

**Project Acronym:** STAR  
**Grant Agreement number:** 956573 (H2020-ICT-2020-1 – Research and Innovation Action)  
**Project Full Title:** Safe and Trusted Human Centric Artificial Intelligence in Future Manufacturing Lines  
**Project Coordinator:** INTRASOFT International



Funded by the Horizon 2020  
Framework Programme of the  
European Union

## DELIVERABLE

### D2.3 – Review of Applicable Standards and Regulations

<b>Dissemination level</b>	PU -Public
<b>Type of Document</b>	Report
<b>Contractual date of delivery</b>	30/09/2021
<b>Deliverable Leader</b>	R2M
<b>Status - version, date</b>	Final – v1.0, 30/09/2021
<b>WP / Task responsible</b>	WP2
<b>Keywords:</b>	Standards, Regulations, Directives, Architectures

*This document is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 956573. It is the property of the STAR consortium and shall not be distributed or reproduced without the formal approval of the STAR Management Committee. The content of this report reflects only the authors' view. The European Commission is not responsible for any use that may be made of the information it contains.*

## Executive Summary

This deliverable provides a review of industrial standards relating to Artificial Intelligence (AI) in manufacturing, including recommendations for human-centric manufacturing systems and safety, security, and data management related technical standards. The objective is to highlight some of the most relevant standards, while detailing the possible considerations when designing and developing AI applications for the manufacturing industry such as those developed in the STAR<sup>1</sup> project.

This deliverable, also, provides for an overview of the most relevant EU regulations that are either already applicable or at the proposal stage and may, thus, create an impact for the manufacturing industry, including in relation to those applications envisioned under STAR. Finally, a series of reference architectures and infrastructures that may be useful to developers and users of innovative technologies in the manufacturing industry are also presented.

This deliverable provides a brief entry point for the interested user and technology provider, who can take advantage of the information in this document to access the standards and directives and plan how to apply them in their organization.

---

<sup>1</sup> STAR - Safe and Trusted Human Centric Artificial Intelligence in Future Manufacturing Lines (<https://star-ai.eu/>)

<b>Deliverable Leader:</b>	R2M
<b>Contributors:</b>	Arthurs’ Legal, Intrasoft, Ubitech, RUG, Philips
<b>Reviewers:</b>	Siemens, JSI
<b>Approved by:</b>	Charalampos Ipektsidis, John Soldatos (INTRASOFT)

<b>Document History</b>			
<b>Version</b>	<b>Date</b>	<b>Contributor(s)</b>	<b>Description</b>
0.1	17/02/2021	R2M	Initial version + Table of Contents
0.2	08/03/2021	R2M	Design of methodology
0.3a	26/03/2021	RUG, Philips	List of relevant standards
0.3b	09/04/2021	Ubitech, Intrasoft	List of relevant standards and architectures
0.4	12/04/2021	R2M	Tables with relevant standards and regulation
0.5	20/04/2021	Arthur’s Legal	Initial contribution on Directives and regulations
0.6a	12/05/2021	Intrasoft	Contribution on Architectures
0.6b	31/05/2021	R2M	Initial batch of Standards
0.7	25/06/2021	Arthur’s Legal	Regulation and directive analysis
0.8a	18/08/2021	R2M	Final batch of Standards
0.8b	10/09/2021	R2M, Arthur’s Legal	Guidelines and recommendations
0.9a	13/09/2021	R2M	Final integrated version for review
0.9b	23/09/2021	JSI, Siemens	Final Reviewed Version
1.0	30/09/2021	INTRA	QA and submitted version

# Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>2</b>
<b>TABLE OF CONTENTS.....</b>	<b>4</b>
<b>TABLE OF FIGURES.....</b>	<b>5</b>
<b>DEFINITIONS, ACRONYMS AND ABBREVIATIONS .....</b>	<b>6</b>
<b>1 INTRODUCTION.....</b>	<b>8</b>
1.1 SCOPE AND OBJECTIVES .....	8
1.2 OUTLINE.....	8
<b>2 METHODOLOGY .....</b>	<b>9</b>
2.1 METHODOLOGY FOR THE REGULATORY DISCUSSION.....	9
2.2 METHODOLOGY FOR STANDARDS AND ARCHITECTURES .....	10
<b>3 EU REGULATIONS.....</b>	<b>12</b>
3.1 CONTEXT .....	12
3.2 ANALYSIS OF REGULATIONS RELEVANT FOR STAR .....	14
3.2.1 <i>CyberSecurity Regulations</i> .....	14
3.2.2 <i>Privacy Regulations</i> .....	17
3.2.3 <i>Safety Regulations</i> .....	19
3.2.4 <i>Other Applicable Regulations and recommendations</i> .....	22
3.2.5 <i>Proposed Regulations</i> .....	23
3.3 GUIDELINES AND RECOMMENDATIONS .....	26
<b>4 STANDARDS AND ARCHITECTURES .....</b>	<b>28</b>
4.1 CONTEXT .....	28
4.2 ANALYSIS OF STANDARDS .....	29
4.2.1 <i>Technical, Management and Security Standards</i> .....	29
4.2.2 <i>Safety and Health Standards</i> .....	36
4.2.3 <i>Other Relevant Standards</i> .....	41
4.3 INDUSTRIAL ARCHITECTURES AND INFRASTRUCTURES.....	45
4.3.1 <i>Reference Architecture Models</i> .....	45
4.3.2 <i>Infrastructures for Industrial Systems</i> .....	50
4.4 GUIDELINES AND RECOMMENDATIONS .....	50
<b>5 CONCLUSION.....</b>	<b>52</b>
<b>6 REFERENCES.....</b>	<b>53</b>

## Table of Figures

FIGURE 1: POSITION IN DATA FLOW .....	9
FIGURE 2: REFERENCE ARCHITECTURE MODEL INDUSTRY 4.0 (RAMI 4.0).....	47
FIGURE 3: FUNCTIONAL DOMAINS IN THE IIRA .....	48
FIGURE 4: BDVA REFERENCE ARCHITECTURE MODEL FOR BIGDATA ANALYTICS AND MACHINE LEARNING.....	50

## Definitions, Acronyms and Abbreviations

Acronym/ Abbreviation	Title
<b>WP</b>	Work Package
<b>AI</b>	Artificial Intelligence
<b>AMQP</b>	Advanced Message Queue Protocol
<b>B2MML</b>	Business to Manufacturing Markup Language
<b>BDVA</b>	Big Data Value Association
<b>CM</b>	Conceptual Model
<b>CPPS</b>	Cyber Physical Production Systems
<b>CRM</b>	Customer Relationship Management
<b>DXF</b>	Drawing Interchange Format
<b>ERP</b>	Enterprise Resource Planning
<b>ETSI</b>	European Telecommunications Standards Institute
<b>FDI</b>	Factory Design and Improvement
<b>IEC</b>	International Electrotechnical Commission
<b>IGES</b>	Initial Graphics Exchange Specification
<b>IIC</b>	Industrial Internet Consortium
<b>IIoT</b>	Industrial Internet of Things
<b>IoT</b>	Internet of Things
<b>IRTF</b>	Internet Research Task Force
<b>ISMS</b>	Information Security Management System
<b>ISO</b>	International Organization for Standardization
<b>ITU-T</b>	International Telecommunication Union
<b>OAGIS</b>	Open Applications Group Integration Specification
<b>OOEF</b>	OASIS Open Europe Foundation
<b>OT</b>	Operational Technology
<b>MES</b>	Manufacturing Execution System
<b>ML</b>	Machine Learning
<b>MQTT</b>	Message Queue Telemetry Protocol
<b>NIST</b>	National Institute of Standards and Technology
<b>PLC</b>	Programmable Logic Controller
<b>PLM</b>	Product Lifecycle Management
<b>PPR</b>	Product, Process, Resource
<b>RA</b>	Reference Architecture
<b>RAMI4.0</b>	Reference Architecture Model Industrie 4.0
<b>SAI</b>	Securing Artificial Intelligence
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SCM</b>	Supply Chain Management
<b>SDO</b>	Standards Development Organization
<b>SSO</b>	Standards Setting Organization
<b>TOSCA</b>	Topology and Orchestration Specification for Cloud Applications
<b>VRML</b>	Virtual Reality Modelling Language
<b>W3C</b>	World Wide Web Consortium
<b>XKMS</b>	Xml Key Management Specification

<b>XML</b>	eXtensible Markup Language
------------	----------------------------

# 1 Introduction

## 1.1 Scope and Objectives

This deliverable provides a review of several relevant industrial standards, regulations and directives relating to AI in manufacturing, including recommendations for human-centric manufacturing systems and safety, security, and data management related technical standards. The objective of this deliverable is to highlight some of the most relevant standards and directives, while surfacing the possible considerations when designing and developing AI applications for the manufacturing industry such as those developed in the STAR project.

The number of available standards, applicable regulations, and other recommendations and reference architectures that can influence the development of AI solutions for the manufacturing sector is considerable, and as technology advances, new ones appear; therefore, in this deliverable, we aspire only to provide some indications on standards and regulations that the project partners have found relevant for the development of AI systems in the manufacturing industry.

The list of standards, architectures, and directives analysed originated from the industrial partners of the project, who, in a series of consultations, informed us about the ones they were using, thinking of using, or the ones they found most interesting. This list was extended with some significant standards which were similar in subject matter to those suggested by the project partners. Although a plethora of standards and regulations have been discussed and summarised, providing a starting point for STAR users and developers, the discussion below is not exhaustive, in the sense that other standards and regulations could be, also, considered, to some extent at least, as relevant for the scope of STAR.

## 1.2 Outline

The deliverable is divided as follows: first, we introduce the topic and present the methodology and the tables used to summarize the information from the standards and directives.

After that, we provide the context and the discussion of several regulations and directives. Then, we present a number of remarkable standards and reference architectures.

Finally, we present our conclusions and the need for further monitoring of the progress of various standards.

## 2 Methodology

### 2.1 Methodology for the regulatory discussion

We thought that the best way to collect and display information on directives and regulations was through a series of factsheets on each of them. This allowed us to keep the document at a considerable readable size while visually displaying the same elements for each of the directives and regulations.

Below is the information we collect in each sheet:

- **Name:** Codename, name and/or alternative name of the regulation or directive
- **Also known as:** What is the short or common name for the regulation?
- **When applicable:** Since when does the regulation apply, or when will it be applicable?
- **Purpose:** What is the purpose of the regulation?
- **Scope:** To which area does the subject matter of the regulation apply?
- **Key implications:** What are generally the key implications of the regulation?
- **Position in data flow:** The position in the data flow indicates – approximately – at which stage of the creation of a product, service, or process, the applicable regulation is more relevant. 'Functionality & interface' are upstream, whereas 'Sustainability & Feasibility' are downstream (figure below).



Figure 1: Position in data flow

- **Stakeholders:** Which parties have rights, obligations, or are otherwise directly involved under this regulation?
- **Relevance to STAR:** Why and to what extent is this regulation relevant to STAR? What are the key implications of this regulation for STAR?
- **Relevance to Manufacturing Industry:** Why and to what extent is this regulation relevant to the manufacturing industry? What are the key implications of this regulation for the manufacturing industry?
- **Link:** Web link to the regulation

Therefore, the sheet or card looks like this.

<b>Name</b>	
<b>Also known as</b>	
<b>When applicable</b>	
<b>Purpose</b>	
<b>Scope</b>	
<b>Key implications</b>	
<b>Position in data flow</b>	
<b>Stakeholders</b>	
<b>Relevance to STAR</b>	
<b>Relevance to Manufacturing Industry</b>	
<b>Link</b>	

## 2.2 Methodology for standards and architectures

Standards and regulations follow a similar approach. There are hundreds on the market and in the literature, and we have looked for a concise method to list and analyse some of the most relevant ones.

Below is the information we collect in each sheet

- **ICS - TC** Does this standard belong to a family? Is it part of a bigger group of architectures? Does it belong to a technical committee?
- **Purpose:** What is the purpose of the standard
- **Scope:** To which area does this standard apply? Which are the main users of this standard?
- **Key implications:** What are generally the key implications of the standard?
- **Relevance to STAR:** Why and to what extent is this standard relevant to STAR? What are the key implications of these standards for STAR? What are the benefits of this architecture for STAR members or STAR Developers? Is relevant for any of the work packages of the project?
- **Relevance to Manufacturing Industry:** Why and to what extent is this standard relevant to the manufacturing industry? What are the key implications of this standard for the manufacturing industry? How is this architecture useful for the manufacturing industry?
- **Link:** Web link to the standard or to the standard family

Thus, the sheet for standards and architectures looks like this.

<b>Name</b>	
<b>ICS - TC</b>	
<b>Purpose</b>	
<b>Scope</b>	

<b>Key implications</b>	
<b>Relevance to STAR</b>	
<b>Relevance to Manufacturing Industry</b>	
<b>Link</b>	

For the architectures, we follow a slightly different approach, and instead of classifying and framing them in templates and cards, we follow a more narrative style. This allows us to detail in each of them aspects that are different and allows us to include some descriptive images.

## 3 EU Regulations

### 3.1 Context

Emerging technologies and ubiquitous flows of digital data have transformed the economy and society considerably over the last couple of years. To streamline this increasing pervasiveness of the digital infrastructure, the European Commission has been publishing numerous regulations and policy documents. This section discusses existing legislation as well as proposed frameworks related to security, data protection, privacy, and safety, in this order.

Cybersecurity has been a critical issue within Europe over the last decades and is still a topic of high importance. In 2004, the European Union Agency for Cybersecurity (ENISA) was founded to become the European network and information security agency.<sup>2</sup> ENISA plays an important role in the assistance of EU institutions, bodies, and agencies as well as of member states for the implementation of cybersecurity policies. Since the introduction of the Cybersecurity Act in 2019, ENISA's capabilities have been strengthened, and the institute has been made ready to play a key role in the establishment of cybersecurity certification frameworks.<sup>3</sup> Another important security related regulation introduced in recent years are the eIDAS<sup>4</sup>, which was the first EU legal framework for cross-border electronic identification and authentication. The NIS Directive, adopted in 2016, was the first EU-wide cybersecurity regulation, in alignment with the EU Cybersecurity Strategy.<sup>5</sup> The NIS Directive will be revised into the proposed NIS II Directive, which enlarges the scope of the NIS.<sup>6</sup> Yet, the related developments are ongoing, in the sense that the Commission has published the Cybersecurity Strategy, that will help Europe to build resilience against cyber threats, and provides some guiding principles to bolster cybersecurity.

Apart from cybersecurity issues, personal data protection (3.2.2) and privacy (3.2.3) are of principal importance to protect fundamental human rights and freedoms when personal data are at stake. To protect the right to privacy, the General Data Protection Regulation (GDPR)<sup>7</sup>, the ePrivacy Directive<sup>8</sup> and forthcoming ePrivacy Regulation<sup>9</sup> were published. These all apply specifically to the processing of *personal* data, which are, any information

<sup>2</sup> Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. Official Journal L 077

<sup>3</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/201

<sup>4</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

<sup>5</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

<sup>6</sup> Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

<sup>7</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

<sup>8</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

<sup>9</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

relating to an identified or identifiable natural person. The ePrivacy Directive has been applicable for almost 20 years by now yet is currently being updated to take the shape of the ePrivacy Regulation, which will broaden the scope to make it adapt to the reality of the modern electronic communications infrastructure. Whereas the GDPR focuses on enhancing control of individuals over their own personal data while being applicable as such across all Member States and across all sectors, the ePrivacy Directive and possibly forthcoming Regulation are sector-specific concerning, namely, the electronic communications sector.

The safety regulations are generally more mature than those associated with data protection, as can be observed from the applicability dates of the Machinery Directive (2006)<sup>10</sup>, the Product Liability Directive (1988)<sup>11</sup> and the Radio Equipment Directive (2014)<sup>12</sup>. The Machinery Directive is currently under revision to make it align with the new legislation on product health and safety, and make it adapt to challenges presented in the modern digital landscape.<sup>13</sup> Despite of its age, the product Liability Directive is still very relevant. Note that this Directive is currently under review; in this respect, it is intended that its scope is extended, so that digital product safety and cybersecurity will be covered under the forthcoming amended version.

Highly relevant for the activities performed in the STAR project is the newly proposed Artificial Intelligence Act.<sup>14</sup> This Artificial Intelligence Act is the product of years of discussions around an EU framework for regulating the use of AI. In 2018, the Commission has launched its first AI Strategy<sup>15</sup>, which established the AI Alliance that was responsible for mapping the implications of AI on society<sup>16</sup>. In the very same year, the High-Level Expert Group (HLEG) on AI was appointed to advise on the AI strategy.<sup>17</sup> The work of the HLEG was incorporated in the publication of the Whitepaper on AI at the beginning of 2020<sup>18</sup>, and eventually contributed to the proposed Regulation on Artificial Intelligence in April 2021, which is currently under review. The implications of this proposal, insofar they are known, are discussed in section 3.2.6.4.

---

<sup>10</sup> Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

<sup>11</sup> Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

<sup>12</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

<sup>13</sup> European Commission (no date). Machinery Directive – revision [online resource]. Available at: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2019-Machinery-Directive-revision\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/2019-Machinery-Directive-revision_en).

<sup>14</sup> Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1>.

<sup>15</sup> Communication from the Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions COM (2018) 237 final, available at: <https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe>.

<sup>16</sup> The European AI Alliance [web page], available at: <https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>.

<sup>17</sup> Shaping Europe's Digital Future: High-level expert group on artificial intelligence [web page], available at: <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>.

<sup>18</sup> White Paper on Artificial intelligence – A European approach to excellence and trust COM (2020) 65 final, available at: [https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).

Finally, in section 3.2.5, the European Accessibility Act is discussed, which may be relevant given STAR’s objective to address ergonomics and accessibility.

## 3.2 Analysis of Regulations relevant for STAR

### 3.2.1 CyberSecurity Regulations

#### 3.2.1.1 Regulation 2019/881/EU

<b>Name</b>	<b>Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/201</b>
<b>Also known as</b>	The Cybersecurity Act
<b>When applicable</b>	27 June 2019
<b>Purpose</b>	To ensure an adequate level of cybersecurity by establishing a cybersecurity certification framework for digital products, services, and processes across the EU. To this end, the Cybersecurity Act lays out objectives, tasks and organisational matters for the European Union Agency for Cybersecurity (ENISA) and establishes governance and rules for certification of ICT products and services.
<b>Scope</b>	Applies EU-wide to ICT products, processes, and services, without prejudice to competencies regarding activities concerning public security, defence, national security, and the activities of the State in areas of criminal law.
<b>Key implications</b>	The Cybersecurity Act introduces certification schemes for digital products, services, and processes. Each European scheme should specify: (a) the categories of products and services covered; (b) the cybersecurity requirements, such as standards or technical specifications; (c) the type of evaluation, such as self-assessment or third party; and (d) the intended level of assurance.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	European Agency for Cybersecurity (ENISA), operator of essential services, digital service provider, national accreditation bodies, conformity assessment bodies.
<b>Relevance to STAR</b>	The extensive data flows throughout the STAR piloting activities could raise cybersecurity concerns, which makes the Cybersecurity Act a useful framework. This framework is particularly relevant when ICT products, processes and services are being used. Certain products, processes and services are central in the STAR pilots, for example for quality inspections, simulations and data sharing. Therefore, The Cybersecurity Act

	is applicable.
<b>Relevance to Manufacturing Industry</b>	The rise of digital technologies in the manufacturing industry introduces new cybersecurity challenges. Therefore, it is necessary to have adequate cybersecurity mechanisms in place. The Cybersecurity Act is relevant to the manufacturing industry insofar ICT products, processes and services are involved, and will introduce certification schemes for cybersecurity. Moreover, ENISA will provide guidance for Industry 4.0 Cybersecurity. <sup>19</sup>
<b>Link</b>	<a href="https://eur-lex.europa.eu/eli/reg/2019/881/oj">https://eur-lex.europa.eu/eli/reg/2019/881/oj</a>

### 3.2.1.2 Regulation 910/2014/EU

<b>Name</b>	<b>Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC</b>
<b>Also known as</b>	eIDAS
<b>When applicable</b>	September 2018
<b>Purpose</b>	To provide an advanced, harmonized legal framework for cross-border electronic identification, authentication, and website certification within the EU, to guarantee information security and to foster innovation.
<b>Scope</b>	Applies to electronic identification schemes notified by the Member States, and trust service providers established in the Union.
<b>Key implications</b>	With the introduction of the eIDAS, qualified electronic signatures gain the same legal status as handwritten signatures; it stipulates that the legal effects and admissibility of digital signatures as evidence in legal proceedings should be recognised in all member states. However, each member state has the freedom to define the legal effects of the standard electronic signature. Furthermore, the eIDAS requires trust service providers to take appropriate technical and organisational measures to manage security risks for trust service providers.
<b>Position in data flow</b>	Midstream.
<b>Stakeholders</b>	Parties that rely upon an electronic identification or a trust service, signatories, public sector bodies, conformity assessment bodies, trust service providers, electronic seal creators.
<b>Relevance to STAR</b>	Moving towards interoperability of electronic identification across the EU countries can help to foster innovation. The

<sup>19</sup> ENISA is setting the ground for Industry 4.0 Cybersecurity (May 20, 2019). Available at: <https://www.enisa.europa.eu/news/enisa-news/enisa-is-setting-the-ground-for-industry-4-0-cybersecurity>.

	eIDAS is relevant to STAR insofar electronic identification schemes are being used or trust service providers are involved. It will guide the validation of such electronic signatures.
<b>Relevance to Manufacturing Industry</b>	Moving towards interoperability of electronic identification across the EU countries can help to foster innovation in the manufacturing industry. The relevance to the manufacturing industry depends on whether electronic identification schemes are being used or whether trust service providers are involved. The key implication is that the electronic identification schemes will be recognised, which can allow organisations to verify identities of stakeholders.
<b>Link</b>	<a href="http://data.europa.eu/eli/reg/2014/910/oj">http://data.europa.eu/eli/reg/2014/910/oj</a>

### 3.2.1.3 Directive (EU) 2016/1148

<b>Name</b>	<b>Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union</b>
<b>Also known as</b>	NIS Directive
<b>When applicable</b>	9 May 2018
<b>Purpose</b>	The NIS Directive was the first regulation to provide legal measures to increase the overall level of cybersecurity in the EU. The NIS directive will be upgraded soon, into the NIS II directive. The NIS II is discussed in the section on proposed regulations.
<b>Scope</b>	The NIS directive applies to operators of essential services and digital service providers. The directive lays down measures aimed at achieving a high level of security of network and information systems.
<b>Key implications</b>	The key implications are the implementation of risk management and reporting obligations for operators of essential services (including energy, transport, banking, financial market, health, drinking water and digital infrastructure) and digital service providers. The Member States must ensure that digital service providers notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	European Agency for Cybersecurity (ENISA), operators of essential services, digital service provider, DNS service provider.
<b>Relevance to STAR</b>	There are currently no indications that the STAR partners are operators of essential services as defined in this directive. However, the partners could possibly be classified as digital

	service providers. This depends on whether partners are internet exchange points (IXPs) <sup>20</sup> , domain name systems (DNSs) <sup>21</sup> and top-level domains (TLDs) <sup>22</sup> , which segments fall under the digital infrastructure to which the NIS applies. If the NIS Directive applies, the key implication is that authorities should be notified of relevant incidents.
<b>Relevance to Manufacturing Industry</b>	See relevance for STAR.
<b>Link</b>	<a href="http://data.europa.eu/eli/dir/2016/1148/oj">http://data.europa.eu/eli/dir/2016/1148/oj</a>

### 3.2.2 Privacy Regulations

#### 3.2.2.1 Regulation (EU) 2016/679

<b>Name</b>	<b>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC</b>
<b>Also known as</b>	General Data Protection Regulation
<b>When applicable</b>	25 May 2018
<b>Purpose</b>	To protect the fundamental rights and freedoms of natural persons – specifically privacy or personal data protection.
<b>Scope</b>	Applies to the processing activities of personal data of citizens in the EU or by processors or controllers located in the EU. Personal data are data of an identified or identifiable natural person. Processing can include the collection, organization, structuring, sharing, or erasure of data.
<b>Key implications</b>	Processing activities of personal data need a lawful basis, such as consent, performance of a contract, legitimate interest, vital interest, legal requirement, or public interest. Furthermore, the GDPR specifies the roles of entities involved in the data processing activities, such as the controller and the processor, and the corresponding responsibilities. The GDPR also provides rights to individuals whose personal data are processed. These rights include the right to transparency, the right of access to their personal data, the right to be forgotten, and the right to object to processing of personal data for certain purposes.

<sup>20</sup> The function of an internet exchange point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. Nor does an IXP provide other services unrelated to interconnection, although this does not preclude an IXP operator from providing unrelated services. An IXP exists to interconnect networks that are technically and organisationally separate. The term 'autonomous system' is used to describe a technically stand-alone network.

<sup>21</sup> 'Domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names; 'DNS service provider' means an entity which provides DNS services on the Internet.

<sup>22</sup> 'Top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD).

	Finally, the GDPR lays down six principles that are guiding in the EU data protection activities, namely (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimisation; (d) accuracy; (e) storage limitation; and (f) integrity and confidentiality.
<b>Position in data flow</b>	Midstream.
<b>Stakeholders</b>	Data subjects, data controllers, data processors, data recipient, third parties under authority of controller or processor, enterprises, supervising authorities, international organisations.
<b>Relevance to STAR</b>	The GDPR is relevant for the protection of privacy of individuals or groups whose data are processed within the STAR pilots. Given that the GDPR applies when personal data are processed, the framework seems to be relevant at least in pilot #1 (workers stress test and insight in worker profile) and pilot #2 (information on work experience and academic qualification). The GDPR shall also be relevant for the collection of personal information of workshop participants. The key implications are the need for consent or other lawful grounds for processing the data.
<b>Relevance to Manufacturing Industry</b>	The transition towards a more digitalised manufacturing industry goes hand in hand with increased capacity for data collection, including, potentially, personal data. The GDPR functions to protect stakeholders whose data are collected and is therefore becoming increasingly relevant for the industry as a whole.
<b>Link</b>	<a href="http://data.europa.eu/eli/reg/2016/679/oj">http://data.europa.eu/eli/reg/2016/679/oj</a>

### 3.2.2.2 Directive 2002/58/EC

<b>Name</b>	<b>Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)</b>
<b>Also known as</b>	ePrivacy Directive
<b>When applicable</b>	12 July 2002
<b>Purpose</b>	To protect the privacy of EU citizens, and the confidentiality of tracking and monitoring practices. To ensure alignment with the GDPR, the ePrivacy Directive is currently being updated into the <i>ePrivacy Regulation</i> .
<b>Scope</b>	Applies to the processing of personal data related to the publicly available electronic communications sector, such as the internet or mobile phone networks, and is thus sector specific.
<b>Key implications</b>	Given that it is a directive, the requirements for protecting privacy have been implemented into national laws or regulations. The eDP Directive will, among other things, address the confidentiality of communication between

	machines (Internet of Things) or individuals on publicly accessible networks. Section # will further elaborate on this.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	Users, subscribers, service providers.
<b>Relevance to STAR</b>	The ePrivacy Directive is helpful for protecting the privacy of data subjects in particular sectors. For STAR, it is relevant to the extent to which mobile phone networks and the internet are part of the pilot. The key implications depend on the national law of the country where the pilot is being executed and/or where the pilot partners are based.
<b>Relevance to Manufacturing Industry</b>	The ePrivacy Directive does not explicitly state its relevance for the manufacturing industry. However, it is relevant to the extent to which mobile phone networks and the internet are involved. The key implications depend on the national law of the country where the manufacturing activities are held and/or where the manufacturer is based.
<b>Link</b>	<a href="http://data.europa.eu/eli/dir/2002/58/oj">http://data.europa.eu/eli/dir/2002/58/oj</a>

### 3.2.3 Safety Regulations

#### 3.2.3.1 Directive 2006/42/EC

<b>Name</b>	<b>Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)</b>
<b>Also known as</b>	Machinery Directive
<b>When applicable</b>	6 June 2006
<b>Purpose</b>	To ensure the safety of operators, maintenance personnel, equipment, and the environment, to promote the free movement of machinery within a single market, and to guarantee a high level of protection of EU workers and citizens.
<b>Scope</b>	Applies to products that can be considered machinery, interchangeable equipment, safety components, lifting accessories, chains, robes and webbing, removable mechanical transmission devices, partly completed machinery. It only applies to products that are to be placed on the EU market for the first time.
<b>Key implications</b>	The Machinery Directive introduces health and safety requirements for machinery. No additional implications are expected with the introduction of AI in manufacturing. The specific requirements are transcribed into national law for each country of the European Union.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	Manufacturer (or its authorized representative)

<b>Relevance to STAR</b>	Introduction of health and safety requirements. The key implications depend on the national law of the country where the pilot is being executed and/or where the pilot partners are based.
<b>Relevance to Manufacturing Industry</b>	The Machinery Directive is relevant as it introduces health and safety requirements to protect the safety of personnel. Moreover, it fosters the free movement of machinery within the EU. The key implications depend on the national law of the country where the manufacturing activities are held and/or where the manufacturer is based.
<b>Link</b>	<a href="http://data.europa.eu/eli/dir/2006/42/oj">http://data.europa.eu/eli/dir/2006/42/oj</a>

### 3.2.3.2 Directive 85/374/EEC

<b>Name</b>	<b>Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products</b>
<b>Also known as</b>	Product Liability Directive
<b>When applicable</b>	30 July 1988
<b>Purpose</b>	To have a common rule on strict liability on the producer for damages due to a defective product; right of consumers to claim damages suffered from a defective product.
<b>Scope</b>	Applies to any product marketed in the EEA. However, the Directive is currently under review; its scope is expected to extend. in order to provide for digital product safety, including for cybersecurity aspects.
<b>Key implications</b>	Producers will be held reliable for damage caused by their products, unless they fall within the exceptions. The implications in a digital world with AI, robots, and IoT are ambiguous.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	Producer or manufacturer
<b>Relevance to STAR</b>	Should the Product Liability Directive provides for digital product safety, it may be applicable with regards to new technologies such as machines communicating with each other in a manufacturing context, given this excerpt from a working document of the European Commission: 'Facing the challenges of digital transformation and in particular to facilitate the investment into and the development of the digital economy, questions arose concerning the clarity of the legal framework, in particular the scope of the Directive to deal with liability issues for IoT devices and complex autonomous systems.' <sup>23</sup> The key implications for STAR are therefore unclear as of now.

<sup>23</sup> Commission Staff Working Document 52018SC0157.

<b>Relevance Manufacturing Industry</b>	<b>to</b>	The concepts of 'product', 'producer', 'defect' and 'damage' may need to be re-evaluated to align with the modern industry, which is increasingly driven by new technologies and connected devices.
<b>Link</b>		<a href="http://data.europa.eu/eli/dir/1985/374/oj">http://data.europa.eu/eli/dir/1985/374/oj</a>

### 3.2.3.3 Directive 2014/53/EU

<b>Name</b>	<b>Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC</b>	
<b>Also known as</b>	Radio Equipment Directive	
<b>When applicable</b>	6 May 2014	
<b>Purpose</b>	To make sure that radio equipment meets applicable standards, including safety, health and electromagnetic compatibility.	
<b>Scope</b>	'applies to electrical or electronic products, which intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination, or electrical or electronic products which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination'. <sup>24</sup>	
<b>Key implications</b>	No additional implications are expected for the use of AI in manufacturing.	
<b>Position in data flow</b>	Upstream.	
<b>Stakeholders</b>	Manufacturer (or its authorized representative), importers, distributors, economic operators, national accreditation body, conformity assessment body.	
<b>Relevance to STAR</b>	The Radio Equipment Directive provides guidance for radio equipment to meet certain standards. It applies insofar electrical or electronic products are used as indicated by the 'Scope'. The key implications depend on the national law of the country where the pilot is being executed and/or where the pilot partners are based.	
<b>Relevance Manufacturing Industry</b>	<b>to</b>	The Radio Equipment Directive provides guidance for radio equipment to meet certain standards. It applies insofar electrical or electronic products are used as indicated by the 'Scope'. The key implications depend on the national law of the country where the manufacturing activities are held and/or where the manufacturer is based.

<sup>24</sup> Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC OJ L 153, available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014L0053>

<b>Link</b>	<a href="http://data.europa.eu/eli/dir/2014/53/oj">http://data.europa.eu/eli/dir/2014/53/oj</a>
-------------	---

### 3.2.4 Other Applicable Regulations and recommendations

#### 3.2.4.1 Directive 2019/882/EU

<b>Name</b>	<b>Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services</b>
<b>Also known as</b>	European Accessibility Act
<b>When applicable</b>	7 May 2019
<b>Purpose</b>	To guarantee accessibility to certain products and services by eliminating and preventing barriers to the free movement of these, particularly with regards to persons with disabilities
<b>Scope</b>	The directive applies to products and services relevant for persons with disabilities (18), including products used for the provision of those services. These can include: computer hardware systems, self-service terminals, consumer terminal equipment with computing capability, e-readers, electronic communication services, audio-visual media services, certain transport services, consumer banking services, e-commerce services.
<b>Key implications</b>	The European Accessibility Act harmonises rules on accessibility in the EU. Furthermore, it will enable people with disabilities and elderly to gain access to products and services, and reduce barriers to access to transport, education, and jobs
<b>Position in data flow</b>	Downstream.
<b>Stakeholders</b>	Persons with disabilities, service providers, manufacturers (or its authorized representative), importers, distributors, economic operators, consumers, enterprises.
<b>Relevance to STAR</b>	It is questionable whether this is relevant. The proposal mentions under 2.2.2.5: '3) Ergonomics and accessibility. STAR considers human factors and designs systems that boost human-machine interactions. STAR's systems will be aligned to standards for ergonomics of human-machine interactions and user interface accessibility, notably to standards produced by ISO and W3C.' Given that it is a directive, the key implications depend on the national law of the country where the pilot is being executed and/or where the pilot partners are based.
<b>Relevance to Manufacturing Industry</b>	The key implications depend on the national law of the country where the manufacturing activities are held and/or where the manufacturer is based.
<b>Link</b>	<a href="http://data.europa.eu/eli/dir/2019/882/oj">http://data.europa.eu/eli/dir/2019/882/oj</a>

### 3.2.5 Proposed Regulations

#### 3.2.5.1 EC Proposal for a Regulation on European data governance (Data Governance Act)

<b>Name</b>	<b>Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance</b>
<b>Also known as</b>	Data Governance Act
<b>When applicable</b>	25 November 2021
<b>Purpose</b>	To increase trust in data intermediaries and to strengthen data-sharing mechanisms across the EU. The DGA responds to the issue of the lack of availability of data for research and innovation.
<b>Scope</b>	Data sharing and intermediaries.
<b>Key implications</b>	Introduction of mechanisms for the re-use of data produced by the public sector, creation of data intermediaries, and the establishment of the European Data Innovation Board.
<b>Position in data flow</b>	Downstream.
<b>Stakeholders</b>	Data holders, data users, public sector bodies, bodies governed by public law.
<b>Relevance to STAR</b>	Given that the use and exchange of digital data are central in STAR, the Data Governance Act is relevant insofar it encourages data sharing and introduces requirements for trusted data intermediaries. A potential risk associated with the transnational nature of STAR is that this could be a barrier for sharing data through the assessment provision of data protection regimes of third countries, that can block the transfer of highly sensitive data.
<b>Relevance to Manufacturing Industry</b>	For the transition of the manufacturing landscape towards more cyber and digital infrastructure, including emerging technologies such as IoT and AI, the exchange of data is expected to grow massively. Principles such as trust and interoperability are essential for responsible data sharing, emphasizing the importance of the Data Governance Act for the manufacturing industry. One of the benefits for the industry is the creation of sector-specific data spaces to enable the sharing of data within a specific sector, which the Act is intending to do. The implication is that data sharing activities will be further regulated.
<b>Link</b>	<a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767</a>

#### 3.2.5.2 COM/2017/010

<b>Name</b>	<b>Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the</b>
-------------	---

	<b>respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC</b>
<b>Also known as</b>	ePrivacy Regulation
<b>When applicable</b>	Draft was finalised on 10 February 2021 by the EU Council
<b>Purpose</b>	To update the 2002 ePrivacy directive such that it aligns with the GDPR.
<b>Scope</b>	The ePrivacy Regulation widens the scope of the directive.
<b>Key implications</b>	As the ePrivacy Directive becomes the ePrivacy Regulation, it will become self-executing and legally binding in EU countries. The privacy rules apply to communication services, such as WhatsApp and Skype, and to new forms of electronic communications such as IoT. Compared to the Directive, the rules are tightened. Key implications are to the regulation of metadata and streamlining cookies provision. Consent is will no longer be required for non-privacy intrusive cookies.
<b>Position in data flow</b>	Midstream.
<b>Stakeholders</b>	Interpersonal and electronic communication services, end-users
<b>Relevance to STAR</b>	The ePrivacy Regulation is helpful for protecting the privacy of the people whose data are being processed. It is particularly relevant where personal data are processed through electronic communication. Moreover, the ePrivacy Regulations mentioned that the principle of confidentiality also applies to machine-to-machine communications. This could be relevant when wearables are used (pilot #1) for stress-monitoring, but also to possible further exchange of personal data among machines.
<b>Relevance to Manufacturing Industry</b>	For the manufacturing industry, the ePrivacy Regulation is relevant for protecting the privacy of data subjects. With the introduction of modern communication services in the sector, such as WhatsApp and Skype, but also IoT, the sector may have to comply with the rules of the ePrivacy Directive. Not only will it lead to restrictions, but it will also simplify processes such as cookie provision and the collection of meta-data.
<b>Link</b>	<a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010</a>

### 3.2.5.3 Updated NIS Directive (NIS II)

<b>Name</b>	<b>Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148</b>
<b>Also known as</b>	NIS II
<b>When applicable</b>	20 days after publication in the Official Journal of the European Union.

<b>Purpose</b>	to address the limitations of the old NIS Directive that arise as digital information systems are becoming increasingly ubiquitous. The main issues, according to the European Commission, are (1) insufficient level of cyber resilience of businesses operating in the EU; (2) inconsistent resilience across the Member States and sectors; and (3) insufficient common understanding of the main threats and challenges among the Member States and lack of joint crisis response.
<b>Scope</b>	NIS II enlarges the scope of NIS I, to include providers of public electronic communications networks, wastewater and waste management, manufacturing of certain critical products, food, digital services such as social network and data centre services, space, postal services, public administration
<b>Key implications</b>	With the NIS II Directive, the Commission aims to adapt the previous NIS Directive in line with the changing technical and threat landscape and to make it more future proof. To this end, the NIS II Directive has expanded its scope and included more sectors and services that are either essential or important entities including public administration, providers of public electronic communications networks or services, digital services such as social media platforms, space and wastewater and waste management. Earlier distinction between operators of essential services and digital service providers has also been eliminated. Security requirements have also been further strengthened under the new Directive with a list of focused measures such as incident response and crisis management, cybersecurity testing, use of encryption and vulnerability handling and disclosure.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	DNS service providers, TLD name registry, cloud computing service provider, data centre service provider, IXPs, DNSs, TLDs, social networking services platform, public administration entities.
<b>Relevance to STAR</b>	To the extent to which involved parties engage with digital services and manufacturing of critical products. Unclear whether this is the case
<b>Relevance to Manufacturing Industry</b>	The key implications depend on the national law of the country where the manufacturing activities are held and/or where the manufacturer is based.
<b>Link</b>	<a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN</a>

### 3.2.5.4 COM (2021) 206 proposal for Artificial Intelligence Act

<b>Name</b>	<b>COM (2021) 206: Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence ('Artificial</b>
-------------	---

	<b>Intelligence Act') and Amending Certain Union Legislative Acts.</b>
<b>Also known as</b>	Artificial Intelligence Act
<b>When applicable</b>	20 days after publication in the Official Journal of the European Union.
<b>Purpose</b>	To encourage the development, deployment and use of secure, trustworthy and human-centric artificial intelligence.
<b>Scope</b>	Applies to placing on the market and putting into service of AI systems
<b>Key implications</b>	AI systems are divided into four risks levels. Depending on the risk level, they are subject to transparency requirements, data quality, documentation and cybersecurity requirements, or fully prohibited.
<b>Position in data flow</b>	Upstream.
<b>Stakeholders</b>	Providers, users, authorized representatives, importers, distributors, operators market surveillance authorities, national supervisory authority, national competent authority.
<b>Relevance to STAR</b>	The STAR infrastructure most likely qualifies as limited risk AI. Therefore, individuals, including, for example, workers, should be informed that they interact with an AI system. Currently, there is no indication that STAR pilots involve high-risk or prohibited uses of AI within the context of this framework.
<b>Relevance to Manufacturing Industry</b>	If the STAR activities will be applied to management and operation of critical infrastructure, that is, road traffic and supply of water, gas, heating and electricity, these will be subject to the obligations for high-risk AI systems.
<b>Link</b>	<a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1</a>

### 3.3 Guidelines and Recommendations

As it can be derived from the analysis of regulations in section 3.2, the regulatory framework should not be seen necessarily as a barrier, as it introduces mechanisms that can streamline data collection processes, encourage data sharing and enable the use of digital identities across the EU. In this spirit, the following recommendations could further contribute to enabling STAR to effectively comply with the relevant regulations:

- Build-in strong security mechanisms *by design*, which implies that appropriate mechanisms are incorporated in the early stages of the project.
- Carefully map the data flows, including the sources of data collection, the data transfers, as well as all stakeholders that have insight into the data or are otherwise involved in the data processing activities. This is particularly important where connected devices exchanging data are used.
- Anonymise or pseudonymise all personal data used to the extent possible. Where and when personal data processing is absolutely necessary, STAR needs a lawful basis allowing for such processing.

- Focus on the data minimisation principle, limiting the collection of data to what is directly relevant and necessary to accomplish a specific purpose.

Furthermore, it is recommended to monitor the regulatory developments in relation to the proposed EU regulations, in order to make the STAR project future proof. This implies, among others, that:

- The risk level of all AI technologies used for the purposes in STAR should be assessed in the light of the proposed Artificial Intelligence Act, and appropriate measures should be taken to build trust in these technologies in accordance with the Act.

## 4 Standards and Architectures

### 4.1 Context

There have been several efforts in the literature to conduct an analysis of standards for the manufacturing sector. In general, due to the wide scope and the extensive collection of standards available, these analyses, like ours, focus on a specific part of the spectrum. Some of the most relevant analyses are detailed below.

Choi et al (Choi, 2016), presented an analysis based on Factory Design and Improvement (FDI) process and the ISA-88 hierarchical model of manufacturing operations. In their document they focus on PPR (Product, Process, Resource) standards, categorising standards related to Product data (e.g.: DXF, IGES, VRML), Process data (e.g.: OAGIS, ANSI/ISA-95) and Resource data (e.g.: B2MML, AP242) and their coverage on the FDI functional matrix.

Li et al. (Li, 2018) reviewed several smart manufacturing standards and analysed several industrial architectures. In particular, they focused on the standards developed by the following standard development organizations (SDOs):

- ISO/TC184 automation systems and integration, which develops standards related to information systems, control devices, or data integration and interoperability.
- IEC/TC65 industrial-process measurement, control and automation, focused on activities that impact the integration of components, as well as different aspects of such systems, such as safety and security.
- ISO/IEC/JTC1 information technology, focused on ICT standards in different scopes, including security, multimedia, or smart cards among others.

The National Institute of Standards and Technology (NIST) published in 2016 a landscape of standards focused especially on Smart Manufacturing Systems, which among other things details standards related to the different phases of product development, from design to end-of-life and recycling. This landscape covers modelling, data exchange, production system engineering and operation and maintenance standards, and identifies 8 priority areas in which standardization should advance: i) Smart Manufacturing System reference model and reference architecture; ii) Internet of Things reference architecture for manufacturing; iii) Manufacturing service models; iv) Machine to machine communication; v) PLM/MES/ERP/SCM/CRM integration; vi) Cloud manufacturing; vii) Manufacturing sustainability; and viii) Manufacturing cybersecurity.

W. Ziegler in (Ziegler, 2020) analyses the standardisation landscape in the AI field, by focusing on the standards developed by five international and European SDOs (IEEE, ISO/IEC, ITU-T, ETSI, CEN-CENELEC) and two standards-setting organizations (SSO): W3C and IRTF.

One of his main points is that even if the SDOs and SSOs are doing actions in the AI field, the standardisation activities are limited, and their number is low and does not increase at the same rate as developments and applications.

A new European player in standardisation activities and pursuing to increase the list of available standards on AI is the OASIS Open Europe Foundation (OOEF). OOEF is the European sovereign affiliate organisation to the international non-profit, OASIS Open, which works to advance and support Europe's role in open source and open standards development. OOEF activities include: participation in collaborative projects supported by

the EU and EU Member States, organisation and participation in events for promoting the adoption of open-source projects, engagement in European-specific activities to progress open source and open standards. The list of standards relevant for the Manufacturing domain and the AI technology covers Communication/messaging protocols (AMQP, MQTT), Cloud service management (TOSCA), privacy management (PMRM), security, and production planning (PPS), among other topics.

## 4.2 Analysis of Standards

### 4.2.1 Technical. Management and Security Standards

#### 4.2.1.1 ISO/IEC 27001

<b>Name</b>	<b>ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements</b>
<b>ICS - TC</b>	35.030 IT Security, 03.100.70 Management systems - ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
<b>Purpose</b>	Specify the requirements for implementing an information security management system (ISMS)
<b>Scope</b>	It is applicable to organisations (public or private) of any type and size, willing to implement an ISMS within the organization.
<b>Key implications</b>	Enablement of the assessment and treatment of security risks. Implementation and management of security controls
<b>Relevance to Manufacturing Industry</b>	This standard covers 3 main points, impacting the IT systems in the manufacturing industry: i) the understanding and monitoring of security risks (including the knowledge of potential vulnerabilities, threats and the impact of them). ii) design and implementation of security controls to reduce the risks; and iii) the implementation of the process for the continuous management of the information security requirements. An organisation can become ISO 27001 certified.
<b>Relevance to STAR</b>	Knowing and understanding the security risks and establishing mechanisms to manage them efficiently is important for pilots and potential users of the platform. Even if the end-users are not considering the need for certification, it is of interest for them to take this standard into account when designing their security management system. An end-user may value positively or require certification of a provider, so in some cases and contexts certification may be necessary. This standard may be of interest for activities such as those carried out in WP3.
<b>Link</b>	<a href="https://www.iso.org/standard/54534.html">https://www.iso.org/standard/54534.html</a> ISO/IEC 27001 family: <a href="https://www.iso.org/isoiec-27001-information-security.html">https://www.iso.org/isoiec-27001-information-security.html</a>

#### 4.2.1.2 ISO/IEC 27002

<b>Name</b>	<b>ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls</b>
<b>ICS - TC</b>	35.030 IT Security   ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
<b>Purpose</b>	Specify and provide guidelines for the implementation and management of security controls.
<b>Scope</b>	It is applicable to organisations (public or private) of any type and size.
<b>Key implications</b>	Intended to allow organisation to select controls for implementing ISO/IEC 27001 based ISMSs
<b>Relevance to Manufacturing Industry</b>	Facilitates the selection of controls for the implementation of an ISMS. Guides in the implementation of common and well-known security controls. Assists in the creation of guidelines for the management of the organization's ISMS.
<b>Relevance to STAR</b>	This standard provides security controls and guidance on how to implement them. It covers issues related to data access, cryptography, asset management and information exchange, all of which are of importance when designing the project platform and of interest to potential users of the platform. This standard may be of interest for activities such as those carried out in WP3.
<b>Link</b>	<a href="https://www.iso.org/standard/54533.html">https://www.iso.org/standard/54533.html</a>

#### 4.2.1.3 ISO/IEC 27701:2019

<b>Name</b>	<b>Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines</b>
<b>ICS - TC</b>	35.030 IT Security - ISO/IEC JTC 1/SC 27 Information security, cybersecurity, and privacy protection
<b>Purpose</b>	Specify the requirements and guidelines for implementing Privacy Information Management System (PIMS).
<b>Scope</b>	It is applicable to organisations (public or private) of any type and size, willing to implement privacy management within the organization.
<b>Key implications</b>	Enhance Information Security Management System (ISMS) with additional privacy information management requirements.
<b>Relevance to Manufacturing Industry</b>	The guidelines and recommendations in this standard allow Personally Identifiable Information Controllers and Personally Identifiable Information Processors to manage privacy controls and allows the organisations to implement efficient Privacy Information management Systems, including policies and procedures for personal information management, including these needed to align the policies to privacy and Data protection regulations. ISO 27701 relies on ISO 27001, so both could be executed

	together as a single project
<b>Relevance to STAR</b>	In some cases, project pilots or middleware users need to manage personal information (e.g., activity data). In those cases, it is important to understand the risks and establish policies and procedures to reduce the main risks related to that private information. This standard may be of interest for activities such as those carried out in WP2 and WP3.
<b>Link</b>	<a href="https://www.iso.org/standard/71670.html">https://www.iso.org/standard/71670.html</a>

#### 4.2.1.4 IEC 62714

<b>Name</b>	<b>Engineering data exchange format for use in industrial automation systems engineering - Automation Markup Language (AutomationML)</b>
<b>ICS - TC</b>	25.040.40 - Industrial process measurement and control 35.060 - Languages used in information technology 35.240.50 - IT applications in industry TC 65/SC 65E
<b>Purpose</b>	Specify a data exchange format tailored to the needs of production system engineering
<b>Scope</b>	Neutral, open, vendor independent, and freely available standard
<b>Key implications</b>	Enable lossless bilateral (engineering) data exchange along the entire life cycle of production systems.
<b>Relevance to Manufacturing Industry</b>	IEC 62714 family defines an XML (AutomationML) schema-based data format for the data exchange among heterogeneous engineering tools. AutomationML combines and adapts industry standards to reduce data interchange and integration issues. The standards currently integrated in AutomationML are: <ul style="list-style-type: none"> <li>• CAEX for object topologies, hierarchies, properties</li> <li>• COLLADA for geometries and kinematics</li> <li>• PLCopen XML for discrete behaviour of objects</li> </ul>
<b>Relevance to STAR</b>	Both HMI development and the use of robots in the industrial environment are of interest to the project. Middleware users may need support for the exchange of engineering data, for example, to describe devices or to facilitate integration with available tools. While the project's middleware does not have to implement its support, it is of interest to know the implications of the standard since data in that standard could flow through the middleware's communication mechanisms. This standard may be of interest for activities such as those carried out in WP2 and WP5.
<b>Link</b>	<a href="https://www.automationml.org/">https://www.automationml.org/</a>

#### 4.2.1.5 W3C XML security Standards

<b>Name</b>	<b>W3C XML security Standards - Family</b>
<b>ICS - TC</b>	Various ICS - W3C working groups

<b>Purpose</b>	Specify some security extension for the usage and interchange of XML data
<b>Scope</b>	Neutral, open, vendor independent, and freely available standard
<b>Key implications</b>	XML is one of the most used document encoding and data exchange format. Some security mechanisms are defined to create a more secure environment for XML
<b>Relevance to Manufacturing Industry</b>	XML (Extensible Markup Language) is a machine- and human-readable document encoding format, originally developed for the Web, but used for data exchange and processing in various industrial applications. XML has several extensions that allow you to create more secure environments when it comes to the manipulation and use of XML data. Among them, we can name: XML signature: integrity, signer and message authentication XML encryption: specifies the process for encrypting data and representing the resulting data in XML format XKMS: defines protocols for registering and distributing public keys, for use, for example, with XML signature and encryption.
<b>Relevance to STAR</b>	Some of the components using the STAR platform may use XML as a data exchange format. Although, as in the case of other formats, a specific support implementation should not be necessary, since it is ideal to be agnostic to the format of the data exchanged, it is interesting to take into account and be aware of the possibilities of the standard. For example, by pilots, if they are considering the use of this format and security extensions. This standard may be of interest for activities such as those carried out in WP2 and WP5.
<b>Link</b>	<a href="https://www.w3.org/standards/xml/">https://www.w3.org/standards/xml/</a>

#### 4.2.1.6 ETSI Cybersecurity and AI Standards

<b>Name</b>	<b>ETSI TC CYBER &amp; SAI Standards</b>
<b>ICS - TC</b>	Various - TC CYBER & TC SAI
<b>Purpose</b>	Offer market-driven cyber security standardization solutions, recommendations and guidelines, and the improvement of the security of AI
<b>Scope</b>	End-users, providers, manufacturers, operators and regulators. Applicable to different domains.
<b>Key implications</b>	Understand and reduce cross-domain cybersecurity implications. Ensure that artificial intelligence is secure
<b>Relevance to Manufacturing Industry</b>	Network security, security of sensors and IoT devices, cybersecurity tools, or machine-to-machine security are some of the topics covered by the ETSI CYBER standards.  SAI is focusing on 3 main topics. All of them impacting the manufacturing domain <ul style="list-style-type: none"> <li>● Securing and protecting AI components from attacks:</li> <li>● Mitigation against malicious and dangerous AI</li> </ul>

	<ul style="list-style-type: none"> <li>Using AI to improve security measures</li> </ul> <p>Notable standards are:</p> <ul style="list-style-type: none"> <li>ETSI GR SAI 004: Securing Artificial Intelligence (SAI); Problem Statement</li> <li>ETSI GR SAI 005: Securing Artificial Intelligence (SAI); Mitigation Strategy Report</li> <li>ETSI TR 103 787-1 CYBER; Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials</li> </ul>
<b>Relevance to STAR</b>	<p>CYBER &amp; SAI are two of the committees of ETSI developing standards related to safe and secure AI systems. Their focus on being cross-sectorial, and taking into account user and SME awareness, make several of these standards of interest to SMEs planning to implement safe and secure systems. The design challenges sections of the ETSI GR SAI 004 and especially its section related to attacks, which details poisoning attacks, input and evasion attacks, backdoor attacks and reverse engineering attacks, are of absolute interest to the STAR project. This standard may be of interest for activities such as those carried out in WP3.</p>
<b>Link</b>	<p><a href="https://www.etsi.org/committee/cyber">https://www.etsi.org/committee/cyber</a> <a href="https://www.etsi.org/committee/sai">https://www.etsi.org/committee/sai</a></p>

#### 4.2.1.7 ISO/IEC 18033

<b>Name</b>	<b>ISO/IEC 18033 Information technology — Security techniques — Encryption algorithms</b>
<b>ICS - TC</b>	35.030 IT Security - ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
<b>Purpose</b>	Provide definitions, recommendations and guidelines for data encryption and confidentiality.
<b>Scope</b>	End-users, providers, manufacturers, operators and regulators. Applicable to different domains.
<b>Key implications</b>	Recommend encryption algorithms. Specify encryption algorithms for use in different scenarios.
<b>Relevance to Manufacturing Industry</b>	<p>This family of standard includes, so far, 5 different types of cyphers and encryption methods: i) asymmetric ciphers; ii) block ciphers; iii) stream ciphers; iv) Identity-based ciphers; v) Homomorphic encryption. All of them have a direct impact on the communications and the data used in the manufacturing industry.</p> <p>Asymmetric ciphers (public-key cryptography) are based on the use of a pair of keys: public and private, to provide confidentiality (transmit encrypted messages), integrity (prevent changes to information), authenticity (e.g., Digital Signatures) and non-repudiation.</p> <p>Block ciphers are symmetric encryption methods (using one</p>

	<p>secret key) to enforce the confidentiality of data being transmitted or stored.</p> <p>Stream ciphers are another symmetric encryption method, where the key is combined with a pseudorandom stream of digits, so the encryption can be applied to individual bits of a stream.</p> <p>Identity-based ciphers are encryption mechanisms where the public key can be generated from a known unique identifier (e.g., a mail address, an IP address...)</p> <p>Homomorphic encryption enables computations to be performed on encrypted data.</p> <p>Both block ciphers and stream ciphers are in everyday use for transmitting information in industry and other sectors. Public key mechanisms are also being used for integrity and authenticity (e.g., certificates). Identity-based and Homomorphic systems are less widely used currently but are of interest for simplifying asymmetric encryption or for performing operations on encrypted stored data.</p>
<b>Relevance to STAR</b>	<p>Several STAR pilots and users will need to store unique or private information, and others will need to transmit and share this information between platform modules. For this reason, and to provide a secure communication and data storage ecosystem for industry, the platform needs to support at least symmetric and asymmetric encryption. This standard may be of interest for activities such as those carried out in WP3.</p>
<b>Link</b>	<p><a href="https://www.iso.org/standard/54530.html">https://www.iso.org/standard/54530.html</a></p>

#### 4.2.1.8 ISO/IEC 29100

<b>Name</b>	<b>Information technology — Security techniques — Privacy framework</b>
<b>ICS - TC</b>	35.030 IT Security - ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
<b>Purpose</b>	Define a framework around privacy and the processing of personally identifiable information (PII)
<b>Scope</b>	Applicable to natural persons and organisations. Applicable to different domains.
<b>Key implications</b>	Specify common privacy terminology; define the stakeholders and their roles in the processing of PPI; Provide privacy principles and considerations
<b>Relevance to Manufacturing Industry</b>	This standard establishes a framework for the protection of PII (biometric identifiers, names and surnames, location information, ...) and establishes recommendations on how PII should be identified, how data should be controlled and how this data should be transmitted. This framework is applicable to various industries, including the manufacturing sector, and allows the organization to control security risks, comply with legal requirements, and reduce potential privacy breaches, which in turn can impact the organization's image.

<b>Relevance to STAR</b>	In the case of pilots, and in the case of potential users of the platform, it will be necessary to deal with PPI, for example, some biometric information or simply data from shopfloor operators. Knowing and establishing privacy controls is important for pilots related to AI systems, and facilitating privacy is important for both the STAR platform and the technology providers that will run on top of the STAR ecosystem. This standard may be of interest for activities such as those carried out in WP3.
<b>Link</b>	<a href="https://www.iso.org/standard/45123.html">https://www.iso.org/standard/45123.html</a>

#### 4.2.1.9 ISO/IEC 27040

<b>Name</b>	<b>Information technology — Security techniques — Storage security</b>
<b>ICS - TC</b>	35.030 IT Security - ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
<b>Purpose</b>	Define recommendations for planning, designing and implementing data storage security
<b>Scope</b>	Addressed to technology providers, manufacturers, operators and even users and managers. Applicable to different domains.
<b>Key implications</b>	Define storage security terminology. Provide guidance on the security aspects associated with storage and storage technologies. Define some scenarios related to the secure storage of data
<b>Relevance to Manufacturing Industry</b>	Data warehousing is a key issue in manufacturing information systems, and especially in the use of AI in the manufacturing industry. AI models require information to be trained and information to be used. This information is stored for decision making or for visualization. How, where and with what protection to store this data requires knowing the risks and implementing a secure storage approach.
<b>Relevance to STAR</b>	As mentioned above, some of the pilots will collect information from the operators, this information is considered PII. In addition, for statistical use, data will be collected on visits and usage of some of the modules and platforms. In both cases, it is important to design an adequate storage security strategy. Regarding the data to be stored, there will be information in text mode and binary formats (e.g., images) that will have to be stored on a disk. There will also be data that will be stored in different databases, especially relational and Time Series Databases. The data used to train the AI modules are mostly generated by devices or humans in the shopfloor. This information has to be stored securely, to prevent unwanted dissemination of information. This standard may be of interest for activities such as those carried out in WP3, WP4, WP5 and WP6.

<b>Link</b>	<a href="https://www.iso.org/standard/44404.html">https://www.iso.org/standard/44404.html</a>
-------------	---

#### 4.2.1.10 ISO/TS 15066

<b>Name</b>	<b>ISO/TS 15066 Robots and robotic devices — Collaborative robots</b>
<b>ICS - TC</b>	25.040.30 Industrial robots. Manipulators ISO/TC 299 Robotics
<b>Purpose</b>	Define safety requirements for collaborative industrial robots
<b>Scope</b>	Addressed to industrial robot manufacturers, operators, technology providers
<b>Key implications</b>	Technical specification complementing ISO10218 - Safety Requirements for Industrial Robots, with focus on collaborative robots. Guide the risk assessment related to collaborative robot systems and applications.
<b>Relevance to Manufacturing Industry</b>	<p>Some of the tasks performed in the shopfloor require collaboration between humans and robots, and in some cases, both occupy the same space.</p> <p>Specifically, this TS describes 4 collective operation techniques:</p> <ul style="list-style-type: none"> <li>• Safety-rated monitored stop</li> <li>• Hand guiding</li> <li>• Speed and separation monitoring</li> <li>• Power and force limiting</li> </ul> <p>Understanding this collaboration and knowing the risks is essential to avoid incidents resulting from robot-human contact. Maximum speed control, emergency stops, immediate contact stops, and other technologies are some of the technologies applicable to industrial robots and especially to cobots.</p>
<b>Relevance to STAR</b>	This technical specification and the standard ISO 10218 “Robots and robotic devices - Safety requirements for industrial robots”, are of special interest due to one of the use cases related to humans and robots occupying the same space. The pilot aims to detect potential hazards thanks to computer vision. Knowledge and risk reduction is key to the use of AI systems in industry. This standard may be of interest for activities such as those carried out in WP6.
<b>Link</b>	<a href="https://www.iso.org/standard/62996.html">https://www.iso.org/standard/62996.html</a>

### 4.2.2 Safety and Health Standards

#### 4.2.2.1 ISO 10075

<b>Name</b>	<b>Ergonomic principles related to mental workload</b>
<b>ICS - TC</b>	13.180 Ergonomics 01.040.13 Environment. Health protection. Safety (Vocabularies)

	ISO/TC 159/SC 1 General ergonomics principles
<b>Purpose</b>	Define concepts related to mental workload and how to measure it; Provide design principles.
<b>Scope</b>	Addressed to ergonomic experts, designers, operators, users. Applicable to different domains.
<b>Key implications</b>	Define terms related to mental workload, stress and strain, their consequences and the relationship between them. Define methods to measure and assess the mental workload and provide requirements for measurement instruments. Provide guidance about the design of the workplace, equipment and activities.
<b>Relevance to Manufacturing Industry</b>	Van Acker (Van Acker, 2020) in his dissertation on mental workload monitoring in the manufacturing industry, details several studies that show the relationship between fatigue and frustration and safety risks, loss of quality or performance, as well as detailing how changes in health (physical and mental) effects on workers lead to changes in burnout and job satisfaction. Ergonomics, the correct design of tasks and workplaces has a direct impact on the safety and security of workers. The incorporation of standards related to ergonomics and improving the quality of the worker's environment also impacts on the safety of innovative manufacturing environments.
<b>Relevance to STAR</b>	In STAR there are pilots related to the collaboration of humans with the machines and robots in the surroundings, pilots with short cycle time inspections, or areas of the workplace where operators should not be so as not to impact the processes or suffer mishaps. The knowledge of the mental workload and its impact on the worker is relevant when designing the spaces for carrying out proof of concept trials and even defining the tasks that operators have to perform.
<b>Link</b>	<a href="https://www.iso.org/standard/66900.html">https://www.iso.org/standard/66900.html</a>

#### 4.2.2.2 ISO 16982

<b>Name</b>	<b>Ergonomics of human-system interaction</b>
<b>ICS - TC</b>	13.180 Ergonomics ISO/TC 159/SC 4 Ergonomics of human-system interaction
<b>Purpose</b>	Explain the concept of usability and how to apply it for design and evaluation
<b>Scope</b>	Addressed to ergonomics experts, designers, developers, validation and quality assurance, projects managers, purchasers of equipment
<b>Key implications</b>	Define key terms and concepts around usability, detailing the fundamentals behind the usability concept and explaining its usability and applicability.
<b>Relevance to Manufacturing</b>	While the standard does not specify how to implement usability methods, it does detail usability practices in different contexts.

<b>Industry</b>	The information detailed in the standard includes different cases that occur in the industry, from the design of new products to the purchase of equipment for everyday use. All of these uses have implications for usability and ergonomics, and therefore understanding usability values through this standard along with the support of a human factors expert can be important for evaluating and implementing systems with a focus on user performance and comfort.
<b>Relevance to STAR</b>	Human-machine collaboration, from the point of user satisfaction and comfort, and with performance improvement objectives are interesting for AI-related use cases in the shopfloor. Any improvements that these AI algorithms, or the STAR platform can offer in terms of usability, will be beneficial to the platform's users. This standard may be of interest for activities such as those carried out in WP4.
<b>Link</b>	<a href="https://www.iso.org/standard/31176.html">https://www.iso.org/standard/31176.html</a>

#### 4.2.2.3 ISO 9241

<b>Name</b>	<b>Ergonomics of Human System Interaction</b>
<b>ICS - TC</b>	13.180 Ergonomics ISO/TC 159/SC 4 Ergonomics of human-system interaction
<b>Purpose</b>	Cover different aspects of Ergonomics related to human machine interaction
<b>Scope</b>	Addresses ergonomics experts, designers, developers, validation and quality assurance, projects managers, purchasers of equipment
<b>Key implications</b>	Multi-part standard covering different aspects related to ergonomics. These aspects range from software, terminals and displays, to input devices and ergonomics in the workplace.
<b>Relevance to Manufacturing Industry</b>	If the 16982 is an interesting standard for the industry, this one can be considered a compendium of ergonomics guidelines, not only focused on usability. Design decisions are often made based on developers' personal preferences or perceptions of what might be in the user's best interest. Having a collection of recommendations from experts in the field allows the industry to have a frame of reference and a set of documents to rely on in order to develop ergonomic interfaces and improve the usability and performance of human-machine interaction.
<b>Relevance to STAR</b>	Several of the pilots mention human-machine interaction, and in several cases, the usability of the solutions is interesting to pursue. This standard is extensive and covers usability and ergonomics at various levels. It is not expected that pilots will comply with all recommendations, but it could be worthwhile to use some of the software related standards as best practices. This standard may be of interest for activities such as those carried out in WP4.
<b>Link</b>	<a href="https://en.wikipedia.org/wiki/ISO_9241">https://en.wikipedia.org/wiki/ISO_9241</a>

	<a href="https://www.iso.org/standard/21922.html">https://www.iso.org/standard/21922.html</a>
--	---

#### 4.2.2.4 ISO 6385

Name	Ergonomics principles in the design of work systems
<b>ICS - TC</b>	13.180 Ergonomics ISO/TC 159/SC 1 General ergonomics principles
<b>Purpose</b>	Define fundamental principles of Ergonomics. Establish guidelines for designing of work systems
<b>Scope</b>	Addressed to ergonomics experts, work systems manufacturers, designers, managers, workers
<b>Key implications</b>	Definition of work system to indicate a variety of working places and conditions. Summarize considerations related to the worker interaction with the work system, including the tasks, workplace, team, tools, etc.
<b>Relevance to Manufacturing Industry</b>	The standard is interesting from the point of view of taking into account different aspects of the work environment that affect ergonomics. Many of these are not only technical, but include aspects such also as worker breaks or multitasking. The standard also recommends including workers in ergonomic decisions. The ergonomic needs of people with special needs are also taken into account in the standard.
<b>Relevance to STAR</b>	As with the other standards, and especially those related to ergonomics, it is not intended to be 100% followed in STAR, but it is true that considering the ergonomics principles of this standard together with the others related to ergonomics and design can improve the usability of the project's systems.
<b>Link</b>	<a href="https://www.iso.org/standard/63785.html">https://www.iso.org/standard/63785.html</a>

#### 4.2.2.5 ISO 26800

Name	Ergonomics — General approach, principles and concepts
<b>ICS - TC</b>	13.180 Ergonomics 01.040.13 Environment. Health protection. Safety ISO/TC 159/SC 1 General ergonomics principles
<b>Purpose</b>	Specify basic ergonomics principles and concepts
<b>Scope</b>	Addressed to ergonomics experts, work systems manufacturers, designers, managers, workers
<b>Key implications</b>	improve the safety, performance, reliability, availability, and maintainability of the design result throughout its life cycle, preserving and promoting health and satisfaction of the involved people.
<b>Relevance to Manufacturing Industry</b>	This standard is a short standard, establishing the basis and concepts of ergonomics. For industry, it can be a good starting point especially if one wants to go deeper into ergonomics related topics. This standard takes into account the views of different people involved in the work and is therefore useful to take into account different perspectives.

<b>Relevance to STAR</b>	At the project level, this standard can be interesting for getting understanding or for reaching an agreement on the terminology related to usability and ergonomics.
<b>Link</b>	<a href="https://www.iso.org/standard/42885.html">https://www.iso.org/standard/42885.html</a>

#### 4.2.2.6 ISO 45001

<b>Name</b>	<b>Occupational health and safety management systems</b>
<b>ICS - TC</b>	ISO/TC 283 Occupational health and safety management 13.100 Occupational safety. Industrial hygiene 03.100.70 Management systems
<b>Purpose</b>	Protect workers and visitors from work-related accidents and work-related illnesses.
<b>Scope</b>	Addressed to organisations of any size. Oriented to Safety managers, managers, workers, business owners
<b>Key implications</b>	Specify the requirements for a Safety and Health management system. Guide organisation in designing and providing safe workplaces avoiding work related illnesses and accidents. This standard focused on the continual improvement and continuous achievement of occupational health and safety objectives together with the fulfilment of legal health and safety requirements. ISO 45001 is based on OHSAS 18001 (Occupational Health and Safety Assessment Series) but is not considered an update but a new standard. (British Standards Institution canceled OHSAS 18001 to adopt ISO 45001)
<b>Relevance to Manufacturing Industry</b>	ISO 45001 is oriented to organisations of any size. ISO 45001 is intended to replace OHSAS 18001 and therefore be certifiable. The standard requires that Occupational Health and Safety risks be addressed and controlled, and opportunities analysed. Apart from the benefits related to the protection and reduction of accidents, the application of this standard shows commitment to corporate responsibility and can benefit by improving the organization's brand identity.
<b>Relevance to STAR</b>	ISO itself mentions that certification is not an absolute necessity, and that it is enough to implement it responsibly, and thus make it public, for it to be beneficial in practice. Discussing and planning with stakeholders the organizational health and safety measures and establishing a management system, as is done with other similar standards such as 9001, can be useful for the industry in general and of course for the manufacturing industry, where machines and humans share space, as shown in one of the pilots of STAR.
<b>Link</b>	<a href="https://www.iso.org/iso-45001-occupational-health-and-safety.html">https://www.iso.org/iso-45001-occupational-health-and-safety.html</a>

#### 4.2.2.7 ISO 12100

<b>Name</b>	<b>Safety of machinery</b>
<b>ICS - TC</b>	13.110 Safety of machinery

	ISO/TC 199 Safety of machinery
<b>Purpose</b>	Specify terminology and principle for achieving safety in the design of machinery and provide a methodology for the same purpose.
<b>Scope</b>	Addressed to manufacturers, workers, managers, business owners
<b>Key implications</b>	Identify different hazards and risks in the design of machinery. This standard assists machine designers in the development of safe machines for their designated use, while helping other stakeholders to understand the terminology and different types of hazards and problems. For example, the standard takes into account hazards of these different types: i) Mechanical; ii) Thermal; iii) Electrical; iv) Vibration related; v) noise-related; vi) related to materials and substances; vii) Radiation; viii) related to overlooking ergonomic principles
<b>Relevance to Manufacturing Industry</b>	Especially from the point of view of machine manufacturers, it is interesting to know the potential problems and risks. Using the standard as a reference point for terminology is also valuable. For example, to correctly define the difference between risks and hazards or to know how to classify these types of hazards and to know their main consequences. ISO 12001 also allows the calculation of risks, so that they can be analysed, evaluated and minimized.
<b>Relevance to STAR</b>	In the case of our project, the use cases are not so much focused on machine manufacturing as on machine usage. In any case, for potential users of the STAR middleware or tools, and who are thinking of developing machinery that is complemented by AI technologies, it may be of interest to know the terminology and assess the risks once the potential hazards are known. This standard may be of interest for activities such as those carried out in WP6.
<b>Link</b>	<a href="https://www.iso.org/standard/51528.html">https://www.iso.org/standard/51528.html</a>

## 4.2.3 Other Relevant Standards

### 4.2.3.1 ISO 9001

<b>Name</b>	<b>Quality management systems</b>
<b>ICS - TC</b>	03.100.70 Management systems 03.120.10 Quality management and quality assurance ISO/TC 176/SC 2 Quality systems
<b>Purpose</b>	Define the requirements for a Quality Management System (QMS). Improve efficiency and customer satisfaction.
<b>Scope</b>	Managers, Quality managers. The ISO 9001 requirements are intended to be applicable to any organization of any type and size.
<b>Key implications</b>	Specify a set of requirements related to the management of

	the entire organisation and its processes. Enables the organization to demonstrate the ability to meet customer statutory and regulatory requirements and allows the organization to improve user satisfaction.
<b>Relevance to Manufacturing Industry</b>	ISO 9001 is the most well-known and globally recognised Quality Management System standard. It enables the organisation to produce consistent outcomes, improving and maintaining client satisfaction all in a measurable and monitorable way. ISO 9001 includes the common Plan-Do-Check-Act (PDCA) approach to manages processes and systems, and to create a continuous cycle of improvement
<b>Relevance to STAR</b>	This standard, like the others in this section, is not specific to manufacturing companies and does not specifically relate to AI systems for safety and security. In any case, ISO 9001 is the most recognized quality standard, and therefore may be of interest to organizations using STAR solutions. Any functionality in these solutions that can facilitate in any way the implementation of the standard would be welcome. This standard may be of interest for activities such as those carried out in WP1.
<b>Link</b>	<a href="https://www.iso.org/iso-9001-quality-management.html">https://www.iso.org/iso-9001-quality-management.html</a> <a href="https://www.iso.org/standard/62085.html">https://www.iso.org/standard/62085.html</a>

#### 4.2.3.2 ISO 14001

<b>Name</b>	<b>Environmental management system</b>
<b>ICS - TC</b>	03.100.70 Management systems 13.020.10 Environmental management ISO/TC 207/SC 1 Environmental management systems
<b>Purpose</b>	Specify the requirements for an environmental management system that organizations can use to monitor and improve their environmental performance
<b>Scope</b>	Managers. The ISO 14001 requirements are intended to be applicable to any organization of any type and size.
<b>Key implications</b>	ISO 14001 allows organisations to define their environmental objectives, while helping them to reduce waste and environmental damage.
<b>Relevance to Manufacturing Industry</b>	Companies can get ISO 14000 certification. Enables companies to identify and manage risks related to the environment and strengthen efforts in the prevention and protection of the environment. The standard can also improve brand image and demonstrate alignment with an image of a sustainable and environmentally friendly company.
<b>Relevance to STAR</b>	Waste management or environmental risks are not one of the key points of the project. Knowing the risks associated with an organization is important, so if in addition to knowing other types of risks one wants to have an environmental management system, implementing ISO 14001 (and even

	getting certified) can be useful.
<b>Link</b>	<a href="https://www.iso.org/iso-14001-environmental-management.html">https://www.iso.org/iso-14001-environmental-management.html</a> <a href="https://www.iso.org/standard/60857.html">https://www.iso.org/standard/60857.html</a>

#### 4.2.3.3 ISO 31000

<b>Name</b>	<b>Risk management</b>
<b>ICS - TC</b>	03.100.01 Company organization and management in general ISO/TC 262 Risk management
<b>Purpose</b>	Help organizations achieve objectives. Improve the identification of threats and plan resources to reduce the risks.
<b>Scope</b>	Management. Applicable to any organization of any type and size.
<b>Key implications</b>	Helps to understand the risks of the organization and the external and internal factors that increase uncertainty about the achievement of objectives. It allows to increase the information for decision making at different stages and in diverse contexts in which the organization is situated.
<b>Relevance to Manufacturing Industry</b>	ISO 31000 is independent of the industry or sector, and thus applicable to the manufacturing industry. This standard is not a certifiable standard but can contribute to the preparation of audits and the certification of other standards.
<b>Relevance to STAR</b>	This is another of the standards that are not specific to AI, manufacturing and safety, but may be of interest for risk awareness and uncertainty reduction. This standard may be of interest for activities such as those carried out in WP1 and WP2.
<b>Link</b>	<a href="https://www.iso.org/standard/65694.html">https://www.iso.org/standard/65694.html</a> <a href="https://www.iso.org/iso-31000-risk-management.html">https://www.iso.org/iso-31000-risk-management.html</a>

#### 4.2.3.4 ISO 26000

<b>Name</b>	<b>Social Responsibility</b>
<b>ICS - TC</b>	03.100.02 Governance and ethics ISO/TMBG Technical Management Board - groups
<b>Purpose</b>	Assist organisations in operating in a socially responsible way and contribute to sustainable development
<b>Scope</b>	Management. Applicable to any organization of any type and size.
<b>Key implications</b>	Provides background and guidance on social responsibility. guides implementing socially responsible behaviour throughout the organization. Collaborates in the promotion of sustainable development. Identify engaging potential with stakeholders.
<b>Relevance to Manufacturing Industry</b>	ISO 26000 is independent of the size, location and sector of the organisation so is applicable to the manufacturing industry. ISO 26000 provides guidance, and it cannot be certified. Is not based on providing requirements but on guiding organisations on maintaining a more sustainable approach. For the

	manufacturing industry the contribution to sustainable development, the improvements in the collaboration with stakeholders following a similar approach, and the benefits in the brand image can be positive.
<b>Relevance to STAR</b>	This standard along with others mentioned in this section do not present requirements but offers a guide for organizations to go beyond their activity and contribute to relevant causes. As with all other manufacturing organizations, STAR users can benefit from a brand image, stakeholder engagement, and a commitment to social responsibility.
<b>Link</b>	<a href="https://www.iso.org/iso-26000-social-responsibility.html">https://www.iso.org/iso-26000-social-responsibility.html</a> <a href="https://www.iso.org/standard/42546.html">https://www.iso.org/standard/42546.html</a>

#### 4.2.3.5 OASIS PMRM

<b>Name</b>	<b>OASIS Privacy Management Reference Model (PMRM)</b>
<b>ICS - TC</b>	OASIS Privacy Management Reference Model (PMRM) TC
<b>Purpose</b>	The OASIS PMRM TC works to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations.
<b>Scope</b>	PMRM provides a guideline or template for developing operational solutions to privacy issues. It also serves as an analytical tool for assessing the completeness of proposed solutions and as the basis for establishing categories and groupings of privacy management controls.
<b>Key implications</b>	Offer guidance to developers and engineers to identify security and privacy risks during the development and the implementation stage of an industrial service.
<b>Relevance to Manufacturing Industry</b>	The PMRM, as a methodology, covers a series of tasks that allows to define Uses Cases and to identify flows of data across complex environment, thus crossing the single shopfloor or manufacturing domain and covering the value chain dimension. Moreover, the PMRM is not prescriptive and the users of the PMRM may choose to adopt some parts of the modes and not all of them.
<b>Relevance to STAR</b>	In some cases, project pilots or middleware users need to manage personal information (e.g., activity data). In those cases, it is important to understand the risks and establish policies and procedures to reduce the main risks related to that private information. This standard may be of interest for activities such as those carried out in WP6.
<b>Link</b>	<a href="http://docs.oasis-open.org/pmr/pmr/v1.0/cs02/PMRM-v1.0-cs02.html">http://docs.oasis-open.org/pmr/pmr/v1.0/cs02/PMRM-v1.0-cs02.html</a>

#### 4.2.3.6 OASIS TOSCA

<b>Name</b>	<b>OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC</b>
<b>ICS - TC</b>	OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) Technical Committee

<b>Purpose</b>	TOSCA aim is enhancing the portability and operational management of cloud and other types of applications and services across their entire lifecycle.
<b>Scope</b>	TOSCA will enable the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behaviour of these services (e.g., deploy, patch, shutdown)-independent of the supplier creating the service, and any particular cloud provider or hosting technology. TOSCA will also make it possible for higher-level operational behaviour to be associated with cloud infrastructure management
<b>Key implications</b>	TOSCA provides support to design, write, integrate and deploy cloud services in a cloud environment as well as in a mix of cloud environments and on-premise environments; being a standard, it offers the guidance for the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behaviour of these services (e.g., deploy, patch, shutdown) independent of the supplier creating the service, and any particular cloud provider or hosting technology.
<b>Relevance to Manufacturing Industry</b>	TOSCA will support the design and management of complex cloud-based systems, also hybrid ones where part of the services are available on the Cloud and other at manufacturing companies' premises, thus boosting the integration and management of data stored in different systems and locations. TOSCA TC has launched a new Ad Hoc Workgroup focused on IoT/Edge/Fog to explore opportunities for TOSCA applications within these new domains
<b>Relevance to STAR</b>	TOSCA could help all those project pilots or service developer users that need to deploy new services or access data in the cloud-based infrastructure of the project.
<b>Link</b>	<a href="https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca">https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca</a>

## 4.3 Industrial Architectures and Infrastructures

### 4.3.1 Reference Architecture Models

Being STAR a project about digital manufacturing systems, and about the integration of AI technologies, it is important to know and be aligned with some of the reference architectures, infrastructures and technologies that are becoming practically standard.

The advent of Industry 4.0 and smart manufacturing has given rise to the specifications of various architectures and reference models for developing digitally enabled industrial systems, notably systems that leverage Cyber Physical Production Systems (CPPS). These models describe the structuring principles and the main building blocks of modern industrial systems.

In most cases, these reference models lead to industrial systems that fall in the realm of the Industrial Internet of Things (IIoT). The latter include data-intensive components such as components based on Big Data analytics and Machine Learning (ML). As such their

structuring principles are relevant to the development of AI systems. The following paragraphs review some of the most popular reference models for architecting Industry 4.0 systems including AI systems.

#### 4.3.1.1 Reference Architecture Model Industrie 4.0 (RAMI 4.0)

RAMI4.0 provides structuring concepts and a vocabulary for understanding Industry 4.0 systems and their deployment. RAMI describes the structure and main elements of Industry 4.0 system by means of a 3D layered model (Figure 2). The three layers of the 3D model corresponding to:

- The Architecture axis (Layers), which comprises six different layers indicating functionalities at different granularities of the system, from the asset to the business level.
- The Process axis (Value Stream), which illustrates the stages of an asset's lifecycle, along with a corresponding value creation process based on IEC 62890.
- The Hierarchy axis (Hierarchy levels), which presents describes the breakdown structure of assembled components based on a taxonomy that starts from the product and goes up to the connected smart factory. The various levels are driven by the DIN EN 62264-1 and DIN EN 61512-1 standards.

The architecture layers of RAMI4.0 include:

- The Asset Layer, which describes physical systems and components (e.g., machines, motors, software applications, spare parts).
- The Integration Layer, which links the physical and digital/cyber worlds based on components like drivers and middleware.
- The Communication Layer, which deals with communications between the integration and information layers. It employs network protocols (e.g., TCP/IP, HTTP, FTP) over LAN and WAN networks, including wireless networks.
- The Information Layer, which provides (digital) information about sales, purchase orders, suppliers, locations, etc. along with information on materials, machines and components that support the production.
- The Functional Layer, which comprises production rules, actions, processing, and system control.
- The Business Layer, which is associated with the business strategy, the business environment, and business goals of the enterprise, including promotions, offers, pricing models and cost analysis.

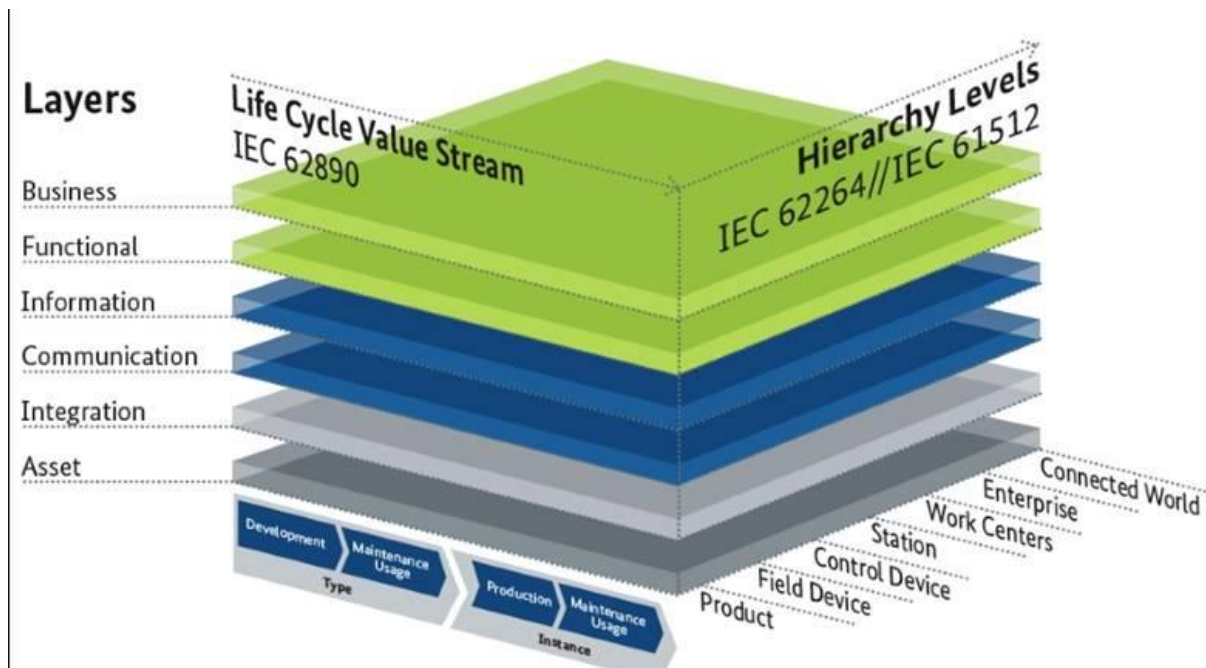


Figure 2: Reference Architecture Model Industry 4.0 (RAMI 4.0)

#### 4.3.1.1.1 Process Value Streams

The Process axis deals with the lifecycle and processes of an object, which typically comprises a product, physical entities (e.g., machines and spare parts), or even virtual entities (e.g., documents and project plans). Every product needs to be updated, restructured, redesigned, or reformed for maintenance purposes. In this context, the process layer specifies Types and Instances as its main methods. A product in a development state is referred to as a "Type". Once moved to production, it becomes an "Instance". As illustrated in the RAMI4.0 cube, a "Type" is also subject to maintenance activities. A product returns to the "Type" state, whenever it is redesigned, or a new feature is being added to it.

#### 4.3.1.1.2 Hierarchical Levels

The hierarchy levels of the corresponding axis are as follows: (i) Product, which abstracts the product that is manufactured in a factory; (ii) Field device, such as sensor and electronic devices that capture and/or control data from the field; (iii) Control device, which corresponds to the Operational Technology (OT) that manages input and output. Prominent examples are PLCs (Programmable Logic Controllers) and DCSs (Distributed Control Systems); (iv) Station, which enables operators to coordinate several processes and monitoring the results, by means of automation systems such as SCADA; (v) Work Center, which keeps track of manufacturing information and parameters that enable quality management; (vi) Enterprise, which comprises the core business processes (e.g., production planning, production scheduling, marketing and sales, financial modules) that are usually managed through an ERP system; (vii) Connected World, which deals with the interlinking of all stakeholders as part of their supply chain interactions (including information sharing and exchange among them).

#### 4.3.1.2 The Industrial Internet Consortium Reference Architecture (IIRA)

The IIRA specifies a common architecture framework for developing interoperable IoT systems for different vertical industries. It is an open, standards-based architecture, which

has broad applicability. The latter makes it a vehicle for interoperability, mapping, and practical deployment of IoT technologies, as well as standards development. To ensure its broad applicability, the IIRA is fairly generic, abstract and high-level. Hence, it can be used to drive the structuring principles of an IoT system, without however specifying its low-level implementation details. It is also a very good vehicle for communicating concepts and facilitating stakeholders’ collaboration.

Based on the analysis of multiple use cases in a different sector, the IIRA presents the structure of IoT systems from four viewpoints, namely business, usage, functional and implementation viewpoints. Among these four viewpoints, it’s the functional viewpoint that specifies the functionalities of an IIoT system. To this end, the functional viewpoints specify distinct functionalities in the form of the so-called “functional domains”. Functional domains can be used to decompose an IoT systems in a set of important building blocks, which are applicable across different vertical domains and applications. As such functional domains are used to conceptualize concrete functional architectures. The IIRA decomposes a typical IoT/IIoT system into five functional domains (see Figure 3), namely a control domain, an operations domain, an information domain, an application domain and a business domain as outlined in. The implementation viewpoint of the IIRA is based on a three-tier architecture, which follows the edge/cloud computing paradigm. It includes an edge, a platform and an enterprise tier.

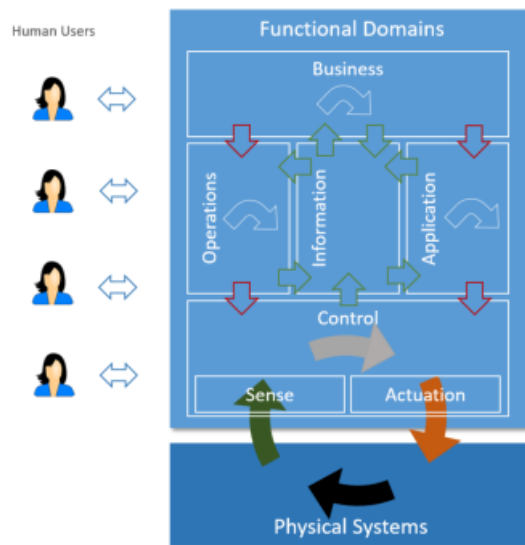


Figure 3: Functional Domains in the IIRA

#### 4.3.1.3 The OpenFog Reference Architecture (RA)

The OpenFog Consortium was a consortium of high-tech industrial enterprises companies and research/academic institutions, which are collaborating towards standardizing and promoting the fog computing paradigm. Since December 2018, the OpenFog Consortium and the IIC have joined forces<sup>25</sup> Fog computing is directly associated with IoT, as it leverages fog nodes (i.e., essentially IoT devices) in order to enable reliable, low latency IoT applications. Fog computing alleviates the limitations and drawbacks of conventional cloud computing in various scenarios where low-latency and processing close to the field is required. The RA of the OpenFog consortium illustrates the structure of fog computing

<sup>25</sup> <https://www.iiconsortium.org/press-room/12-18-18.htm>

systems. It presents how fog nodes can be connected partially or fully to enhance the intelligence and operation of an IoT system. Moreover, it presents solutions about growing system wide intelligence away from low-level processing of raw data. The RA is described in terms of different views, including functional and deployment views. OpenFog compliant systems include some cross-cutting functionalities (i.e., functionalities that are applied across all layers of an IoT / OpenFog system). These cross-cutting functionalities are conveniently called “perspectives”.

#### 4.3.1.4 ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)

ISO/IEC 30141:2018<sup>26</sup> provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top-down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model (CM). The latter has been derived based on a heuristic analysis of system characteristics that are common in most IoT systems (e.g., auto-configuration, discoverability, scalability, etc.). The CM describes typical IoT entities or actors, along with their relationships. The architecture is described by means of five complementary views i.e., functional, system, communications, information and usage.

#### 4.3.1.5 BigData Value Reference Model

The BDV Reference Model provides the means for representing AI, ML, and BigData analytics pipelines<sup>27</sup>. It distinguishes between two different elements: (i) Elements that are at the core of the BDVA (Big Data Value Association); and (ii) Features that are developed in strong collaboration with related European activities. The model is structured into horizontal and vertical concerns:

- Horizontal concerns focus on the data processing chain, starting with data collection and ingestion, and extending to data visualisation. Horizontal concerns do not imply a layered architecture. For instance, visualisation may be applied directly to collected data without the need for intermediate functions like data processing and analytics.
- Vertical concerns address cross-cutting issues that apply to all horizontal functions and may include non-technical aspects.

The BDV Reference Model is compatible with reference architectures for AI, most notably with the ISO JTC1 WG9 Big Data Reference Architecture.

---

<sup>26</sup> <https://www.iso.org/standard/65695.html>

<sup>27</sup> [https://www.iso.org/files/live/sites/isoorg/files/developing\\_standards/docs/en/big\\_data\\_report-jtc1.pdf](https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/big_data_report-jtc1.pdf)

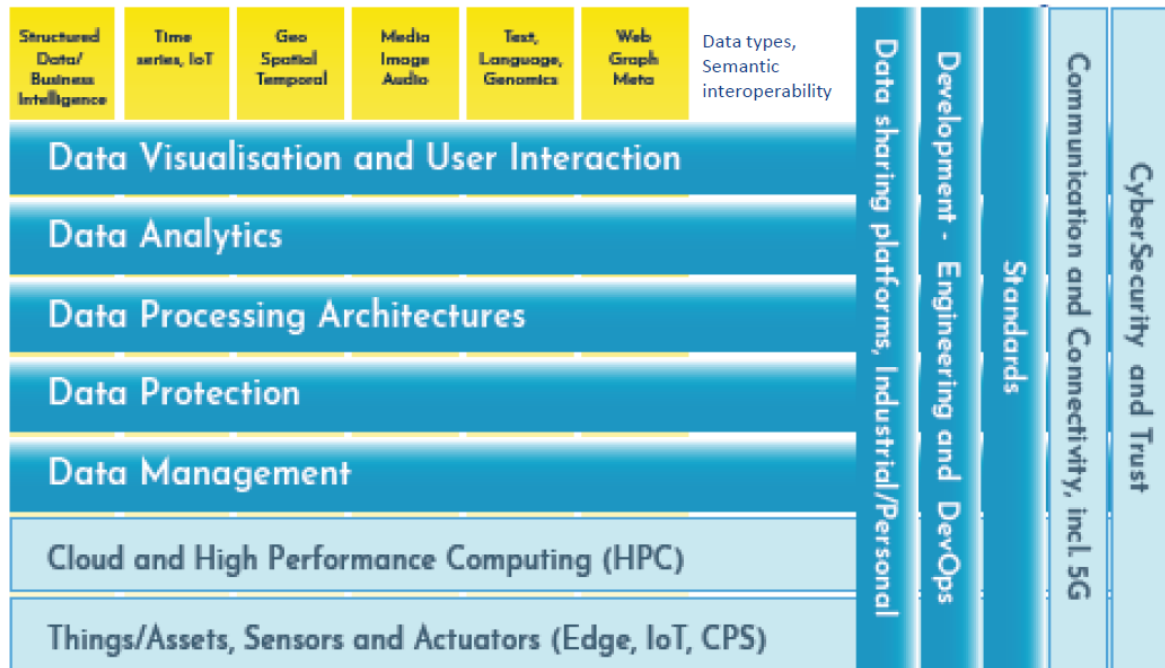


Figure 4: BDVA Reference Architecture Model for BigData Analytics and Machine Learning

### 4.3.2 Infrastructures for Industrial Systems

As far as infrastructures are concerned, we can mention GAIA-X<sup>28</sup> (a Federated Data Infrastructure for Europe). GAIA-X is an initiative launched by representatives from business, science and politics on a European level to create a proposal for the next generation of a European data infrastructure and thus enable EU companies to compete globally, exploiting data and services made available in an open digital and trusted ecosystem. GAIA-X connects centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. The resulting federated form of data infrastructure strengthens the ability to both access and share data securely and confidently. Specifically, for the Industry4.0 sector, GAIA-X infrastructure opens opportunities for the development of new solutions for Smart Manufacturing, Supply Chain collaboration, Shared Production, Predictive Maintenance, Connected ShopFloor and more.

## 4.4 Guidelines and Recommendations

As far as standards are concerned, different options have been presented: some related to technical, management and security, others more focused on safety and health and finally some more generic standards.

The latter include quality standards such as ISO 9001, and also some recommendations on sustainability and environmental risk management. All of these can be useful from a more global point of view if the company's management is aiming for certification (in the case of ISO 9001) or simply following recommendations to improve its brand image, or relations with the environment or customers.

As for safety and health standards, many of them are related to human-machine interaction, to input devices, or to how to share space with machines. All of them have relevance for innovative projects in the manufacturing environment. In the project pilots, there is no need

<sup>28</sup> <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>

to follow these standards to the letter, if the organization is not considering applying them, but it is important to maintain the ideas that these standards promote, Safety and Health in the workplace and in the day-to-day design of the operators, when designing the proofs of concept.

Finally, in relation to security, and being a project with trust, safety and security as key concepts, it is interesting to know the risks related to these aspects. Therefore, the evaluation and management of technical risks, either following one of the suggested standards or inspired by them, is important to evaluate and validate the results based on the platform developed in the project.

Regarding architectures, the ones we have presented are reference architectures that can simplify implementations or at least reduce the time and effort spent to design an architecture for a specific project. From that point of view, they are interesting for the manufacturing industry and for the potential users of the project

## 5 Conclusion

We aimed to produce an extensive overview of the most relevant standards and regulations that could serve project members and interested parties as a point of entry and access to different documents. As mentioned, we did not intend to cover all the hundreds/thousands of possibilities that exist, but rather to invite partners to provide some of the applicable standards or directives they were interested in or had simply heard about. These standards and guidelines have been used to classify them into groups and to make a kind of datasheet for each one. In this way, users can get an idea of the content and applicability, and visit both the standardization committees and groups, as well as the links to these standardization documents or directives.

It is worth mentioning that we have attempted to extend the information with some reference architectures that might be of interest to developers of safe systems for the manufacturing industry and also some technical groups and standards that may also be relevant.

During the elaboration of this deliverable two book chapters were written, one on standards and architectures, and one on directives, regulations and legal aspects. These chapters have been included in the book "Trusted Artificial Intelligence in Manufacturing" (John Soldatos (ed.))

## 6 References

- Choi, S. e. (2016). An analysis of technologies and standards for designing smart manufacturing systems. *Journal of research of the national institute of standards and technology* 121, 422-433.
- John Soldatos (ed.), D. K. (n.d.). *Trusted Artificial Intelligence in Manufacturing: A Review of the Emerging Wave of Ethical and Human Centric AI Technologies for Smart Production"*. , Boston-Delft: now publishers, <http://dx.doi.org/10.1561/9781680838770>.
- Li, Q. T. (2018). Smart manufacturing standardization: Architectures, reference models and standards framework. *Computers in Industry*, 101, 91-106.
- Van Acker, B. (2020). *Mental Workload Monitoring in the Manufacturing Industry: Conceptualisation, Operationalisation and Implementation*. Doctoral dissertation, Ghent University.
- Ziegler, W. (2020). A Landscape Analysis of Standardisation in the Field of Artificial Intelligence. *Journal of ICT Standardization* , 151-184.