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.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
2 Normative references 8
3 Terms, definitions, abbreviated terms and acronyms 8
3.1 Terms and definitions 8
3.2 Abbreviated terms and acronyms 15
4 Smart Manufacturing challenges for cybersecurity 15
5 Systems engineering 16
6 Applying IEC 62443 (all parts) to smart manufacturing 24
6.1 General 24
6.2 Relation to ISO/IEC 27000 (all parts) 25
6.3 Reference model 26
6.4 Foundational requirements 26
6.5 Zones and conduits in system of systems 27
6.6 Security risk assessment and security levels 27
6.7 Security lifecycle 27
6.8 Auditing and logging 28
6.9 Conclusion 28
7 Smart Manufacturing security threats 28
7.1 General 28
7.2 Use case view on cybersecurity 29
7.2.1 General 29
7.2.2 Use case “Manufacturing of individualized products” 29
7.2.3 Use case “Standardization of production technologies” 31
7.2.4 Use case “Flexible scheduling and resource allocation” 32
7.2.5 Use case “Modularization of production system” 33
7.2.6 Use case “Feedback loops” 35
7.2.7 Use case “Simulation in operation” 36
7.2.8 Use case “Simulation in design and engineering” 38
7.2.9 Use cases “Update and functional scalability of production resources” and “Device configuration” 38
7.2.10 Use case “Information extraction from production systems” 39
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” 41
7.2.12 Use case “Design for energy efficiency” Use case “Optimization of energy” 41
7.2.13 Use case “Seamless models” 42
7.3 Smart Manufacturing lifecycle view on cybersecurity 43
8 Summary of challenges 44
8.1 General 44
8.2 Identification and Authentication Control (AC) 45
8.3 Use Control (UC) 45
8.4 Data and System Integrity (DI) 47
8.5 Data Confidentiality (DC) 48
8.5.1 General 48

8.5.2 Intended Use 48
8.5.3 Data Confidentiality 49
8.6 Restricted Data Flow (RDF) 49
8.7 Timely Response to Events (TRE) 49
8.8 Resource Availability (RA) 50
Annex A (informative) Mapping use cases to foundational requirements 51
Annex B (informative) Secure identities 52
Bibliography 53

Figure 1 – The IEC 62443 series 24
Figure 2 – Details of the application of individual parts of IEC 62443 by different roles during the individual life cycles of automation assets 25
Figure 3 – Use case “Manufacturing of individualized products” 29
Figure 4 – Use case “Standardization of production technologies” 31
Figure 5 – Use case “Flexible scheduling and resource allocation” 32
Figure 6 – Use case “Modularization of production system” 33
Figure 7 – Use case “Feedback loops” 36
Figure 8 – Use case “Simulation in operation” 37
Figure 9 – Use case “Simulation in design and engineering” 38
Figure 10 – Use case “Information extraction from production systems” 40
Figure 11 – From Value Streams to Value Networks 43
Figure 12 – Lifecycles, users/stakeholders, granted privileges, and views 46
Figure 13 – Privacy and Intended Use 48

Table 1 – ISO/IEC/IEEE 15288 System engineering process 17
Table 2 – Use case “Manufacturing of individualized products” 30
Table 3 – Use case “Standardization of production technologies” 32
Table 4 – Use case “Flexible Scheduling and resource allocation” 33
Table 5 – Use case “Modularization of production system” 34
Table 6 – Use Case “Feedback loops” 36
Table 7 – Use case “Simulation in operation” 37
Table 8 – Use case “Simulation in design and engineering” 38
Table 9 – Use case “Update and functional scalability of production resources”, Use case “Device configuration” 39
Table 10 – Use case “Information extraction from production systems” 40
Table 11 – Use case “Machine learning” 41
Table 12 – Use case “Design for energy efficiency”, Use case “Optimization of energy” 42
Table 13 – Use case “Seamless models” 43
Table 14 – Smart Manufacturing Lifecycle View on Cybersecurity 44
Table 15 – Identification and Authentication Control (AC) challenges 45
Table 16 – Use Control (UC) challenges 46
Table 17 – Data and System Integrity (DI) challenges 47
Table 18 – Data Confidentiality (DC) challenges regarding privacy 48
Table 19 – Data Confidentiality (DC) requirements other than privacy 49

Table 20 – Restricted Data Flow (RDF) challenges 49
Table 21 – Timely Response to Events (TRE) challenges 50
Table 22 – Resource Availability (RA) challenges 50
Table A.1 – Mapping use cases to foundational requirements 51

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*