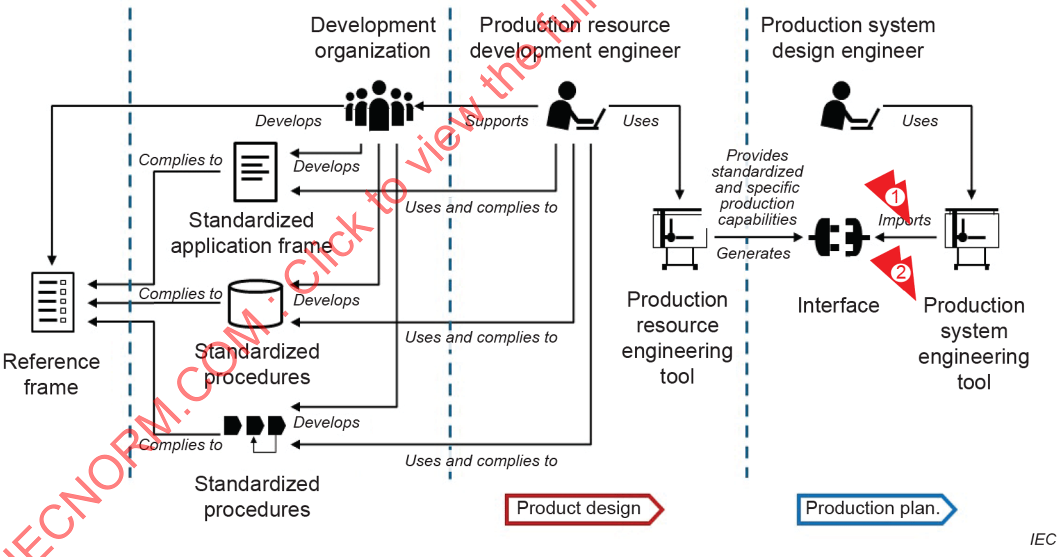


Figure 4 – Use case "Standardization of production technologies"

Figure 4 shows possible points of attack. The potential threats and security challenges are detailed in Table 3.

Table 3 – Use case "Standardization of production technologies"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Disclosure of detailed construction plans (e.g., 3D models) within the production network.	Confidentiality	DC05 Confidentiality of product intellectual property – Ensure confidentiality of IP contained in construction plans	Digitized information exchanged within production system allows easy reproduction. Different IP stakeholders involved (construction plan for product, production technique, operator)
2	Disclosure of third party product, production, or processing know how (e.g., 3D models, technology data) while being used/processed by a manufacturing device.	Confidentiality	DC07 Trusted execution - third party providers of production know-how need to be ensured that their IP is not compromised by the production devices using it.	Production device and production techniques can be decoupled (e.g., product models, technology data dynamically provided by independent parties)

7.2.4 Use case "Flexible scheduling and resource allocation"

Production manager wants to minimize down time (outages) and optimize the usage of production resources.

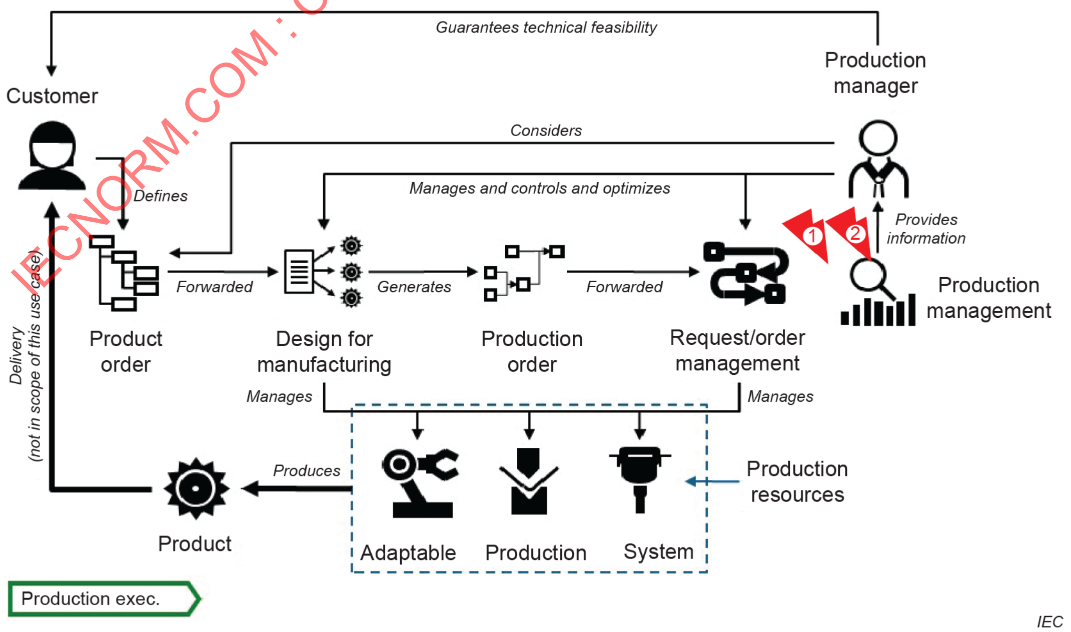


Figure 5 – Use case "Flexible scheduling and resource allocation"

Figure 5 shows possible points of attack. The potential threats and security challenges are detailed in Table 4.

Table 4 – Use case "Flexible Scheduling and resource allocation"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker spoofs (unexpected) event resulting in rescheduling of automation system.	Integrity	AC06 Authentication of rescheduling demanders UC01Use Control of production plan DI04 Data integrity of production plans – Rescheduling of production plan needs to be initiated/confirmed by authorized party.	Constant change is a feature – derivations from the intended behaviour are not obvious to human operators.
2	Attacker manipulates information on available production resources making the manufacturer unable to fulfil his assurances.	Integrity Availability	DI04 Data integrity of production plans TRE02 Timely response when system is only partially available	Dynamic adoption to available resources instead of fixed resource allocation.

7.2.5 Use case "Modularization of production system"

Manufacturer wants to setup an adaptable production system based on interchangeable production resources to better react on changing customer respective market demands.

A new field component adds itself automatically into an existing production system.

The production system is reconfigured because, e.g.,

- The product has to be made using different equipment due to availability (e.g. unexpected downtime of a scheduled machine)
- The equipment is reconfigured in order to make a different product

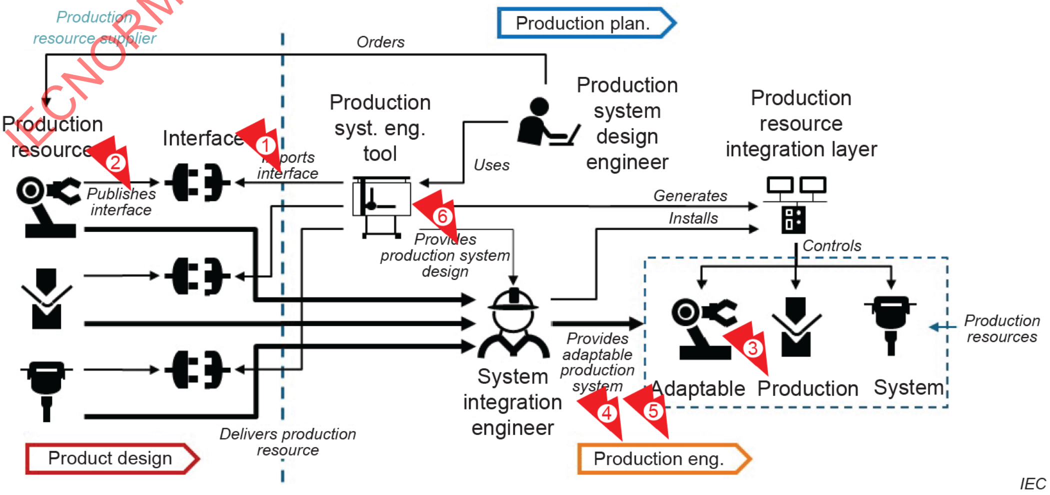

Production resource supplier
Orders
Production plan.
Production resource
Interface
Imports interface
Publishes interface
Production syst. eng. tool
Uses
Production system design engineer
Production resource integration layer
Generates
Installs
Controls
Provides production system design
System integration engineer
Provides adaptable production system
Adaptable Production System
Production resources
Delivers production resource
Product design
Production eng.
1
2
3
4
5
6
IEC

Figure 6 – Use case "Modularization of production system"

Figure 6 shows possible points of attack. The potential threats and security challenges are detailed in Table 5.

Table 5 – Use case "Modularization of production system"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Field device adds itself to the production system and accesses confidential information not intended for this device.	Confidentiality	UC05 Use Control of field devices – The new field device access permissions need to be set according to its intended task in the production process.	Security bootstrapping process. The device is initially unknown but requires sufficient permissions to integrate/interact with the existing system.
2	New field device impersonates another field device (e.g., offers functionality it cannot actualy provide) in order to get access to confidential information.	Confidentiality	AC02 Authentication of devices/sensors – Device needs to provide authenticated information about its identity and properties/functionalities.	No dedicated engineering processes.
3	(Compromised) new field device disturbs the production process.	Availability	UC05 Use Control of field devices – The new field device access permissions need to be set according to its intended task in the production process. RDF02 Task oriented data flow restriction – Communication range of new device need to be restricted according to its intended task in the production process.	
4	Attacker exploits intermediate states which do not have a defined security level.	Confidentiality, Integrity	DI06 System integrity during transitions – Verify that the complete path through the transition is secure. This potentially excludes several (optimal) transition paths. For example, instead of directly transitioning from A to B it is required to go through an additional state C in order to stay secure.	Reconfiguration of existing production system during operation.

Ref	Threat	Protection Goal	Challenge	SM Specific?
5	Attacker takes benefit of protection gap of individual devices during transition, e.g., zone protection may fail while a device is relocated.	Integrity	DI07 End-point self-contained basic protection – For ACS systems with static engineering it is often assumed that a device is located in a dedicated zone of trust and protected by the perimeter of that zone. This assumption does no longer hold for all smart manufacturing systems. Each device needs to provide some basic self-protection on a restricted functional level. Some advanced functionality is not offered after the device was able to verify that certain (security) conditions are met by the environment.	Individual devices/endpoints can no longer rely on a stable operational environment
6	Attacker defines a new configuration state (or redefines an old one) which can be exploited more easily	Integrity	DI03 Data integrity of new functions/configurations – New configuration needs to be validated and authorized before being implemented AC04 Authentication of configuration change providers – Only authorized sources are able to initiate configuration changes.	Configuration changes are normal and therefore not always suspicious

7.2.6 Use case “Feedback loops”

Manufacturing company wants that a customer (respective market) feeds experience from usage (respective perception) of the delivered product back to the manufacturing company to optimize the offering to the customer (respective market).

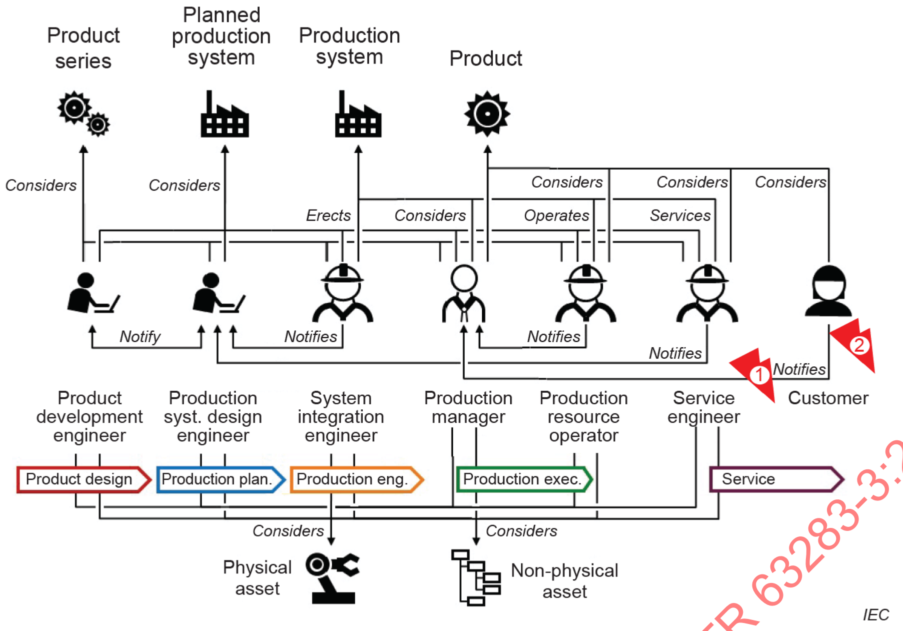


Figure 7 – Use case “Feedback loops”

Figure 7 shows possible points of attack. The potential threats and security challenges are detailed in Table 6.

Table 6 – Use Case “Feedback loops”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker/consumer feeds back invalid data into the production process.	Integrity	AC01 Authentication of the customer – ensure authenticity/reliability of feedback data between customer domain and production domain	Connected smart products are part of the whole lifecycle (cf. IEC PAS 63088 product layer). Especially direct use of customer data in a feedback look is new.
2	Attacker builds end-customer profile (e.g., behaviour, location) based on feedback data.	Confidentiality	DC01 Privacy of customer data – protect privacy of collected end user data.	

7.2.7 Use case “Simulation in operation”

Production manager wants to simulate a model of the production to optimize production, to check the principle feasibility, to reduce security risks resulting from reconfigurations of the production system and/or speed-up reconfigurations of the production system.

Focus of the security analysis is the use of current data within predefined simulation models.

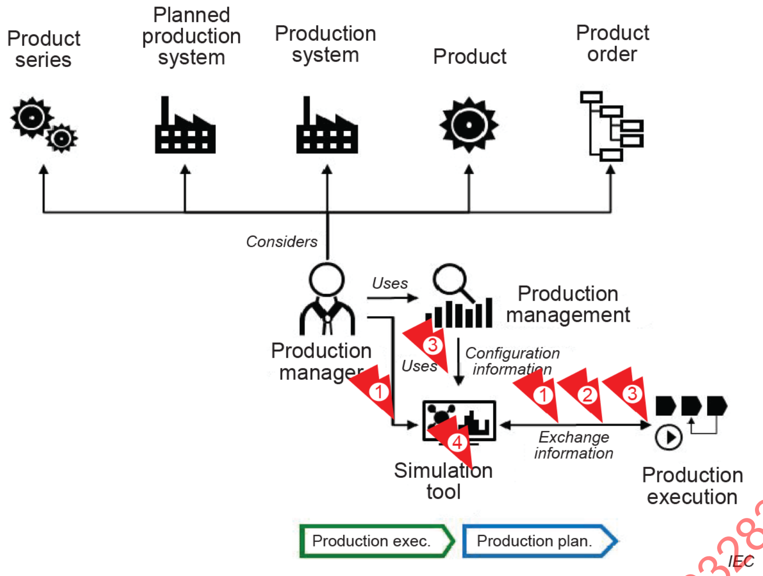


Figure 8 – Use case "Simulation in operation"

Figure 8 shows possible points of attack. The potential threats and security challenges are detailed in Table 7.

Table 7 – Use case "Simulation in operation"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Simulation data is used by an attacker/competitor to analyze the production process in order to gain a competitive advantage.	Confidentiality	DC03 Confidentiality of simulation model data – Keep simulation model and data confidentiality	Constant exchange of data increases the exposure of critical data.
2	Attacker disturbs the information exchange between simulation model and actual production system and inhibits timely decisions	Availability	RA01 Availability of current simulation data – Ensure that simulation runs on current data	Smart Manufacturing offers simulation in order to support critical decisions.
3	Attacker feeds invalid data into simulation model in order to induce incorrect decisions (e.g., a production runs out of supply)	Integrity, Availability	AC03 Authentication of simulation data providers UC03 Use Control of simulation model – Only properly identified and authorized parties provide data for the simulation	
4	Attacker manipulates the simulation model in order to induce incorrect decisions	Integrity	DI02 Data integrity of simulation model – Integrity of simulation model (and system running the simulation) needs to be ensured.	

7.2.8 Use case “Simulation in design and engineering”

Plant designer engineer wants to simulate a model of the designed production system to reduce security risks resulting from production system engineering and/or to speed-up production system engineering.

Focus of the security analysis is the creation and distribution of simulation models for an actual production system.

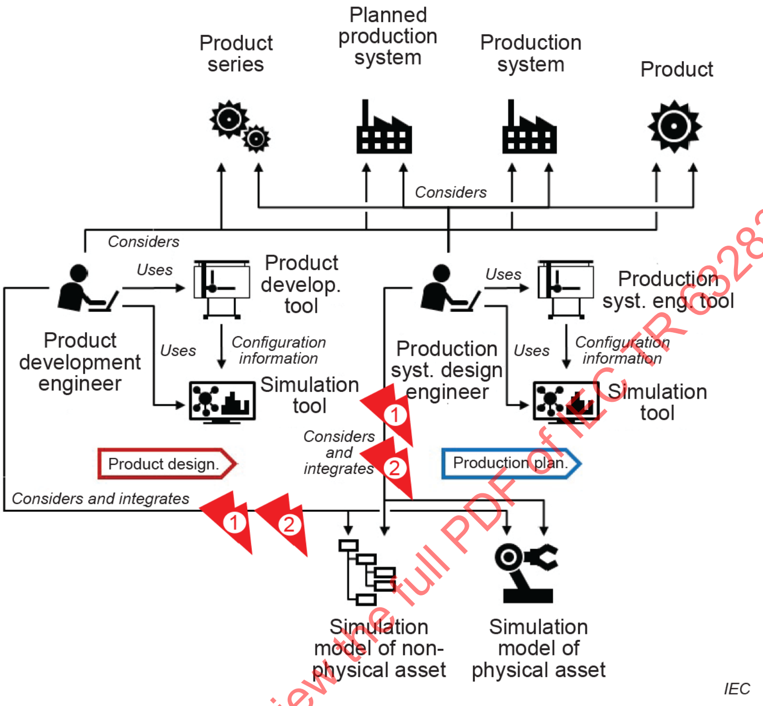

Product series
Planned production system
Production system
Product
Considers
Considers
Uses
Product develop. tool
Product development engineer
Uses
Configuration information
Simulation tool
Uses
Production syst. eng. tool
Production syst. design engineer
Uses
Configuration information
Simulation tool
Considers and integrates
Product design.
Production plan.
Considers and integrates
1
2
1
2
Simulation model of non-physical asset
Simulation model of physical asset
IEC

Figure 9 – Use case “Simulation in design and engineering”

Figure 9 shows possible points of attack. The potential threats and security challenges are detailed in Table 8.

Table 8 – Use case “Simulation in design and engineering”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Virtual plant simulation is used by an attacker to evaluate potential vulnerabilities of the OT system and prepare an attack on the actual production system.	Confidentiality	UC03 Use Control of simulation model – Restrict access to simulation model	Availability of comprehensive and current digitized factory model.
2	Simulation model is used by an attacker/competitor to analyze the production process in order to gain a competitive advantage.	Confidentiality	DC03 Confidentiality of simulation model data – Keep simulation model and data confidentiality	Availability of comprehensive and current digitized factory model.

7.2.9 Use cases “Update and functional scalability of production resources” and “Device configuration”

The objective of “Update and functional scalability of production resources” is that the production resource supplier provider wants to offer additional functionality based on software, which can be unlocked after the production resource was sold and already used by a manufacturer to create additional revenue streams. Manufacturer wants to use only that functionality of a production resource, which is necessary for his specific purpose, but wants to be able to react on market changes very flexible by upgrading (or even downgrading) a production resource.

The objective of "Device configuration" is that the Software application provider wants to offer software applications which can be flexibly deployed to devices or to a generic computing infrastructure.

Potential threats and security challenges are detailed in Table 9.

Table 9 – Use case "Update and functional scalability of production resources", Use case "Device configuration"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker/customer uses advanced manufacturing functionality without having paid for it.	Integrity	UC04 Use Control of production capabilities – Only authorized users access specific production capabilities	Functionality is no longer solely determined by hardware but becomes "software defined"
2	Attacker installs malicious additional functionality having a negative impact on the machine or its environment.	Integrity, Availability	AC07Authentication of providers for functional enhancements DI03 Data integrity of new functions/configurations – New functionality needs to be verified and authorized before being installed.	
3	Attacker reverse engineers/extracts IP from functional update. Note: Functional update may even be provided by different stakeholder than the device, e.g., as an app.	Confidentiality	DC05 Confidentiality of product intellectual property – protect know how of updates installed and operated in potentially hostile execution environments	Functional enhancements added to devices by independent third parties.

7.2.10 Use case "Information extraction from production systems"

Manufacturer wants to collect information of a production system in a side-effect free and easy way in order to analyse and process this information using a generic computing infrastructure

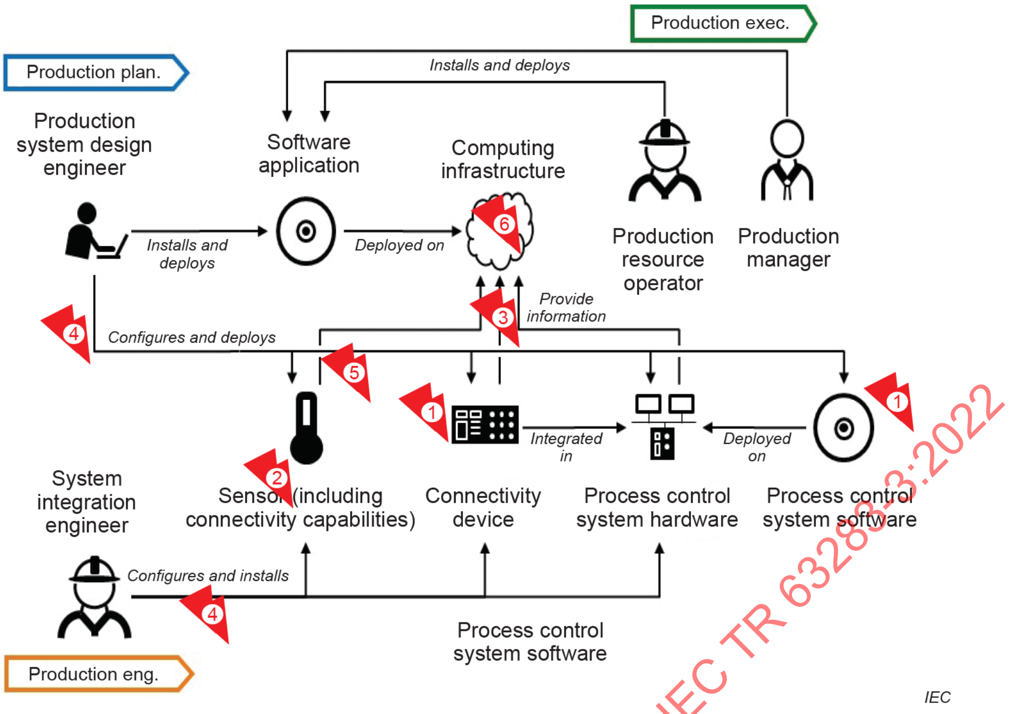


Figure 10 – Use case "Information extraction from production systems"

Figure 10 shows possible points of attack. The potential threats and security challenges are detailed in Table 10.

Table 10 – Use case "Information extraction from production systems"

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker spoofs device or sends own or modified data to backend service and misleads analytics.	Integrity	AC02 Authentication of devices/sensors AC09 Authentication of sensor data DI08 Integrity of collected and aggregated sensor data – Especially the integrity for aggregated data in case the raw data is no longer available needs to be addressed.	
2	Attacker places counterfeited sensor or smart sensor aggregation device (e.g., EDGE analytics) in production system providing invalid sensing results.	Integrity	DI09 Ensure genuineness of installed devices/sensors	Direct connectivity from sensor to backend (e.g., cloud analytics)
3	Attacker intercepts sensor data exchanged with backend system.	Confidentiality	DC02 Confidentiality of data on the network	

Ref	Threat	Protection Goal	Challenge	SM Specific?
4	Attacker changes sensor configuration in a way that data unintentionally leaves the production system.	Integrity	UC05 Use Control of field devices – Protect configuration of device/sensor parameterization parameters	
5	Manipulated sensor sends (raw) data to backend service which was not intended to leave the production system.	Confidentiality	RDF03 Limitation of (raw) sensor data flow/exposure – The customer/operator of the system is enabled to decide which data is provided to external service providers.	
6	Collected sensor data (e.g., video streams) are misused to track personnel, build staff (performance) profiles, ….	Confidentiality	DC08 Privacy of employee/staff related/relatable sensor data	

7.2.11 Use case “Self-optimization of production resources”
Use case “Optimization of operation through machine learning”
Use case “Optimization in design and engineering through machine learning”

Data analytics applies machine learning (ML) technologies (e.g., artificial neural networks) on large data amounts collected by field devices and smart sensors (7.2.9).

Potential threats and security challenges are detailed in Table 11.

Table 11 – Use case “Machine learning”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker provides manipulated training or test data to introduce a bias into the ML system.	Integrity	DI10 Integrity of (collected and aggregated sensor) data used for ML training and testing	Use of ML
2	Attacker provides manipulated input data to ML system to provoke untrained/undefined behaviour (input data not covered by the training data)	Integrity	DI08 Integrity of collected and aggregated sensor data	Use of ML
3	Attacker extracts confidential information originally contained in the training data from the AI model.	Confidentiality	DC09 Exposure of confidential data contained in ML training data	Use of ML and training data.
4	Attacker tries to benefit from uncertainty of human operator arising from missing explainability of AI results.	Availability Integrity	TRE06 Ensure explainability of ML system proposals/instructions	Taking decisions based on ML system output

7.2.12 Use case “Design for energy efficiency”
Use case “Optimization of energy”

Production manager wants to optimize the operation of the production system according to specific KPIs related to energy efficiency, for example energy consumption and/or energy costs.

Potential threats and security challenges are detailed in Table 12.

Table 12 – Use case “Design for energy efficiency”, Use case “Optimization of energy”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker manipulates the system while shutdown. The manipulation is not noticed as security systems/solutions are also affected by the shutdown or are not available during power-off. This may also happen unintentionally.	Integrity Availability	RA05 Availability of sensors and monitoring – Sensors required for security monitoring need to be kept online and continuously monitored. DI05 Data integrity of engineering data – Whatever is needed to verify the integrity of the system at design time now needs to be available also at operation time.	Opportunistic shutdown of part of the system while in operation.
2	Attacker uses an unprotected function for energy management and powers down (part of) the production system.	Availability	AC04 Authentication of configuration change providers – Only authorized sources are able to initiate changes. UC05 Use Control of field devices – provide access control for device power management functions or smart switches	
3	Attacker uses shutdown to physically access a device (e.g., due to reduced physical security during shutdown) and retrieves confidential data from the device.	Confidentiality	RDF04 Limit temporal availability of information, e.g., delete information after use	

7.2.13 Use case “Seamless models”

Manufacturer has an interest in managing the increasing technical complexity of products and production systems to make balanced and secured decisions, to improve the workflows and to reduce the total costs.

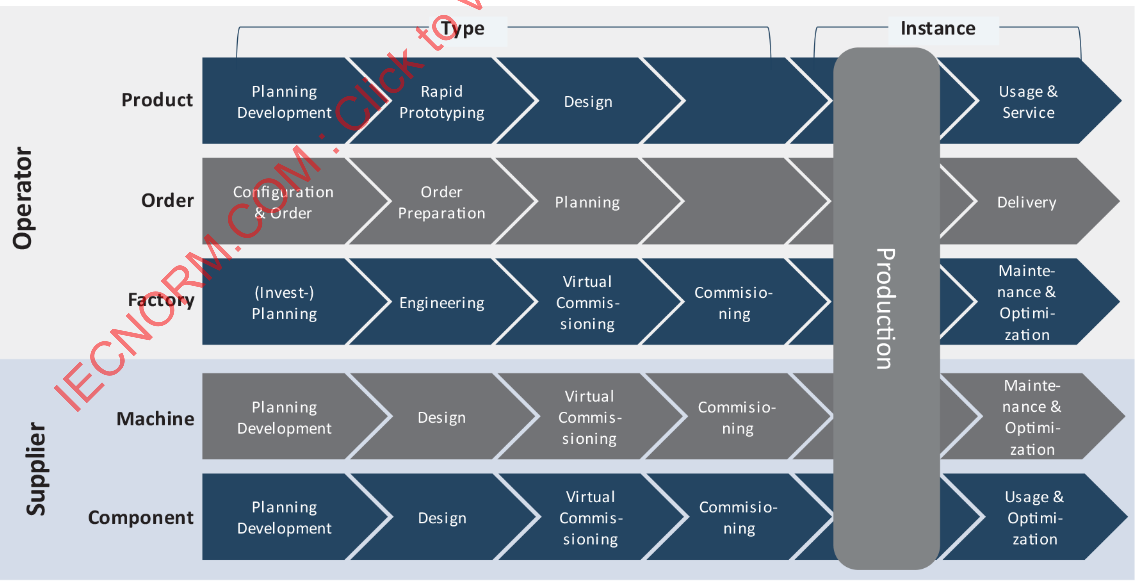
Potential threats and security challenges are detailed in Table 13.

Table 13 – Use case “Seamless models”

Ref	Threat	Protection Goal	Challenge	SM Specific?
1	Attacker gets access to sensitive engineering and design data (e.g., CAD models, construction plans) usually not exposed on the OT system.	Confidentiality	DC04 Confidentiality of engineering data – the used exchange format provides means to protect the confidentiality of the data UC02 Use Control of information – only authorized entities are able to access the protected information	Digitized information exchanged within production system allows easy reproduction.
2	Attacker manipulates engineering and/or design data in order to downgrade the production process or product quality.	Integrity	DI01 Data integrity of exchanged data – the used exchange format provides means of integrity protection	

7.3 Smart Manufacturing lifecycle view on cybersecurity

Smart Manufacturing requires close interaction between processes belonging to different life-cycle tracks. As shown in Figure 11, the different tracks do not only interact during production but exchange information among each other over their entire lifetime.



Source: based on Plattform Industrie 4.0 AG 1 / based on Prof. Bauernhasl, Fraunhofer IPA

IEC

Figure 11 – From Value Streams to Value Networks

The Smart Manufacturing Lifecycle View on Cybersecurity is shown in Table 14.

Table 14 – Smart Manufacturing Lifecycle View on Cybersecurity

Lifecycle Process under attack	Threat	Challenge
Configuration & Order	Attacker eavesdrops production schedule information transmitted to the factory across the internet, e.g., to gain competitive advantages	DC02 – e.g., encrypt network data or use VPN DC01 – protect confidentiality of customer order information stored on SM assets DC10 – protect configuration of production schedule stored on SM assets
Planning	Attacker changes production schedule information transmitted to the factory across the internet, e.g., to cause production delays or overproduction	DC02 – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange
Maintenance & Optimization	Attacker changes production performance information transmitted from the factory across the internet, e.g., to cause financial harm to the company (missed orders or unneeded overproduction)	DC02 – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange
Usage & Service	Attacker eavesdrops information transmitted to the company from smart products reporting maintenance and warranty status across the internet, e.g., to identify customers and their reported problems	DC02 – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange
Optimization	In order to increase performance (e.g., to speed up order processes) the level of protection is decreased. Attacker eavesdrops information transmitted from the factory to suppliers or from smart production equipment, reporting maintenance and warranty status across the internet, e.g., to identify competition equipment and run rates, and to identify production equipment that could be replaced (targeted sales)	DC – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange
Design, Planning	Attacker eavesdrops information transmitted to the factory about product definitions and manufacturing instructions across the internet, e.g., to steal intellectual property	DC02 – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange
Design, Planning	Attacker changes information transmitted to the factory about product definitions, manufacturing instructions, or quality test specifications across the internet, e.g., to cause company brand harm, harm to customers, or harm to production equipment.	DC02 – e.g., encrypt network data or use VPN AC05, UC06 – only authenticated and authorized entities are allowed to participate in the information exchange

8 Summary of challenges

8.1 General

TF cybersecurity performed a – not yet exhaustive – threat analysis for smart manufacturing based on a selection of smart manufacturing use cases, life-cycle processes, and features. The following 8.2 to 8.8 provide a brief overview on the basic challenges that need to be addressed to be able to build a secure smart manufacturing system.