

HORIZON 2020

European Connected Factory Platform for Agile Manufacturing



European Factory
Platform

WP11: Dissemination, Collaboration and Standardisation

D11.9: Regulatory Alignment, Compliance and Standardisation Strategies - Final Report

Vs: 1.0

Deliverable Lead and Editor: Andreas Feigl, Karl Grün, Erwin Haubert and Martin Lorenz (ASI)

Contributing Partners: ICE, FIT, SFRG, A-D, CERTH, FOR, NXW, C2K, CNET, ASC, SRDC, IAI

Date: 2022-12-02

Dissemination: Public

Status: <Draft | Consortium Approved | EU Approved>

Short Abstract

The deliverable describes the final report about the strategy of EFPP regarding the alignment and compliance of activities and results of the project with standards and regulations.

Grant Agreement:
825075



Document Status

Deliverable Lead	Andreas Feigl, Karl Grün, Erwin Haubert and Martin Lorenz (ASI)
Internal Reviewer 1	ICE
Internal Reviewer 2	AID
Type	Deliverable
Work Package	WP11: Dissemination, Collaboration and Standardisation
ID	D11.9: Regulatory Alignment, Compliance and Standardisation Strategies - Final Report
Due Date	2022-12-31
Delivery Date	2022-12-02 (V1.0)
Status	<Draft Consortium Approved EU Approved>

History

See Annexe A.

Status

This deliverable is subject to final acceptance by the European Commission.

Further Information

www.efpf.org

Disclaimer

The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document.

Furthermore, the information is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sole risk and liability.

Project Partners:



Executive Summary

This report is part of the WP11 “Dissemination, Collaboration and Standardisation” and targets standardisation, which is an important pillar in EFPF looking at how the results of the EFPF project can be brought to bear in the European economic. The work for this deliverable is performed in task T11.3, which focuses on regulatory alignment, compliance and standardisation strategies

This document serves as a guide for the EFPF partners on the most relevant standards (published and under development) and regulations with an impact on the successful operation of the tasks and technical deliverables of the project. This document additionally serves as a guide emphasizing standardisation activities (standards under development) that are strategically important to EFPF, to ensure an alignment between the standards and the project outcomes.

Section 0 is an introduction to the EFPF project and provides information about the context, purpose and structure of this deliverable. Section 1 provides the detailed overview of active participation of the EFPF partners in standardisation activities and is based on an extensive survey. Section 2 summarises the responses received from EFPF partners on regulations that affect or may affect EFPF in the future. Section 3 contains the standardisation strategy, which is divided in three parts, i.e. strategic areas of involvement in standardisation committees elaborating standards, participation in strategic standardisation groups and the concept of a CEN Workshop Agreement that supports EFPF as a digital platform. Section 4 highlights our strategy on regulations. Finally, Section 5 concludes the deliverable.

By presenting the EFPF Regulatory Alignment, Compliance and Standardisation Strategy, we highlight the importance of standardisation in the project and in ongoing digital manufacturing initiatives and define a coherent approach towards further standardisation and regulation activities.

Table of Contents

0	Introduction	1
0.1	EFPF Project Overview	1
0.2	Deliverable Purpose and Scope	1
0.3	Target Audience	1
0.4	Deliverable Context	1
0.5	Document Structure.....	2
0.6	Document Status	2
0.7	Document Dependencies	2
0.8	Glossary and Abbreviations.....	2
0.9	External Annexes and Supporting Documents	2
0.10	Reading Notes.....	2
1	Overview of active Participation of EFPF Partners in Standardisation Activities.....	3
1.1	The standardisation ecosystem	3
1.2	Results of the Survey on Standardisation Activities.....	6
1.3	Contributions to standardisation from selected open calls.....	43
2	Overview of Regulations affecting the EFPF Project Partners.....	49
3	Standardisation Strategy.....	56
3.1	Strategic Areas of Participation	57
3.2	Participation in Strategic Groups	63
3.3	CEN-CENELEC Workshop EFPFInterOp.....	64
3.4	Digital Manufacturing Platforms for Connected Smart Factories	69
3.5	Dissemination of EFPF goals in other fields of the standardisation network	70
4	Strategy on Regulations.....	71
5	Summary	74
	Annex A: History	75
	Annex B: References	77

0 Introduction

0.1 EFPF Project Overview

EFPF – European Connected Factory Platform for Agile Manufacturing – is a project funded by the H2020 Framework Programme of the European Commission under Grant Agreement 825075 and conducted from January 2019 until December 2022. It engages 30 partners (Users, Technology Providers, Consultants and Research Institutes) from 11 countries with a total budget of circa 16M€. Further information can be found at www.efpf.org.

To foster the growth of a pan-European platform ecosystem that enables the transition from "analogue-first" mass production, to "digital twins" and lot-size-one manufacturing, the EFPF project will design, build and operate a federated digital manufacturing platform. The platform will be bootstrapped by interlinking four base platforms from FoF-11-2016 cluster funded by the European Commission, early on. This will inform the design of the EFPF Data Spine and the associated toolsets to fully connect the existing user communities of the four base platforms. The federated EFPF platform will also be offered to new users through a unified Portal with value-added features such as single sign-on (SSO), user access management functionalities to hide the complexity of dealing with different platform and solution providers.

0.2 Deliverable Purpose and Scope

The purpose of this deliverable D11.9: Regulatory Alignment, Compliance and Standardisation Strategies - Final Report is to target standardisation, which is an important pillar in EFPF looking at how the results of the EFPF project can be brought to bear in the European economic.

The strategic orientation towards an active participation in the standardisation process is essential for the EFPF project.

Based on the standardisation plan (D11.11) and the Regulatory Alignment, Compliance and Standardisation Strategies (D11.2), this document is the final report about the standardisation and regulation strategies in the areas of interest for the EFPF project.

This deliverable also contains an overview of regional, national, European, or International regulations which affect the operation and foreseen results of the project. These regulations need to be respected by all project partners.

Another very important purpose of this deliverable is to demonstrate, that the novel results of EFPF comply with regulatory requirements and with standards, through which the confidence in, and the market uptake of, these results can be enhanced.

0.3 Target Audience

The deliverable is declared public and therefore its content can be used for raising the awareness of project among wider audience.

This document is intended to refer the EFPF partners at the process of integration of the results of the project into standards and at the regulations with which the project results should be compliant.

0.4 Deliverable Context

This document is one of the cornerstones for achieving the project aims. Its relationship to other documents is as follows:

- **Description of Action (DOA):** Provides the foundation for the actual research and technological content of EFPF. Importantly, the Description of Action includes a description of

the overall project work plan.

- **Project Handbook (D1.1):** Provides the foundation for the practical work in the project throughout its duration and helps to ensure that the project partners follow the same well-defined procedures and practices also in terms of information sharing.

0.5 Document Structure

This deliverable is broken down into the following sections:

- **Section 1: Overview of active Participation of EFPF Partners in Standardisation Activities** describes how the relevant areas of standardisation in EFPF are identified
- **Section 2: Overview of Regulations affecting the EFPF Project Partners** describes relevant regulations in EFPF
- **Section 3: Standardisation Strategy** describes the standardisation strategy of the EFPF project
- **Section 4: Strategy on Regulations** describes the regulations affecting the EFPF project
- **Section 5: Summary**
- **Annexes:**
 - **Annex A:** Document History
 - **Annex B:** References

0.6 Document Status

This document is listed in the Description of Action as "public".

0.7 Document Dependencies

This document is the second part of three deliverables within this task (T11.3) and will serve as the basis for the final regulatory alignment, compliance and standardisation strategy.

0.8 Glossary and Abbreviations

A definition of standard terms related to EFPF, as well as a list of abbreviations, is available at <https://www.EFPF.org/glossary>

0.9 External Annexes and Supporting Documents

Annexes and Supporting Documents:

- Survey on standardisation activities
- Survey on regulations

0.10 Reading Notes

- None

1 Overview of active Participation of EFPF Partners in Standardisation Activities

The standardisation activities in EFPF are designed with the focus on standardisation and utilisation of relevant standards.

ASI, as lead of T11.3, has prepared a survey of the relevant and active standardisation initiatives that EFPF partners can leverage, participate, and contribute towards. The survey was sent out from August 12th to October 28th, 2019 for feedback from the partners. This initial consolidated outlook of the partner feedback was provided in Section 1.1 of D11.2. After this initial feedback round, partners were regularly asked by ASI to update their input:

- June 2021
- December 2021
- June 2022

The consolidated version is provided in Section 1.2 of D11.4.

A webinar was held on February 7th, 2020 to prepare the project partners for an active collaboration on standardisation and to highlight available opportunities. The following topics were presented by ASI during the webinar include:

- The standardisation process of CEN, CENELEC, ISO, and IEC in a nutshell.
- How to influence/contribute to standards currently under development?
- How to initiate the elaboration of a new standard or the revision of an existing standard?
- Intellectual property issues in standardisation (IPR policy of standardisation bodies).
- Are there technical barriers in existing standards to the technical issues of current EFPF project activities? Relation to the current standardisation plan (D11.11).
- Survey on Standardisation Activities.
- Position of EFPF in the Digital Manufacturing Cluster (with ZDMP and QU4LITY projects).

As a follow up action, more webinars and bilateral meetings were organised to gather partner feedback, highlight areas of interest and ongoing developments in the standardisation field and to assist partners in their standardisation activities.

To gain deeper insights in the use of standards and to further improve the contribution of EFPF to standardisation Task T11.3 took advantage of the Open Call Experimentation managed under WP8. The Open Call candidates were asked to provide information which standards they are using for their solutions and in which standardisation activities they participate, if any. The result from those applicants having been positively evaluated are included in section 1.3.

1.1 The standardisation ecosystem

In ISO/IEC Guide 2:2004¹, 1.1 standardisation is defined as an activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context. Important benefits of standardisation are improvement of the suitability of products, processes and services for their intended purposes, prevention of barriers to trade and facilitation of technological cooperation. Standardisation supports the social and economic development by ensuring safety, quality and competitiveness of products, services and processes on various levels (e.g. performance, composition, interoperability, applicability and many more). This in turn supports economic activity of businesses of all sizes and

¹ ISO/IEC Guide 2:2004, Standardisation and related activities — General vocabulary, is adopted in Europe as European Standard EN 45020:2006.

allows them access markets all over the world.

Standardisation is governed by the principles of consensus, openness, inclusiveness transparency, national commitment and coherence as outlined in the Agreement on Technical Barriers to Trade of the World Trade Organisation (WTO TBT Agreement) and in Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation.

The output of standardisation are standards. According to ISO/IEC Guide 2:2004, 3.1 a standard is a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards are voluntary in their application and should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits. Standards are initiated and drafted by stakeholders such as industry, incl. SMEs, public authorities, research organisations, societal and environmental stakeholders, consumer organisations, trade unions and conformity assessment bodies.

There are numerous organisations developing standards, ranging from companies, consortia and industry in the private sector, to national, regional and international organisations. The latter three constitute the bulk of the international standardisation system, required by the WTO TBT Agreement to follow its principles and requirements for standards development. There are also NGOs with specific socio-economic or environmental goals that develop and publish standards.

National Standardisation Bodies (NSB) are standardisation organisations located in each country. They bridge the local communities with groups of relevant stakeholders outside of their country and represent the pillars of the European and International standardisation. Being member of European Standardisation Organisations NSBs are obliged to implement European Standards as national standards and withdraw any conflicting national standards.

The European standardisation activities are conducted within the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI).

CEN brings together the national standardisation bodies of 34 European countries and provides a platform for standardisation in various areas, including products, materials, services, and processes. CENELEC ensures standardisation in the electro-technical engineering field, and ETSI produces standards for information and communications technology.

The network of European standardisation includes more than 200.000 experts from different countries and from the different stakeholders, i.e. business, industry and commerce, service providers, consumers, environmental and societal organisations, public authorities and regulators, as well as other public and private institutions. The European Standardisation Organisations aim to support needs of the market and of different stakeholders, promoting the European Standardisation System and leading the implementation of best practice in standardisation around the world. They collaborate with key stakeholders' organisations at national, European and international level, support international Standardisation and cooperate closely with international Standardisation Organisation such as ISO and IEC. Participation in European Standardisation follows the national delegation principle, i. e. national members (NSB, NC) host national committees populated with national stakeholders and these national committees contribute to the elaboration of European Standards.

International standardisation activities are conducted at three major international Standardisation Organisation: International Organisation for Standardisation (ISO), International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU).

ISO is an independent international organisation that includes 165 national standards bodies as its members. International standards, produced by ISO, cover a wide variety of areas and represent consensus of experts from many countries. All CEN members are also members of ISO.

Members of IEC are 89 National Committees, represented by delegates from industry, research and government bodies of each country. IEC produces standards covering all aspects of production and use of electrical and electronic devices and systems. All CENELEC members are also members of IEC.

CEN and CENELEC have dedicated agreements with the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), promoting the benefits of the international standards to international trade and markets harmonisation. The high level of convergence between the European and international standards is facilitated by the ongoing technical cooperation between CEN and ISO (Vienna Agreement) and between CENELEC and IEC (Frankfurt Agreement). The main objectives of these agreements are to provide a:

- framework for the optimal use of resources and expertise available for standardisation work;
- mechanism for information exchange between international and European Standardisation Organisations to increase the transparency of ongoing work at international and European levels.

International Standards from ISO and IEC following the Vienna or Frankfurt Agreement become the status of European Standards (designation EN ISO, EN ISO/IEC, EN IEC).

ITU is an inter-governmental organisation belonging to the United Nations and develops technical standards that facilitate the use of public telecommunication services and systems for communications in the area of ICT. Its membership comprises nearly 200 countries and almost 800 private-sector entities and academic institutions.

Participation in International Standardisation of ISO and IEC follows the national delegation principle, i. e. national members (NSB, NC) host national committees populated with national stakeholders and these national committees contribute to the elaboration of International Standards.

A vast array of normative documents is classed under the generic label of "private standards". Generally, a normative document developed and published by an organisation outside of the recognized standards development organisations at national, regional or international level is considered to be a private standard. There is not only a vast range of private standards (and growing in number), but there are also significant differences between the bodies and organisations that develop these standards related to such aspects as governance, development approach, stakeholder engagement, transparency, and consensus.

Some of these Private Standards Development Organisations liaise with recognized standards development organisations. Such examples are IEEE and ENISA liaising with ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection or OASIS liaising with ISO/IEC JTC 1/SC 37/WG 2, Biometric technical interfaces.

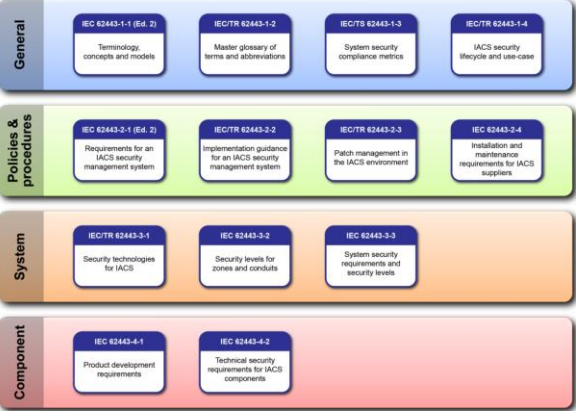
Some specifications from Private Standards Development Organisations were provided by them to recognized standards development organisations in order to be implemented as standards. Such example is the OPC Unified Architecture (OPC UA) being a machine-to-machine communication protocol for industrial automation developed by the OPC Foundation and adopted by IEC as IEC 62541. Another example is ISO/IEC 20922:2016 which was prepared by the OASIS Message Queuing Telemetry Transport (MQTT) Technical Committee and was adopted by Joint Technical Committee ISO/IEC JTC 1, Information technology.

1.2 Results of the Survey on Standardisation Activities

Based on the identification of relevant standardisation activities, the EFPF standardisation related contributions of project partners are expected in the following areas.

NOTE – Standards (published and under development) and Standardisation bodies are hyperlinked to websites for detailed information, incl. previews of standard content.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
CEN Workshop of MONSOON H2020 Project (MOdel based coNtrol framework for Site-wide Optimisation of data-intensive processes)	CWA 17492 , Predictive control and maintenance of data intensive industrial processes	published	This document contains a methodology detailing the machine/deep learning techniques that should be employed with the aim to predict industrial processes or equipment drifts and trigger alarms and potentially help to improve overall equipment effectiveness or the workshop performances. This document can be used as a guide by Manufacturing plant managers and Data Scientists.	Industrial Processes	C2K has studied and implemented this standard for the realisation of data intensive industrial processes. ICE is investigating CWA 17942, in particular, how it can be used to support and enhance the machine learning techniques deployed within the ICEData Analytics – Anomaly Detection Tool.
Eclipse Foundation	Sparkplug Specification	published	Sparkplug™ provides an open and freely available specification for how Edge of Network (EoN) gateways or native MQTT enabled end devices and MQTT Applications communicate bi-directionally within an MQTT Infrastructure. This document details the structure and implementation requirements for Sparkplug™ compliant MQTT Client implementations on both devices and applications.	MQTT, IoT	ICE's Pub Sub Security Service has considered and implemented the Sparkplug specification to provide a framework for the standardised definition of topics in the EFPF Message Bus. FOR has integrated MQTT Sparkplug into TSMATCH, having developed a White paper on the integration aspects.
ETSI ISG IPE	Industry Specification Group (ISG) on IPv6 Enhanced innovation (ISG IPE)	Under development	The aim of this project is the following: <ul style="list-style-type: none"> Identify gaps and recommendations of existing and required IPv6 standards both inside ETSI and in other SDOs; 	Cloud computing, industrial internet	FOR participates in this group, monitoring to ensure alignment with new developments in

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			<ul style="list-style-type: none"> Identify and describe IPv6 Network related use cases & specific scenarios, derived requirements and IPv6 networking challenges in the following areas: IPv6 based 5G (and beyond 5G) IP transport and cloud & IP network convergence IPv6 based enterprise networking and Industrial Internet IPv6 cybersecurity and management, Document an automated networking e2e reference architecture, using IPv6; Describe an IPv6 based specific deployment best practices / guidelines and transition tools for: (1) IPv4 to IPv6, (2) dual stack to IPv6 only; Provide and demonstrate PoCs and test case descriptions to validate IPv6 standards based approaches. 		<p>terms of service interconnection based on IPv6.</p>
<p>IEC/TC 65, Industrial-process measurement, control and automation</p>	<p>IEC TS 62443-1-1:2009, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models IEC TS 62443-1-5 ED1, Rules for IEC 62443 Profiles (under development) IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program IEC 62443-2-2 ED1, Security for industrial automation and control systems – Part 2-2: IACS Security Program Ratings</p>	<p>Published, some parts under development</p>	<p>This multi-part standard is divided into different sections and describes both technical and process-related aspects of industrial cybersecurity. It divides the industry into different roles: the operator, the integrators (service providers for integration and maintenance) and the manufacturers. The different roles each follow a risk-based approach to prevent and manage security risks in their activities.</p>  <p>The diagram illustrates the structure of the IEC 62443 standard, organized into four main categories:</p> <ul style="list-style-type: none"> General: <ul style="list-style-type: none"> IEC 62443-1-1 (Ed. 2): Terminology, concepts and models IEC/TR 62443-1-2: Master glossary of terms and abbreviations IEC/TR 62443-1-3: System security compliance metrics IEC/TR 62443-1-4: IACS security lifecycle and use-case Policies & procedures: <ul style="list-style-type: none"> IEC 62443-2-1 (Ed. 2): Requirements for an IACS security management system IEC/TR 62443-2-2: Implementation guidance for an IACS security management system IEC/TR 62443-2-3: Patch management in the IACS environment IEC 62443-2-4: Installation and maintenance requirements for IACS suppliers System: <ul style="list-style-type: none"> IEC/TR 62443-3-1: Security technologies for IACS IEC 62443-3-2: Security levels for zones and conduits IEC 62443-3-3: System security requirements and security levels Component: <ul style="list-style-type: none"> IEC 62443-4-1: Product development requirements IEC 62443-4-2: Technical security requirements for IACS components 	<p>Industrial process measurement and control, IoT integration, security</p>	<p>Following a preliminary analysis of the published parts of the standard, NXW is considering IEC TS 62443, parts 3 and 4 in particular, to define the guidelines for the development of its next generation factory connectors. CNet will monitor the standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration. CERTH will use IDS Trusted Connector for secure connectivity of fill level sensors of industrial open top containers. This type of connectors following the</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	<p>IEC TR 62443-2-3:2015, Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment</p> <p>IEC 62443-2-4:2015, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers</p> <p>IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers</p> <p>IEC 62443-2-4:2015/COR1:2015, Corrigendum 1 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers</p> <p>IEC TR 62443-3-1:2009, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems</p> <p>IEC 62443-3-2:2020, Security for industrial automation and control</p>		<p>IEC 62443 describes different levels of maturity for processes and technical requirements. The maturity levels for processes are based on the maturity levels from the CMMI framework.</p> <p>Maturity Level: IEC 62443 describes different maturity levels for processes through so-called "maturity levels". To fulfil a certain level of a maturity level, all process-related requirements must always be practiced during product development or integration, i.e. the selection of only individual criteria ("cherry picking") is not standard-compliant.</p> <p>The maturity levels are described as follows:</p> <p>Maturity Level 1 - Initial: Product suppliers usually carry out product development ad hoc and often undocumented (or not fully documented).</p> <p>Maturity Level 2 - Managed: The product supplier is able to manage the development of a product according to written guidelines. It must be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. The processes are repeatable.</p> <p>Maturity Level 3 - Defined (practiced): The process is repeatable throughout the supplier's organisation. The processes have been practiced and there is evidence that this has been done.</p> <p>Maturity Level 4 - Improving: Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.</p> <p>Security Level</p> <p>Technical requirements for systems (IEC 62443-3-3) and products (IEC 62443-4-2) are evaluated in the standard by four so-called Security Levels (SL). The different levels indicate the resistance against different classes of attackers. The standard emphasizes that the levels should be evaluated per technical requirement (see IEC 62443-1-1) and are not suitable for the general classification of products.</p> <p>The levels are:</p>		<p>ISO/IEC 27070 and IEC 62443-3 standards.</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	<p>systems - Part 3-2: Security risk assessment for system design IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels IEC 62443-3-3:2013/COR1:2014, Corrigendum 1 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components IEC TS 62443-6-1 ED1, Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS</p>		<p>Security Level 0: No special requirement or protection required. Security Level 1: Protection against unintentional or accidental misuse. Security Level 2: Protection against intentional misuse by simple means with few resources, general skills and low motivation. Security Level 3: Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation. Security Level 4: Protection against intentional misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation. Concepts: The standard explains various basic principles that should be considered for all roles in all activities. Defense in Depth is a concept in which several levels of security (defense) are distributed throughout the system. The goal is to provide redundancy in case a security measure fails, or a vulnerability is exploited. Zones & Conduits: Zones divide a system into homogeneous zones by grouping the (logical or physical) assets with common security requirements. The security requirements are defined by Security Level (SL). The level required for a zone is determined by the risk analysis. Zones have boundaries that separate the elements inside the zone from those outside. Information moves within and between zones. Zones can be divided into sub-zones that define different security levels (Security Level) and thus enable defence-in-depth. Conduits group the elements that allow communication between two zones. They provide security functions that enable secure communication and allow the coexistence of zones with different security levels.</p>		

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	service providers (under development) IEC TS 62443-6-2 ED1 , Security evaluation methodology for IEC 62443 – Part 4-2: Technical security requirements for IACS components (under development)				
IEC/TC 65 , Industrial-process measurement, control and automation	IEC PAS 63088 , Smart manufacturing - Reference architecture model industry 4.0 (RAMI4.0)	published	IEC PAS 63088 describes a reference architecture model in the form of a cubic layer model, which shows technical objects (assets) in the form of layers, and allows them to be described, tracked over their entire lifetime (or “vita”) and assigned to technical and/or organisational hierarchies. It also describes the structure and function of Industry 4.0 components as essential parts of the virtual representation of assets.	Industrial process measurement and control, IoT, device integration	NXW has investigated the activities, in particular, IEC 62264-1:2013, IEC 61499-1:2012, and IEC PAS 63088:2017. The analysis has confirmed the validity of the current approach where RAMI 4.0 is adopted as a reference but not as a mandatory specification. ASI will promote IEC PAS 63088 that provides a reference model for EFPF as RAMI 4.0 is at the foundation of Industry 4.0 standardisation efforts. CNet will monitor the standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.
IEC/TC 65 , Industrial-process measurement,	IEC 63278-1 , Asset administration shell for industrial applications –	Under development	Part 1 of the IEC 63278 series defines the structure of the Asset Administration Shell in the scope of industrial applications and especially of Smart Manufacturing. This specification defines how to represent an asset of the real	Industrial process measurement and	

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
control and automation	Part 1: Administration shell structure PNW 65-915 ED1 , Asset Administration Shell for Industrial Applications - Part 2: Information meta model PNW 65-916 ED1 , Asset Administration Shell for Industrial Applications - Part 3: Security provisions for Asset Administration Shells		world in the information world by the Asset Administration Shell containing structures, properties and services.	control, IoT, device integration	
IEC/TC 65 , Industrial-process measurement, control and automation	IEC TR 63283-2 , Industrial-process measurement, control and automation – Smart Manufacturing – Part 2: Use cases	published	This part of the IEC 63278 series presents use cases.	Industrial process measurement and control, IoT, device integration	
IEC/TC 65 , Industrial-process measurement, control and automation	IEC TR 63283-3 , Industrial-process measurement, control and automation – Smart Manufacturing – Part 3: Challenges for Cybersecurity	published	This part of the IEC 63278 series deals with challenges for Cybersecurity in the context of smart manufacturing.	Industrial process measurement and control, IoT, device integration, security	
IEC/TC 65 , Industrial-process measurement, control and automation	IEC 63339 , Unified reference model for smart manufacturing	Under development	IEC 63339 specifies a unified reference model for smart manufacturing.	Industrial process measurement and control, IoT, device integration	
IEC/TC 65/SC 65B , Measurement	IEC 61131 , Programmable controllers	Published	Standard IEC 61131 is divided into several parts: Part 1: General information. It is the introductory chapter; it contains definitions of terms that are used in the subsequent	Industrial process measurement	

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
and control devices	Part 1: General information Part 2: Equipment requirements and tests Part 3: Programming languages Part 4: User guidelines (Technical Report) Part 5: Communications Part 6: Functional safety Part 7: Fuzzy control programming Part 8: Guidelines for the application and implementation of programming languages (Technical Report) Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI) Part 10: PLC open XML exchange format		parts of the standard and outlines the main functional properties and characteristics of PLCs. Part 2: Equipment requirements and tests - establishes the requirements and associated tests for programmable controllers and their peripherals. This standard prescribes: the normal service conditions and requirements (for example, requirements related with climatic conditions, transport and storage, electrical service, etc.); functional requirements (power supply & memory, digital and analog I/Os); functional type tests and verification (requirements and tests on environmental, vibration, drop, free fall, I/O, power ports, etc.) and electromagnetic compatibility (EMC) requirements and tests that programmable controllers must implement. This standard can serve as a basis in the evaluation of safety programmable controllers to IEC 61508. Part 3: Programming languages Part 4: User guidelines Part 5: Communications Part 6: Functional safety Part 7: Fuzzy control programming Part 8: Guidelines for the application and implementation of programming languages Part 9: Single-drop digital communication interface for small sensors and actuators (SDCI, marketed as IO-Link) Part 10: PLC open XML exchange format for the export and import of IEC 61131-3 projects	nt and control	
IEC/TC 65/SC 65B , Measurement and control devices	IEC 61499, Function blocks Part 1 : Architecture Part 2 : Software tool requirements Part 4 : Rules for compliance profiles	published	IEC 61499-1:2012 defines a generic architecture and presents guidelines for the use of function blocks in distributed industrial-process measurement and control systems (IPMCSs). This architecture is presented in terms of implementable reference models, textual syntax and graphical representations. The models given in this standard are intended to be generic, domain independent and extensible to the definition and use of function blocks in other standards or for particular applications or application domains.	Industrial process measurement and control, IoT, device integration	NXW has investigated the activities, in particular, IEC 62264-1:2013, IEC 61499-1:2012, and IEC PAS 63088:2017. No parts of the standard have been considered relevant for the company's products. CNet will monitor the standardisation activities on the device integration with IoT

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			<p>IEC 61499-2:2012 defines requirements for software tools to support the following systems engineering tasks enumerated in IEC 61499-1.</p> <p>IEC 61499-4:2013 defines rules for the development of compliance profiles, which specify the features of IEC 61499-1 and 61499-2 to be implemented in order to promote the following attributes of IEC 61499-based systems, devices and software tools.</p>		platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.
IEC/TC 65/SC 65E , Devices and integration in enterprise systems	<p>IEC 62714, Engineering data exchange format for use in industrial automation systems engineering - Automation Markup Language</p> <p>Part 1: Architecture and general requirements</p> <p>Part 2: Role class libraries</p> <p>Part 3: Geometry and kinematics</p> <p>Part 4: Logic</p>	published	<p>IEC 62714 is a solution for data exchange focusing on the domain of automation engineering. The data exchange format defined in the IEC 62714 series (Automation Markup Language, AML) is an XML schema based data format for plant engineering data. The goal of AML is to interconnect engineering tools in their different disciplines, e.g. mechanical plant engineering, electrical design, process engineering, process control engineering, HMI development, PLC programming, robot programming, etc.</p> <p>AML combines existing industry data formats that are designed for the storage and exchange of different aspects of engineering information. These data formats are used on an “as-is” basis within their own specifications and are not branched for AML needs.</p> <p>The core of AML is the top-level data format CAEX. CAEX is utilized to interconnect the different data formats. Therefore, AML has an inherent distributed document architecture.</p>	Industrial process measurement and control	C2K will adopt and harmonise the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K will do this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services.
IEC/TC 65/SC 65E , Devices and integration in enterprise systems	<p>IEC/TR 62541-1:2020, OPC Unified Architecture - Part 1: Overview and concepts</p> <p>IEC/TR 62541-2:2020, OPC Unified Architecture - Part 2: Security Model</p> <p>IEC 62541-3:2020, OPC Unified Architecture - Part 3: Address Space Model</p>	published	<p>IEC 62541-1:2020 presents the concepts and overview of the OPC Unified Architecture (OPC UA). Reading this document is helpful to understand the remaining parts of this multi-part document set. Each of the other parts of IEC 62451 is briefly explained along with a suggested reading order.</p> <p>Part 2 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification.</p>	Industrial process measurement and control, Multilayer applications	<p>NXW is investigating models and ontologies from OPC UA, in particular IEC 62541-5:2020 OPC Unified Architecture – Part 5: Information Model at the border between building and factory concepts. NXW is evaluating as well the addition of OPC-UA to its factory connector for machine-to-machine communication.</p> <p>ICE is investigating the OPC-UA standard, in particular on how it will be used by the new</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	IEC 62541-4:2020 , OPC Unified Architecture - Part 4: Services IEC 62541-5:2020 , OPC Unified Architecture - Part 5: Information Model IEC 62541-6:2020 , OPC Unified Architecture - Part 6: Mappings IEC 62541-7:2020 , OPC Unified Architecture - Part 7: Profiles IEC 62541-8:2020 , OPC Unified Architecture - Part 8: Data Access IEC 62541-9:2020 , OPC Unified Architecture - Part 9: Alarms and conditions IEC 62541-10:2020 , OPC Unified Architecture - Part 10: Programs IEC 62541-11:2020 , OPC Unified Architecture - Part 11: Historical Access IEC 62541-12:2020 , OPC Unified Architecture - Part 12: Discovery and global services IEC 62541-13:2020 , OPC Unified Architecture - Part 13: Aggregates IEC 62541-14:2020 , OPC Unified Architecture - Part 14: PubSub IEC 62541-100:2015 , OPC Unified Architecture		<p>Part 3 defines the OPC Unified Architecture (OPC UA) AddressSpace and its Objects. This document is the OPC UA meta model on which OPC UA information models are based.</p> <p>Part 4 defines the OPC Unified Architecture (OPC UA) Services. The Services defined are the collection of abstract Remote Procedure Calls (RPC) that are implemented by OPC UA Servers and called by OPC UA Clients. All interactions between OPC UA Clients and Servers occur via these Services. The defined Services are considered abstract because no particular RPC mechanism for implementation is defined in this document.</p> <p>Part 5 defines the Information Model of the OPC Unified Architecture. The Information Model describes standardized Nodes of a Server's AddressSpace. These Nodes are standardized types as well as standardized instances used for diagnostics or as entry points to server-specific Nodes.</p> <p>Part 6 specifies the OPC Unified Architecture (OPC UA) mapping between the security model described in IEC TR 62541-2, the abstract service definitions specified in IEC 62541-4, the data structures defined in IEC 62541-5 and the physical network protocols that can be used to implement the OPC UA specification.</p> <p>Part 7 defines the OPC Unified Architecture (OPC UA) Profiles. The Profiles in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs.</p> <p>Part 8 is part of the overall OPC Unified Architecture (OPC UA) standard series and defines the information model associated with Data Access (DA). It particularly includes additional VariableTypes and complementary descriptions of the NodeClasses and Attributes needed for Data Access, additional Properties, and other information and behaviour.</p> <p>Part 9 specifies the representation of Alarms and Conditions in the OPC Unified Architecture. Included is the Information</p>		<p>Administration Shell standard. ICE Workflow Platform WASP (T4.6) is being tuned to support OPC UA based communication in workflows/processes that are designed to link multiple shop-floor assets. ICE has studied the support for OPC-UA in its WASP tool for enabling direct reading from factory PLC's and sensors. The intention is to use sensor data in conditional gateways for dynamic process execution flows. ICE is also studying OPC-UA in the context of the ICE Anomaly Detection tool to increase the number of communication protocols supported by the tool.</p> <p>FOR is following OPC FLC (Field Level Communications), ensuring alignment of requirements in this context towards EFPF. In T4.1, the TSMATCH component (developed by FOR) supports an OPC UA interface towards other EFPF components.</p> <p>CNET is an OPC Foundation member and has started to promote the adoption of this standard in EFPF tasks (T3.5)</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	- Part 100: Device Interface		<p>Model representation of Alarms and Conditions in the OPC UA address space.</p> <p>Part 10 defines the information model associated with Programs in the OPC Unified Architecture. This includes the description of the NodeClasses, standard Properties, Methods and Events and associated behaviour and information for Programs.</p> <p>Part 11 is part of the OPC Unified Architecture standard series and defines the information model associated with Historical Access (HA). It particularly includes additional and complementary descriptions of the NodeClasses and Attributes needed for Historical Access, additional standard Properties, and other information and behaviour.</p> <p>Part 12 specifies how OPC Unified Architecture (OPC UA) Clients and Servers interact with DiscoveryServers when used in different scenarios. It specifies the requirements for the LocalDiscoveryServer, LocalDiscoveryServer-ME and GlobalDiscoveryServer.</p> <p>Part 13 is part of the overall OPC Unified Architecture specification series and defines the information model associated with Aggregates.</p> <p>Part 14 defines the OPC Unified Architecture (OPC UA) PubSub communication model. It defines an OPC UA publish subscribe pattern which complements the client server pattern defined by the Services in IEC 62541-4. PubSub allows the distribution of data and events from an OPC UA information source to interested observers inside a device network as well as in IT and analytics cloud systems.</p> <p>Part 100 is an extension of the overall OPC Unified Architecture standard series and defines the information model associated with Devices.</p>		
IEEE – Institute of Electrical and Electronics Engineers	IEEE 2413:2019 , Standard for an Architectural Framework for the Internet of Things (IoT)	published	An architecture framework description for the Internet of Things (IoT) which conforms to the international standard ISO/IEC/IEEE 42010:2011 is defined. The architecture framework description is motivated by concerns commonly shared by IoT system stakeholders across multiple domains (transportation, healthcare, Smart Grid, etc.). A conceptual basis for the notion of things in the IoT is provided and the	IoT	ICE is referencing IEEE 2413:2019 in its platform development initiatives and is investigating the standard as a means to provide support for IoT based communication in

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			shared concerns as a collection of architecture viewpoints is elaborated to form the body of the framework description.		<p>the workflows and processes of its WASP tool.</p> <p>CNet is promoting the uptake of this standard on IoT architecture in the development of Data Spine (T3.2). Monitoring this standard will also benefit CNet commercial activities in the area of IoT devices.</p> <p>FOR is monitoring the IEEE 2413, the standard references for Smart Cities (P2413.1). FOR has interest in the future developments of this specific part, to ensure standardisation alignment.</p> <p>CERTH will use the same approach (sensors, gateways, edge IT, real time data processing and cloud/data centre) as in COMPOSITION but processing levels can provide an interface for more upper level frameworks that integrate different IoT domains and adhere to the related standards such as the IEEE P2413 standard</p>
Internet Engineering Task Force (IETF)	RFC 6749 /ISSN: 2070-1721 - The OAuth 2.0 Authorisation Framework	published	The OAuth 2.0 authorisation framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849.	Security	<p>Based on the plan in D11.11, WASP has already implemented OpenID Connect (built on top of OAuth 2.0 as a security standard to enable Single Sign-On functionality in EFPF federation.</p> <p>ICE is also implementing OAuth 2.0 within its Anomaly Detection tool to support the</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
IPC-CFX (IPC 2-17 – Connected Factory Initiative Subcommittee)	Software tools for Connected Factory Exchange SDK Version 1.0.5			Application Development	integration with the EFPF security components. The identification of the standard provides an impetus to EFPF (T5.5) to align the relevant application development activities (through the SDK in T5.5) with the IPC-CFX standard. The associated open source “Software tools for Connected Factory Exchange SDK” (Version 1.0.5) will be relevant in this regard. Relevant EFPF partners (e.g. CMS) will also investigate joining the IPC-CFX movement in order to contribute towards the further enhancement/ development of the standard e.g. for the manufacturing applications to be developed in the EFPF project. CMS is the leader of the Connected Factory SDK group (WG-DA-05) and is developing activities towards creating requirements and a common vision for a standard, innovative and reusable SDK to be adopted by the European projects, particularly in the manufacturing area. CMS will continue working towards the standardisation of an SDK and towards the alignment of its current SDK to the new vision and suite of tools.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO Workshop	IWA 39:2022 , Gap analysis for standardisation on sustainable and human-centered societies enabled with cyber physical systems	published	<p>The main purpose of this International Workshop is to discuss and agree between relevant TC/SCs and other stakeholders on what kind of new filed of activities to be addressed and how to deal with those in the field of the integration of Cyber Physical Systems (CPS) and sustainable and human-centered societal systems. The proposed IWA starts with identification of issues, then conducts gap analysis between existing works and standardisation needs, and finally agrees on future possible areas of standards to complement the gap.</p> <p>The goal of this International Workshop Agreement (IWA) is to make a discussion on "The Gap Analysis for Standardisation on Sustainable and Human-centered Societies Enabled with Cyber Physical Systems" and to report the results including gaps identified and future possible areas of standards to complement the gap.</p>	Human	SRFG will observe the work on this topic.
ISO/IEC JTC 1 , Information Technology	ISO/IEC 19464:2014 , Information technology -- Advanced Message Queuing Protocol (AMQP)	published	ISO/IEC 19464:2014 defines the Advanced Message Queuing Protocol (AMQP), an open internet protocol for business messaging. It defines a binary wire-level protocol that allows for the reliable exchange of business messages between two parties. AMQP has a layered architecture and the specification is organized as a set of parts that reflects that architecture.	Application layer	<p>AMQP, MQTT and JSON are essential standards for the application integration and the building blocks of the EFPF Data Spine and the platform. The uptake, interoperability and/or alignment of these standards will be carried out in the tasks dealing with message exchange in EFPF (T3.2 - Data Spine).</p> <p>CERTH considers protocols such as ISO/IEC 19464:2014, ISO/IEC 20922:2016 and ISO/IEC 21778:2017 for the design of its components and its communication with other tools and services.</p> <p>ICE has considered ISO/IEC 19464:2014 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					<p>to the standard will take place in T6.2 to ensure the secure transport of messages to the EFPF Message Bus via AMQP.</p> <p>ICE has implemented ISO/IEC 19464:2014 within in its anomaly detection, data analytics solution for the design of the component and its communication with Message Brokers.</p>
<p>ISO/IEC JTC 1, Information Technology</p>	<p>ISO/IEC 20922:2016, Information technology -- Message Queuing Telemetry Transport (MQTT)</p>	<p>published</p>	<p>ISO/IEC 20922:2016 is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.</p> <p>The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include:</p> <ul style="list-style-type: none"> • Use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications. • A messaging transport that is agnostic to the content of the payload. • Three qualities of service for message delivery: • "At most once", where messages are delivered according to the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after. • "At least once", where messages are assured to arrive but duplicates can occur. 	<p>Application layer</p>	<p>AMQP, MQTT and JSON are essential standards for the application integration and the building blocks of the EFPF Data Spine and the platform. The uptake, interoperability and/or alignment of these standards will be carried out in the tasks dealing with message exchange in EFPF (T3.2 - Data Spine).</p> <p>CNet will monitor the activities related to MQTT (ISO/IEC 20922:2016) due to its importance in the development of Data Spine (T3.2) and CNet's IoT applications.</p> <p>In the context of T4.1 and T3.2, FOR continues the integration of MQTT and addressing interoperability issues towards other protocols, e.g., OPC-UA, CoAP. FOR is monitoring activities concerning MQTT (ISO/IEC 20922:2016) and its industrial counterpart, MQTT</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			<ul style="list-style-type: none"> "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges eing applied. 		<p>Sparkplug, in regard to the TSMATCH and IIoT applications (T4.1), provided a publication (white paper²) and the evolutionary aspects concerning MQTT Sparkplug.</p> <p>CERTH considers protocols such as ISO/IEC 19464:2014, ISO/IEC 20922:2016 and ISO/IEC 21778:2017 for the design of its components and its communication with other tools and services.</p> <p>ICE has considered ISO/IEC 20922:2016 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment to the standard will take place in T6.2 to ensure the secure transport of messages to the EFPF Message Bus via MQTT.</p> <p>ICE has implemented ISO/IEC 20922:2016 within in its anomaly detection, data analytics solution for the design of the component and its communication with other Message Brokers.</p>
ISO/IEC JTC 1, Information Technology	ISO/IEC 21778:2017, Information technology -	published	JSON is a lightweight, text-based, language-independent syntax for defining data interchange formats. It was derived from the ECMAScript programming language but is	Languages used in	AMQP, MQTT and JSON are essential standards for the application integration and the

² See https://www.researchgate.net/publication/358618553_White_Paper_Applying_MQTT_Sparkplug_in_the_EFPF_Platform

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	The JSON data interchange syntax		<p>programming language independent. JSON defines a small set of structuring rules for the portable representation of structured data.</p> <p>The goal of ISO/IEC 21778:2017 is only to define the syntax of valid JSON texts. Its intent is not to provide any semantics or interpretation of text conforming to that syntax. It also intentionally does not define how a valid JSON text might be internalized into the data structures of a programming language. There are many possible semantics that could be applied to the JSON syntax and many ways that a JSON text can be processed or mapped by a programming language. Meaningful interchange of information using JSON requires agreement among the involved parties on the specific semantics to be applied. Defining specific semantic interpretations of JSON is potentially a topic for other specifications. Similarly, language mappings of JSON can also be independently specified. For example, ECMA-262 defines mappings between valid JSON texts and ECMAScript's runtime data structures.</p>	information technology	<p>building blocks of the EFPF Data Spine and the platform. The uptake, interoperability and/or alignment of these standards will be carried out in the tasks dealing with message exchange in EFPF (T3.2 - Data Spine).</p> <p>CERTH considers protocols such as ISO/IEC 19464:2014, ISO/IEC 20922:2016 and ISO/IEC 21778:2017 for the design of its components and its communication with other tools and services.</p> <p>ICE has considered ISO/IEC 21778:2017 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment to the standard will take place in T6.2 to support the communication between service components and external tools and services. This standard has also been implemented by ICE's WASP tool for the design of marketplace services and REST communication between internal components and external EFPF tools and services.</p> <p>ICE has implemented ISO/IEC 21778:2016 within in its anomaly detection, data analytics solution for the design of the component and its communication with</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					Message Brokers where data from devices can be pushed.
ISO/IEC JTC 1, Information Technology	ISO/IEC 19845:2015 , Information technology - Universal Business Language Version 2.1 (UBL v2.2)	published	<p>ISO/IEC 19845:2015 specifies the OASIS Universal Business Language (UBL), which defines a generic XML interchange format for business documents that can be restricted or extended to meet the requirements of particular industries. Specifically, UBL provides the following:</p> <ul style="list-style-type: none"> • A suite of structured business objects and their associated semantics expressed as reusable data components and common business documents. • A library of XML schemas for reusable data components such as "Address", "Item", and "Payment", the common data elements of everyday business documents. • A set of XML schemas for common business documents such as "Order", "Despatch Advice", and "Invoice" that are constructed from the UBL library components and can be used in generic procurement and transportation contexts. 	Languages used in information technology	<p>Considering the cross-platform data model, EFPF platform sees the UBL v2.2 (or v2.3) as a candidate. In the NIMBLE project, the UBL v2.1 version of the standard is used. In the scope of EFPF, the data model of NIMBLE will be upgraded to v2.2, or v2.3 that is expected in December 2019. In the scope of EFPF standardisation activities, SRDC will submit additional user requirements and/or user usage scenarios to the UBL community in order to contribute to UBL 2.3</p> <p>ICE's WASP tool has been enabled to communicate with external process applications that use UBL. ICE is investigating and testing the use of UBL in the WASP platform to work towards the closed integration with UBL with an aim to ensure a closer interface with the BPMN2.0 standard.</p>
ISO/IEC JTC 1, Information Technology	ISO/IEC 30118-1:2018 , Information technology - Open Connectivity Foundation (OCF) Specification - Part 1: Core specification	published	<p>The OCF specifications are divided into two sets of documents:</p> <ul style="list-style-type: none"> • Core Specification documents: The Core Specification documents specify the Framework, i.e., the OCF core architecture, interfaces, protocols and services to enable OCF profiles implementation for Internet of Things (IoT) usages and ecosystems. • Vertical Profiles Specification documents: The Vertical Profiles Specification documents specify the OCF profiles 	Interface and interconnection equipment	

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			to enable IoT usages for different market segments such as smart home, industrial, healthcare, and automotive. The Application Profiles Specification is built upon the interfaces and network security of the OCF core architecture defined in the Core Specification.		
ISO/IEC JTC 1 , Information Technology	ISO/IEC 19510:2013 , Information technology – Object Management Group Business Process Model and Notation	Published	The primary goal of ISO/IEC 19510:2013 is to provide a notation that is readily understandable by all business users, from the business analysts that create the initial drafts of the processes, to the technical developers responsible for implementing the technology that will perform those processes, and finally, to the business people who will manage and monitor those processes. Thus, ISO/IEC 19510:2013 creates a standardized bridge for the gap between the business process design and process implementation and represents the amalgamation of best practices within the business modelling community to define the notation and semantics of Collaboration diagrams, Process diagrams, and Choreography diagrams. ISO/IEC 19510:2013 is identical to OMG BPMN 2.0.1. See in addition: Object Management Group – Business Process Management Initiative	Process	ICE has adopted BPMN 2.0 as a modelling notation for workflows. ICE will continue monitoring the BPMN 2.0 standard. ICE's WASP is using BPMN for designing processes and monitoring their execution. ICE has now extended the use of BPMN in the WASP tool, implementing listeners that include functionality to generate and execute custom code.
ISO/IEC JTC 1/SC 07 , Software and systems engineering	ISO/IEC TS 33052:2016 , Information technology - Process reference model (PRM) for information security management	published	ISO/IEC TS 33052:2016 defines a process reference model (PRM) for the domain of information security management. The model architecture specifies a process architecture for the domain and comprises a set of processes, with each described in terms of process purpose and outcomes.	Security	ICE will investigate this standard and promote its adoption for the development of security reference models (in T6.2)
ISO/IEC JTC 1/SC 07 , Software and systems engineering	ISO/IEC/IEEE 42010:2022 , Software, systems and enterprise — Architecture description	published	This document specifies requirements on the structure and expression of architecture descriptions (ADs) for various entities, including software, systems, enterprises, systems of systems, families of systems, products (goods or services), product lines, service lines, technology, and business domains. In this document, the term entity of interest refers to the entity whose architecture is under consideration in the preparation of an architecture description (AD).	Architecture	
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity	ISO/IEC 27000:2018 , Information technology -- Security techniques -- Information security	published	ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
and privacy protection	management systems -- Overview and vocabulary		of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).		
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27001:2013 , Information technology -- Security techniques -- Information security management systems -- Requirements	published	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27002:2013 , Information technology -- Security techniques -- Code of practice for information security controls	published	ISO/IEC 27002:2013 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27005:2011 , Information Technology -- Security Techniques -- Information Security Risk Management	published	This document provides guidelines for information security risk management. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27009:2020 , Information technology -- Security techniques -- Sector-specific application of ISO/IEC 27001 – Requirements	published	This document specifies the requirements for creating sector-specific standards that extend ISO/IEC 27001, and complement or amend ISO/IEC 27002 to support a specific sector (domain, application area or market).	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security,	ISO/IEC 27017:2015 , Information technology — Security techniques — Code of practice for	published	ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services.	Security, Cloud	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF. SRFG

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
cybersecurity and privacy protection	information security controls based on ISO/IEC 27002 for cloud services				is also interested in contributing to cloud security standards, e.g. ISO/IEC 27017:2015.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27032 , Information Technology — Cybersecurity — Guidelines for Internet Security	Under development	This document provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: <ul style="list-style-type: none"> • information security, • network security, • internet security, and • critical information infrastructure protection (CIIP). 	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 27070:2021 , Information technology — Security techniques — Requirements for establishing virtualized roots of trust	published	This document specifies functional requirements and security requirements for establishment and operation of virtualized Root of Trusts (RoTs). The development of this standard also provides a reference for applying the trusted computing technology in the cloud computing environment. The goal of the document is to provide a unified approach to virtualize RoTs based on hardware trusted modules.	Security	CERTH will use IDS Trusted Connector for secure connectivity of fill level sensors of industrial open top containers. This type of connectors following the ISO/IEC 27070 and IEC 62443-3 standards
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 15408-1:2009 , Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC 15408-2:2008 , Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components ISO/IEC 15408-3:2008 , Information technology — Security techniques — Evaluation criteria for IT	published	ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described.	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	security — Part 3: Security assurance components		<p>ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organisation of components throughout the model.</p> <p>ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes.</p> <p>ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.</p> <p>ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.</p> <p>ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organisation of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.</p>		
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 18033-3:2010 , Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers	published	<p>ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality. ISO/IEC 18033-3:2010 specifies block ciphers. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. ISO/IEC 18033-3:2010 specifies following algorithms:</p> <ul style="list-style-type: none"> 64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT; 128-bit block ciphers: AES, Camellia, SEED. 	Security, Encryption	ICE's Pub Sub Security Service has considered and implemented the Sparkplug specification to provide a framework for the standardised definition of topics in the EFPF Message Bus.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC TS 27100:2020 , Information technology -- Cybersecurity -- Overview and concepts	published	This document <ul style="list-style-type: none"> • provides an overview of cybersecurity. • describes cybersecurity and relevant concepts, including how it is related to and different from information security; • establishes the context of cybersecurity; • does not cover all terms and definitions applicable to cybersecurity. 	Security	SRFG considers the set of Information Security standards for the design of security controls (T6.2) in EFPF.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC 24392 , Information technology -- Security techniques -- Security reference model for Industrial Internet Platform (IIP)	Under development	This International Standard defines a Security Reference Model for Industrial Internet Platform (SRMIIP), which is to be established based on analysis of security risks and threats related to various types of industrial internet platforms. The reference model guides either construction of secure IIPs or security improvement over existing IIPs	Security	SRFG will analyse ISO/IEC 24392 which is in an early stage of development.
ISO/IEC JTC 1/SC 27 , Information security, cybersecurity and privacy protection	ISO/IEC PWI TS 5689, Cybersecurity -- Security frameworks based on the conceptual model of cyber-physical systems	Under development	This document provides the followings: CPS conceptual model – a conceptual model of cyber-physical systems (CPS) and its general features. Concerns and security frameworks – security concerns, which serves as the basis for the discussion of security risks and security controls for the CPS based on the conceptual model – several security frameworks to overcome those security concerns.	Security	
ISO/IEC JTC 1/SC 32 , Data management and interchange	ISO/IEC 6523-1 , Information technology — Structure for the identification of organisations and organisation parts — Part 1: Identification of organisation identification schemes ISO/IEC 6523-2 , Information technology — Structure for the identification of organisations and organisation parts — Part	Under development	Part 1 of ISO/IEC 6523 specifies a structure for globally and unambiguously identifying organisations, and parts thereof, for the purpose of information interchange. This part of ISO/IEC 6523 also makes recommendations regarding cases where prior agreements may be concluded between interchange partners. This part of ISO/IEC 6523 does not specify file organisation techniques, storage media, languages, etc. to be used in its implementation. Part 2 of ISO/IEC 6523 specifies the procedure for registration of organisation identification schemes, and the requirements for the administration of International Code Designator values, to designate these organisation identification schemes.	Data management	EFPF partners (SRFG, CERTH, VLC, C2K) have investigated the standard that provides information on how to identify organisations and organisational parts in data interchange. EFPF tasks on matchmaking (T4.5) and marketplace framework (T3.3) are currently analysing the use of this standard at company registration phase or when exchanging business messages. Some implications

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	2: Registration of organisation identification schemes				on domain specific aspects are being investigated VLC along with other partners is actively investigating the use of these standards for data sharing between platforms. The approach for Business and Networking Intelligence follows the matchmaking task which uses a combination of standard including the ones mentioned here and others such as eClass and UBL.
ISO/IEC JTC 1/SC 38 , Cloud Computing and Distributed Platforms	ISO/IEC 17788:2014 , Information technology -- Cloud computing -- Overview and vocabulary	published	ISO/IEC 17788:2014 provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards.	Cloud computing	The standard provides a comprehensive vocabulary that is relevant to all types of organisations. There is little potential to further enhance this standard and therefore the activities in EFPF project will focus on the use of this standard terminologies across project documents and dissemination channels. FOR is actively involved in the development of the GAIA-X initiative to strengthen Europe's data infrastructure.
ISO/IEC/JTC 1/SC 40 , IT service management and IT governance	ISO/IEC 38500:2015 , Information technology -- Governance of IT for the organisation	published	ISO/IEC 38500:2015 provides guiding principles for members of governing bodies of organisations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organisations. ISO/IEC 38500:2015 applies to the governance of the organisation's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organisation, external service providers, or business units within the organisation.	IT service management, IT governance	SRFG implements the ISO/IEC 38500 and assures that the data accountability map and associated matrix of considerations from ISO/IEC 38505-1 are fully adopted in EFPF. The data governing principles in EFPF are implemented according to the IT governance methods presented in these standards.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO/IEC/JTC 1/SC 40 , IT service management and IT governance	ISO/IEC 38505-1:2017 , Information technology -- Governance of IT -- Governance of data -- Part 1: Application of ISO/IEC 38500 to the governance of data ISO/IEC TR 38505-2:2018 , Information technology — Governance of IT — Governance of data — Part 2: Implications of ISO/IEC 38505-1 for data management	published	ISO/IEC 38505-1:2017 provides guiding principles for members of governing bodies of organisations on the effective, efficient, and acceptable use of data within their organisations. ISO/IEC 38505-1:2017 applies to the governance of the current and future use of data that is created, collected, stored or controlled by IT systems, and impacts the management processes and decisions relating to data. ISO/IEC TR 38505-2 provides guidance to the members of governing bodies of organisations and their executive managers on the implications of ISO/IEC 38505-1 for data management. It assumes understanding of the principles of ISO/IEC 38500 and familiarisation with the data accountability map and associated matrix of considerations, as presented in ISO/IEC 38505-1.	IT service management, IT governance	SRFG implements the ISO/IEC 38500 and assures that the data accountability map and associated matrix of considerations from ISO/IEC 38505-1 are fully adopted in EFPF. The data governing principles in EFPF are implemented according to the IT governance methods presented in these standards.
ISO/IEC/JTC 1/SC 40 , IT service management and IT governance	ISO/IEC 38506:2020 , Information technology -- Governance of IT -- Application of ISO/IEC 38500 to the governance of IT enabled investments	published	This document provides guidance on governance of IT enabled investments to the governing body of all forms of organisations, whether private, public or government entities, and will equally apply regardless of the size of the organisation or its industry or sector. This document also provides guidance that can be applied in the due diligence process related to business acquisitions. This document may provide guidance on the application of the principles documented in ISO/IEC 38500 for ranking IT enabled investments including assessing the value and risks of IT elements in the context of investment banking or as performed by investment companies.	IT service management, IT governance	
ISO/IEC/JTC 1/SC 40 , IT service management and IT governance	ISO/IEC TS 38508 , Information Technology -- Governance of IT -- Governance Implications of the Use of Shared Digital Service Platform among Ecosystem Organisations	under development	This TS aims to provide guidance to the governing bodies of organisations that are accountable for their organisation's use of 'shared digital service platform'. Thus, this standard focuses on governance and not on the technologies themselves. This only covers 'shared digital service platform' to the extent that is necessary to understand the governance implications of their use. This TS develops guidelines on how existing companies can build shared digital service platforms or participate in platform-based digital eco-system usually developed by large companies to spearhead their digital transformations. Although platform strategy can open-up new opportunities, there are	IT service management, IT governance	

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
			also risks, limitations and important responsibilities for organisations.		
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 21823-1:2019 , Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework ISO/IEC 21823-2:2020 , Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability	published	ISO/IEC 21823-1:2019 provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a common understanding of interoperability as it applies to IoT systems and the various entities within them. ISO/IEC 21823-2:2020 specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies: transport interoperability interfaces and requirements between IoT systems; transport interoperability interfaces and requirements within an IoT system	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 21823, even though there are currently no plans to adopt it, it will still be monitored in the future. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30141:2018 , Internet of Things (IoT) -- Reference Architecture	published	This document 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, deriving a high level system based reference with subsequent dissection of that model into five architecture views from different perspectives.	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30141, even though there are currently no plans to adopt it, it will still be monitored in the future. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 ,	ISO/IEC 30144:2020 , Information technology --	published	This document specifies intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure	IoT	NXW has reported internally about the activities of

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
Internet of things and digital twin	Sensor network system architecture for power substations		and communications internal and external to the infrastructure, and technical requirements for iWSN to realize smart electrical power substations.		ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30144, there are currently no plans to adopt it. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30147:2021 , Information technology -- Internet of things -- Methodology for trustworthiness of IoT system/service	published	ISO/IEC 30147: provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015. The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30147, there are currently no plans to adopt it. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30149 , Internet of things (IoT) -- Trustworthiness framework	under development	ISO/IEC 30149 provides principles for IoT trustworthiness based on ISO/IEC 30141 – IoT Reference Architecture.	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30149, there are currently no plans to adopt it. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					<p>interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).</p> <p>SRFG monitors the ongoing development of the Trustworthiness framework in the ISO/IEC NP 30149 - Internet of things (IoT). A possible cooperation with the ISO/IEC JTC 1/SC 41 will be investigated in the context of the EFPF task related to trust (T5.3)</p>
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30161:2020 - Internet of Things (IoT) -- Requirements of IoT data exchange platform for various IoT services	published	ISO/IEC 30161-1 specifies requirements for an Internet of Things (IoT) data exchange platform for various services in the technology areas of: the middleware components of communication networks allowing the co-existence of IoT services with legacy services; the end-points performance across the communication networks among the IoT and legacy services; the IoT specific functions and functionalities allowing the efficient deployment of IoT services; the IoT service communication networks framework and infrastructure; and the IoT service implementation guideline for the IoT data exchange platform	IoT	<p>NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30161, even though there are currently no plans to adopt it, it will still be monitored in the future.</p> <p>CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).</p>
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30162:2021 , Internet of Things (IoT) -- Compatibility requirements and model for devices within industrial IoT systems	published	ISO/IEC 30162:2021 specifies network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of a) data transmission protocols interaction; b) distributed data interoperability & management; c) connectivity framework; d) connectivity transport; e) connectivity network; and f) best practices and guidance to use in IIoT area.	IoT	<p>NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30162, even though there are currently no plans to adopt it, it will still be monitored in the future.</p> <p>CNet has monitored the standardisation activities in the</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30163:2021 , Internet of Things (IoT) -- System requirements of IoT/SN technology-based integrated platform for chattel asset monitoring supporting financial services	published	ISO/IEC 30163 specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including: - System infrastructure that describes functional components; - System and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.; - Performance requirements and performance specifications of each functional component; - Interface definition of the integrated platform system. This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30163, there are currently no plans to adopt it. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC TR 30164:2020 , Internet of things (IoT) -- Edge Computing	published	ISO/IEC TR 30164:2020 describes the common concepts, terminologies, characteristics, use cases and technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware/software optimisation) of edge computing for IoT systems applications. This document is also meant to assist in the identification of potential areas for standardisation in edge computing for IoT.	IoT, Edge computing	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30164, even though there are currently no plans to adopt it, it will still be monitored in the future. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30165:2021 , Internet of Things (IoT) -- Real-time IoT framework	published	ISO/IEC 30165 specifies the framework of a real-time IoT (RT-IoT) system, including RT-IoT system conceptual model based on domain-based IoT reference model defined in ISO/IEC 30141; impacts of time-parameter in terms of four viewpoints (time, communication, control and computation).	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30165, there are currently no plans to adopt it. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC TS 30168 , Internet of Things (IoT) – Generic Trust Anchor Application Programming Interface for Industrial IoT Devices	Under development	ISO/IEC TS 30168 specifies a generic programming interface for the integration of secure elements within Industrial IoT devices. This includes requirements from industrial usage scenarios and applications. This document also provides guidance for implementation, testing, and conformity validation.	IoT	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30168, even though there are currently no plans to adopt it, it will still be monitored in the future. CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30172 , Digital twin - Use cases	Under development	This document provides a collection of representative use cases of DT applications in a variety of domains.	IoT, Digital twin	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30172, even though there are currently no plans to adopt it, it will still be monitored in the future.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	ISO/IEC 30173 , Digital twin - Concepts and terminology	Under development	This document establishes terminology for Digital Twin and describes concepts in the field of Digital Twin, including the terms and definitions of Digital Twin, concepts of Digital Twin (e.g., Digital Twin ecosystem, lifecycle process for Digital Twin, and classifications of Digital Twin), Functional view of Digital Twin and Digital Twin stakeholders. This document can be used in the development of other standards and in support of communications among diverse, interested parties/stakeholders.	IoT, Digital twin	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 30173, even though there are currently no plans to adopt it, it will still be monitored in the future.
ISO/IEC/JTC 1/SC 41 , Internet of things and digital twin	PWI JTC1-SC41-5 , Digital Twin - Reference Architecture	Under development	This document provides a standardized generic Digital Twin (DT) 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 DT along its life cycle, abstracting those into a generic DT Conceptual Model, deriving a high-level system-based reference with subsequent dissection of that model into five architecture views from different perspectives.	IoT, Digital twin	NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards PWI JTC1-SC41-5, even though there are currently no plans to adopt it, it will still be monitored in the future.
ISO/IEC JTC 1/SC 42 , Artificial intelligence	ISO/IEC 23053 , Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	published	This document establishes an Artificial Intelligence (AI) and Machine Learning (ML) framework for describing a generic AI system using ML technology. The framework describes the system components and their functions in the AI ecosystem.	Artificial Intelligence	ICE plans to follow the framework to provide a comprehensive functionality of AI/ML systems in its Anomaly Detection Component
ISO/IEC JTC 1/SC 42 , Artificial intelligence	ISO/IEC TR 24372 , Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems	published	This document provides an overview of the state of the art of computational approaches for AI systems, by describing a) main computational characteristics of AI systems; b) main algorithms and approaches used in AI systems, referencing use cases contained in ISO IEC TR 24030.	Artificial Intelligence	ICE plans to study this standard to identify the state of the art computational approaches that are applicable to anomaly detection and how to add new algorithms in its Anomaly Detection Component ML powered systems
ISO/TC 184 , Automation systems and integration	IEC 63339 , Unified reference model for smart manufacturing	Under development	Developed in ISO/TC 184/JWG 21, Joint ISO/TC 184 - IEC/TC 65/JWG 21 - Smart Manufacturing Reference Model(s) linked to ISO/TC 184	Industrial process measurement and control, IoT, device integration	CNet will monitor the standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					Data Spine with latest standards on IoT integration.
ISO/TC 184 , Automation systems and integration	IEC/TR 63319 , A meta-modelling analysis approach to smart manufacturing reference models	Under development	Developed in ISO/TC 184/JWG 21, Joint ISO/TC 184 - IEC/TC 65/JWG 21 - Smart Manufacturing Reference Model(s) linked to ISO/TC 184	Industrial process measurement and control, IoT, device integration	CNet will monitor the standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.
ISO/TC 184/SC 4 , Industrial data	ISO 10303-236:2006 , Industrial automation systems and integration - Product data representation and exchange - Part 236: Application protocol: Furniture catalogue and interior design - and Application modules	published	ISO 10303-236:2006 specifies the use of ISO 10303 integrated resources necessary for the scope and information requirements for furniture catalogue and interior design. Catalogue data information, product shape representation, parameterized catalogue data information and furniture interior design are within the scope of ISO 10303-236:2006.	Product Catalogue, Industrial process measurement and control	C2K will adopt and harmonise the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K will do this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services. CNet will study the activities on Product Data representations which are relevant to CNet's commercial activities related to the equipment manufacturing.
ISO/TC 184/SC 4 , Industrial data	ISO 20534:2018 , Industrial automation systems and integration - Formal semantic models for the configuration of global production networks	published	This document specifies a formal logic-based concept specialisation approach to support the development of manufacturing reference models that underpin the necessary business specific knowledge models needed to support the configuration of global production networks.	Industrial process measurement and control	C2K will adopt and harmonise the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K will do this by considering the format of data at all levels of the automation model and how this will support interoperability

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					for the platform tools and services. CNet will study the activities on Product Data representations which are relevant to CNet's commercial activities related to the equipment manufacturing.
ISO/TC 184/SC 4 , Industrial data	ISO 23247:2021, Automation systems and integration — Digital Twin manufacturing framework Part 1 : Overview and general principles Part 2 : Reference architecture Part 3 : Digital representation of manufacturing elements Part 4 : Information exchange	Published	The ISO 23247 series defines a framework to support the creation of Digital Twins of observable manufacturing elements including personnel, equipment, materials, manufacturing processes, facilities, environment, products, and supporting documents. The scopes of the four parts of this series are defined below: — Part 1: Overview and general principles - General principles and requirements for developing Digital Twins in manufacturing; — Part 2: Reference architecture - Reference architecture with functional views; — Part 3: Digital representation of manufacturing elements - List of basic information attributes for the observable manufacturing elements; — Part 4: Information exchange - Technical requirements for information exchange between entities within the reference architecture.	Industrial process measurement and control, digital twin	CNet will study the activities on Digital Twin standardisations which are relevant to CNet's commercial activities related to the equipment manufacturing.
ISO/TC 184/SC 4 , Industrial data	ISO 23952:2020 , Automation systems and integration — Quality information framework (QIF) — An integrated model for manufacturing quality information	published	This document describes the general content and structure of the entire QIF information model. It describes the highest level data structures of QIF, that are expanded in Clauses 6 through 12 using data dictionaries and XML schema files. All QIF XML schema files can be found at www.qifstandards.org .	Industrial process measurement and control	
ISO/TC 184/SC 5 , Interoperability, integration, and architectures for enterprise	IEC 62264, Enterprise-control system integration Part 1 : Models and terminology	published	This multi-part standard was jointly developed with IEC SC 65E , Devices and integration in enterprise systems. IEC 62264-1 describes the manufacturing operations management domain (Level 3) and its activities, and the interface content and associated transactions within Level 3 and between Level 3 and Level 4. This description enables	Industrial process measurement and control, IoT,	C2K will adopt and harmonise the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K will do

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
systems and automation applications	<p>Part 2: Objects and attributes for enterprise-control system integration</p> <p>Part 3: Activity models of manufacturing operations management</p> <p>Part 4: Objects and attributes for manufacturing operations management integration</p> <p>Part 5: Business to manufacturing transactions</p>		<p>integration between the manufacturing operations and control domain (Levels 3, 2, 1) and the enterprise domain (Level 4). Its goals are to increase uniformity and consistency of interface terminology and reduce the risk, cost, and errors associated with implementing these interfaces.</p> <p>IEC 62264-2 specifies generic interface content exchanged between manufacturing control functions and other enterprise functions. The interface considered is between Level 3 manufacturing systems and Level 4 business systems in the hierarchical model defined in IEC 62264-1.</p> <p>IEC 62264-3 defines activity models of manufacturing operations management that enable enterprise system to control system integration. The activities defined in this document are consistent with the object models definitions given in IEC 62264-1. The modelled activities operate between business planning and logistics functions, defined as the Level 4 functions and the process control functions, defined as the Level 2 functions of IEC 62264-1.</p> <p>IEC 62264-4 defines object models and attributes exchanged between Level 3 manufacturing operations management activities defined in IEC 62264-3.</p> <p>IEC 62264-5 defines transactions in terms of information exchanges between applications performing business and manufacturing activities associated with Levels 3 and 4. The exchanges are intended to enable information collection, retrieval, transfer and storage in support of enterprise-control system integration.</p>	device integration	<p>this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services.</p> <p>CNet will monitor the standardisation activities on the device integration with IoT platforms. The analysis carried out will be used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.</p>
ISO/TC 184/SC 5 , Interoperability, integration, and architectures for enterprise systems and automation applications	<p>ISO 22549, Automation systems and integration — Assessment on convergence of informatisation and industrialisation for industrial enterprises</p> <p>Part 1: Framework and reference model</p>	published	<p>Part 1 defines the basic principles for an assessment concerning the convergence of informatisation and industrialisation (CII) in industrial enterprises, including the following:</p> <ul style="list-style-type: none"> — assessment framework definitions; — assessment reference model definitions; — assessment reference model components. <p>Part 2 defines the maturity model and the evaluation methodology on convergence of informatisation and</p>	Industrial process measurement and control, Enterprise Systems, Interoperability, Integration	

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
	Part 2 : Maturity model and evaluation methodology		industrialisation in industrial enterprises. The scope of this document includes the following: <ul style="list-style-type: none"> — maturity model definition; — principles of evaluation questionnaires; and — guidance for a maturity evaluation method. 		
ISO/TC 184/SC 5 , Interoperability, integration, and architectures for enterprise systems and automation applications	ISO 11354-1 , Advanced automation technologies and their applications -- Requirements for establishing manufacturing enterprise process interoperability -- Part 1: Framework for enterprise interoperability	published	The purpose of ISO 11354-1:2011 is to specify a Framework for Enterprise Interoperability (FEI) that establishes dimensions and viewpoints to address interoperability barriers, their potential solutions, and the relationships between them. ISO 11354 applies to manufacturing enterprises, but can also apply to other kinds of enterprises. It is intended for use by stakeholders who are concerned with developing and deploying solutions based on information and communication technology for manufacturing enterprise process interoperability. It focuses on, but is not restricted to, enterprise (manufacturing or service) interoperability.	Industrial process measurement and control, Enterprise Systems, Interoperability, Integration	Implemented in T4.4 (WG 1) / INTEROP Enterprise interoperability framework
ISO/TC 262 , Risk Management	ISO 31000:2018 , Risk management — Guidelines	published	ISO 31000:2018 provides guidelines on managing risk faced by organisations. The application of these guidelines can be customized to any organisation and its context. ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific.	risk	Although a working group has been setup by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to focus on the Risk Management topic, there is no current activity in this area. This represents an opportunity for EFPF (particularly the partners involved in the development of Risk Management Tool in T4.4) to support and collaborate with BSI towards the development of standards in this area. One area of interest for EFPF will be to facilitate the exchange of knowledge between BSI and NIST's Risk Management Framework. ASI will facilitate

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					the investigation and collaborations in this area.
ISO/TC 262 , Risk Management	ISO/TR 31004:2013 , Risk management — Guidance for the implementation of ISO 31000	published	<p>ISO/TR 31004:2013 provides guidance for organisations on managing risk effectively by implementing ISO 31000:2009. It provides:</p> <ul style="list-style-type: none"> • a structured approach for organisations to transition their risk management arrangements in order to be consistent with ISO 31000, in a manner tailored to the characteristics of the organisation; • an explanation of the underlying concepts of ISO 31000; • guidance on aspects of the principles and risk management framework that are described in ISO 31000. 	risk	<p>Although a working group has been setup by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to focus on the Risk Management topic, there is no current activity in this area. This represents an opportunity for EFPF (particularly the partners involved in the development of Risk Management Tool in T4.4) to support and collaborate with BSI towards the development of standards in this area. One area of interest for EFPF will be to facilitate the exchange of knowledge between BSI and NIST's Risk Management Framework. ASI will facilitate the investigation and collaborations in this area.</p>
ISO/TC 307 , Blockchain and distributed ledger technologies	ISO 22739:2020 , Blockchain and distributed ledger technologies – Terminology	published	This document provides fundamental terminology for blockchain and distributed ledger technologies.	Block chain	CNET and CERTH will both monitor the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.
ISO/TC 307 , Blockchain and distributed ledger technologies	ISO/TR 23244:2020 , Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations	published	This document provides an overview of privacy and personally identifiable information (PII) protection as applied to blockchain and distributed ledger technologies (DLT) systems.	Block chain	CNET and CERTH will both monitor the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
ISO/TC 307 , Blockchain and distributed ledger technologies	ISO 23257 , Blockchain and distributed ledger technologies — Reference architecture	published	This document specifies a reference architecture for distributed ledger technology (DLT) systems including blockchain systems. The reference architecture addresses concepts, cross-cutting aspects, architectural considerations, and architecture views, including functional components, roles, activities, and their relationships for blockchain and DLT.	Block chain	CNET and CERTH will both monitor the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.
ISO/TC 307 , Blockchain and distributed ledger technologies	ISO/TS 23259 , Blockchain and distributed ledger technologies — Legally binding smart contracts	Under development	Project deleted	Block chain	CNET and CERTH will both monitor the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.
ISO/TC 307 , Blockchain and distributed ledger technologies	ISO/TR 23642 , Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues	Under development		Block chain	CNET and CERTH will both monitor the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.
Java Specification Request, JSR	JSR 268 - Java Portlet specification v2.0	published		Language	ICE's WASP has now implemented the standard Java portlet's as pluggable user interfaces. A portlet container runs the portlets with the run time environment.
Linux Foundation	OpenAPI Specification (OAS 3.0)	published	<p>The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. When properly defined, a consumer can understand and interact with the remote service with a minimal amount of implementation logic.</p> <p>An OpenAPI definition can then be used by documentation generation tools to display the API, code generation tools to generate servers and clients in various programming languages, testing tools, and many other use cases.</p>	RESTful API	<p>To build rest interface, to allow communication between, camunda, liferay, process designer, forms editor</p> <p>ICE's WASP has investigated and started to implement OAS 3.0 for the provision of the tools REST interface which will enable standardised communication between tool components such as camunda process engine, liferay, the process designer and forms editor.</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					ICE's Pub Sub Security Service has implemented OAS 3.0 to provide a rest interface for communication between backend and front-end components.
NIST	SP 800-53 Rev. 5: 2020, Security and Privacy Controls for Information Systems and Organisations	published	This publication provides a catalogue of security and privacy controls for information systems and organisations to protect organisational operations and assets, individuals, other organisations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organisation-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalogue addresses security and privacy from a functionality perspective and from an assurance perspective. Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.	cybersecurity; FISMA; privacy controls; Risk Management Framework; security controls; security requirements; system security	
OpenID Foundation	OpenID Connect	published	<p>OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorisation Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.</p> <p>OpenID Connect allows clients of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID Providers, and session management, when it makes sense for them.</p>	Security	<p>Based on the plan in D11.11, WASP has already implemented OpenID Connect (built on top of OAuth 2.0 as a security standard to enable Single Sign-On functionality in EFPF federation.</p> <p>ICE investigated the OpenID Connect standard as a means for authentication between RabbitMQ (Message Bus) and Keycloak (EFS). OpenID Connect proved insufficient for the use case, only providing support for a UAA server and not a Keycloak sever.</p>

Standardisation Body	Standard	Status	Scope	Keywords	EFPF Action
					ICE is also implementing OAuth 2.0 within its Anomaly Detection tool to support the integration with the EFPF security components.
ZVEI SG 'Models and Standards' and Platform Industry 4.0 working group WG1	RAMI4.0	published	Industry 4.0: Specification Details of the Asset Administration Shell	Industrial process measurement and control, IoT, device integration	

The overview of relevant standardisation activities and ongoing efforts in the EFPF project demonstrates that the project partners are following the initial plan presented in D11.11. In most cases progress has been reported by project partners either in terms of study of relevant standards or their adoption/implementation in the ongoing activities. This emphasis on standardisation is important to streamline the project activities with other/similar activities taking place in the digital manufacturing space. This is in addition to the joint CEN-CENELEC Workshop Agreement (CWA) activity being carried out in the Digital Manufacturing Platforms (DMP) Cluster – a collaborative initiative involving DT-ICT-07 projects, EFFRA and OPEN DEI and Connected Factories 2 CSA – more details of the DMP cluster are available in D11.1. In this respect, the T11.3 leadership continued to be in charge of the standardisation activity in the EFPF project and support project partners in their pledge to contribute towards relevant standards.

1.3 Contributions to standardisation from selected open calls

In the Open Call under Task 8.1 applicants were asked to answer the following question:

How much does your solution use and/or contribute to standards and standardisation?

The following table contains the anonymized results from the selected sub-projects:

Standardisation Body	Standard	Scope related to EFPF
ETSI CIM	NGSI-LD	NGSI-LD is an information model and API for publishing, querying and subscribing to context information. It is meant to facilitate the open exchange and sharing of structured information between different stakeholders. NGSI-LD has been standardized by ETSI (European Telecommunications Standardisation Institute) through the Context Information Management Industry Specification Group, following a request from the European Commission. The acronym NGSI stands for "Next Generation

Standardisation Body	Standard	Scope related to EFPF
		<p>Service Interfaces", a suite of specifications originally issued by the OMA which included Context Interfaces. These were taken up and evolved as NGSiv2 by the European Future Internet Public-Private-Partnership (PPP), which spawned the FIWARE open-source community.</p> <p>The standard is used by the sub-project for extending the EFPF Platform federation with Product Passport services. The sub-project integrated and tested the existing product passport services within the EFPF platform while also testing their integration with EFPF tools and service such as predictive maintenance.</p>
GS1	EPCIS 1.2	<p>Electronic Product Code Information Services (EPCIS) is a global GS1 Standard for creating and sharing visibility event data, both within and across enterprises, to enable users to gain a shared view of physical or digital objects within a relevant business context. "Objects" in the context of EPCIS typically refers to physical objects that are handled in physical steps of an overall business process involving one or more organisations. Examples of such physical objects include trade items (products), logistic units, returnable assets, fixed assets, physical documents, etc. "Objects" may also refer to digital objects which participate in comparable business process steps. Examples of such digital objects include digital trade items (music downloads, electronic books, etc.), digital documents (electronic coupons, etc.).</p> <p>The standard is used by the sub-project to create an intelligent welding quality monitoring and assessment system as a service within the EFPF Platform. This will allow the sub-project to enhance current welding processes while also providing EFPF with validation of several core components including the Data Spine, security Portal and Anomaly Detection module.</p>
IEC/TC 65/SC 65E , Devices and integration in enterprise systems	<p>OPC Unified Architecture –</p> <p>IEC/TR 62541-1:2020, Overview and concepts</p> <p>IEC/TR 62541-2:2020, Security Model</p> <p>IEC 62541-3:2020, Address Space Model</p> <p>IEC 62541-4:2020, Services</p> <p>IEC 62541-5:2020, Information Model</p> <p>IEC 62541-6:2020, Mappings</p> <p>IEC 62541-7:2020, Profiles</p> <p>IEC 62541-8:2020, Data Access</p> <p>IEC 62541-9:2020, Alarms and conditions</p> <p>IEC 62541-10:2020, Programs</p>	<p>Parts of this standards are used by the sub-project in the development of a cloud-based solution to enable to collection of production and manufacturing data, to support the provision of near real time insights to existing and future customers. This will allow the sub-project to access state of the art Industry 4.0 technologies to enhance existing processes while allowing EFPF to validate the tools and services offered in a real-world environment.</p>

Standardisation Body	Standard	Scope related to EFPF
	IEC 62541-11:2020 , Historical Access IEC 62541-12:2020 , Discovery and global services IEC 62541-13:2020 , Aggregates IEC 62541-14:2020 , PubSub IEC 62541-100:2015 , Device Interface	
IEEE 802.3 Ethernet	IEEE 802.3 Ethernet	This standard was applied by the sub-project to create an intelligent welding quality monitoring and assessment system as a service within the EFPF Platform. This will allow the sub-project to enhance current welding processes while also providing EFPF with validation of several core components including the Data Spine, security Portal and Anomaly Detection module.
Internet Engineering Task Force (IETF)	IETF RFC 8428	This specification defines a format for representing simple sensor measurements and device parameters in Sensor Measurement Lists (SenML). Representations are defined in JavaScript Object Notation (JSON), Concise Binary Object Representation (CBOR), Extensible Markup Language (XML), and Efficient XML Interchange (EXI), which share the common SenML data model. A simple sensor, such as a temperature sensor, could use one of these media types in protocols such as HTTP or the Constrained Application Protocol (CoAP) to transport the measurements of the sensor or to be configured. This standard was applied by the sub-project to extend EFPF services realizing lot-size-one manufacturing in European furniture domain.
Internet Engineering Task Force (IETF)	IETF RFC 4180 (CSV)	A comma-separated values (CSV) file is a delimited text file that uses a comma to separate values. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. The use of the comma as a field separator is the source of the name for this file format. A CSV file typically stores tabular data (numbers and text) in plain text, in which case each line will have the same number of fields. The standard was implemented by the sub-project to digitise the production chain of product processing to minimise waste, enable transparency, and optimise production processes. The sub-project aims to achieve this through the use and implementation of EFPF components which will allow EFPF to validate the solutions offered in a real-world scenario, while also allowing the sub-project to develop new software and assess the EFPF platform for future usage.
ISO/IEC JTC 1, Information Technology	ISO/IEC 21778:2017 , Information technology - The JSON data interchange syntax	The goal of ISO/IEC 21778:2017 is only to define the syntax of valid JSON texts. Its intent is not to provide any semantics or interpretation of text conforming to that syntax. It also intentionally does not define how a valid JSON text might be internalized into the data structures of a programming language. There are many possible semantics that could be applied to the JSON syntax and many ways that a JSON text can be processed or mapped by a programming language. Meaningful interchange of information using JSON requires agreement among the involved parties on the specific semantics to be

Standardisation Body	Standard	Scope related to EFPF
		<p>applied. Defining specific semantic interpretations of JSON is potentially a topic for other specifications. Similarly, language mappings of JSON can also be independently specified.</p> <p>The standard was implemented by the sub-project to digitise the production chain of product processing to minimise waste, enable transparency, and optimise production processes. The sub project aims to achieve this through the use and implementation of EFPF components which will allow EFPF to validate the solutions offered in a real-world scenario, while also allowing the sub-project to develop new software and assess the EFPF platform for future usage.</p>
<p>ISO/IEC JTC 1, Information Technology</p>	<p>ISO/IEC 20922:2016, Information technology -- Message Queuing Telemetry Transport (MQTT)</p>	<p>ISO/IEC 20922:2016 is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.</p> <p>The standard was applied by the sub-project to prevent machinery failures in the fish processing industry. The sub-project tests and validates a range of Tools and Services from the EFPF platform, within a real-world environment, and with the aim to share lessons learned within the community. This helps EFPF to validate the tools and services offered.</p>
<p>ISO/IEC JTC 1, Information Technology</p>	<p>ISO/IEC 19845:2015, Information technology - Universal Business Language Version 2.1 (UBL v2.2)</p>	<p>ISO/IEC 19845:2015 specifies the OASIS Universal Business Language (UBL), which defines a generic XML interchange format for business documents that can be restricted or extended to meet the requirements of particular industries.</p> <p>The standard was used by the sub-project to provide an integration of the eBin platform, which focuses on document collaboration in supply chains, with the WASP platform which is provided by EFPF. The sub-project aims to demonstrate workflow automation of the eBin processes through WASP, whilst also allowing eBin functionality to be integrated within the WASP platform. This will allow the sub-project to test alternative workflow technologies for use within the eBin platform.</p>
<p>ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection</p>	<p>ISO/IEC 27001:2013, Information technology -- Security techniques - Information security management systems -- Requirements</p>	<p>ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.</p> <p>The organisation behind the sub-project is certified for quality management (EN ISO 9001:2015) and for the information security management system (ISO 27001:2013).</p>

Standardisation Body	Standard	Scope related to EFPF
<p>ISO/TC 184/SC 5, Interoperability, integration, and architectures for enterprise systems and automation applications</p>	<p>IEC 62264, Enterprise-control system integration</p> <p>Part 1: Models and terminology</p> <p>Part 2: Objects and attributes for enterprise-control system integration</p> <p>Part 3: Activity models of manufacturing operations management</p> <p>Part 4: Objects and attributes for manufacturing operations management integration</p> <p>Part 5: Business to manufacturing transactions</p>	<p>The parts of this standard was applied by the sub-project to develop a cloud based solution to enable to collection of production and manufacturing data, to support the provision of near real time insights to existing and future customers. This will allow the sub-project to access state of the art Industry 4.0 technologies to enhance existing processes while allowing EFPF to validate the tools and services offered in a real-world environment.</p>
<p>ONNX</p>	<p>ONNX</p>	<p>The Open Neural Network Exchange (ONNX) is an open-source artificial intelligence ecosystem of technology companies and research organisations that establish open standards for representing machine learning algorithms and software tools to promote innovation and collaboration in the AI sector. ONNX is available on GitHub.</p> <p>The standard was applied by the partner, who is the leading European producer of paper and packaging, to demonstrate the value of deploying AI “on the edge” in Industrial IoT through the validation of anomaly detection models using the Scalable platform. The sub-project aims to leverage EFPF data analytic solutions for quicker detection of sensor failures. This can help the sub-project to save costs due to machines downtime through more timely maintenance operations.</p>
<p>OpenAPI</p>	<p>OpenAPI Specification</p>	<p>The OpenAPI Specification, previously known as the Swagger Specification, is a specification for machine-readable interface files for describing, producing, consuming, and visualizing RESTful web services. Previously part of the Swagger framework, it became a separate project in 2016, overseen by the OpenAPI Initiative, an open-source collaboration project of the Linux Foundation. Swagger and some other tools can generate code, documentation, and test cases given an interface file.</p> <p>This specification was applied by the sub-project to extend the EFPF Platform federation with Product Passport services. The sub-project will integrate and test the existing product passport services within the EFPF platform while also testing their integration with EFPF tools and service such as predictive maintenance, and all within a real-world.</p>

Standardisation Body	Standard	Scope related to EFPF
Profibus	Profibus	Standard for fieldbus communication in automation technology, which was used by the sub-project to create an intelligent welding quality monitoring and assessment system as a service within the EFPF Platform. This will allow the sub-project to enhance current welding processes while also providing EFPF with validation of several core components including the Data Spine, security Portal and Anomaly Detection module.
W3C	WebAssembly	WebAssembly (abbreviated Wasm) is a binary instruction format for a stack-based virtual machine. Wasm is designed as a portable compilation target for programming languages, enabling deployment on the web for client and server applications. It was used by the sub-project to demonstrate the value of deploying AI “on the edge” in Industrial IoT through the validation of anomaly detection models using the Scalable platform. The project aims to leverage EFPF data analytic solutions for quicker detection of sensor failures.
ZVEI SG 'Models and Standards' and Platform Industry 4.0 working group WG1	RAMI4.0	The Industry 4.0: Specification Details of the Asset Administration Shell was applied by the partner to extend EFPF services realizing lot-size-one manufacturing in European furniture domain. The partner developed novel business models assisting furniture manufacturers and their supply networks embrace such manufacturing.

2 Overview of Regulations affecting the EFPF Project Partners

The scope of this work package (WP11), the task T11.3 (Regulatory Alignment, Compliance and Standardisation Strategies) also includes the identification of regulations affecting the EFPF project.

Therefore, in the scope of T11.3, a preliminary survey has been carried out among the project partners to determine international, European, national, or regional regulations that affect the EFPF project partners and shall be considered to ensure legal compliance.

Results of the Survey on Regulations

The results collected from the regulations survey provide an outlook of relevant regulations that influence of the operations of project partners in the context of carrying out necessary activities in the project. The feedback -summarised in the table below – from individual partners will be taken into account while drafting the collaboration activities, technical developments and the governance mechanism in the EFPF project.

Regulation	How does this regulation affect EFPF	Partner
Airbus T 81 (Handbook)	It's a customer requirement to know which software and materials are used in the factory.	AAM
Benelux-verdrag inzake de intellectuele eigendom (NL)	This Benelux-treatment deals with trademark law. It might not directly affect only EFPF but also products / services that are exposed via EFPF.	ALM
BGBI. I Nr. 66/2002, Federal Law on the Granting of Privileges to Non-Governmental International Organisations (national Austrian law)	This law is the basis for founding the eFF (European Factory Foundation).	BRM
Conflict Minerals (On 1 January 2021 a new law will come into full force across the EU – the Conflict Minerals Regulation);	In politically unstable areas, the minerals trade can be used to finance armed groups, fuel forced labour and other human rights abuses, and support corruption and money laundering. These so-called 'conflict minerals' such as tin, tungsten, tantalum and gold, also referred to as 3TG, can be used in everyday products such as mobile phones and cars or in jewellery. The regulation requires EU companies in the supply chain to ensure that these minerals and metals are imported from responsible and conflict-free sources only. For EFPF this might become important as soon as order and delivery processes are available and performed via the platform, as these should at least indicate that the applicable goods do not violate any regulation. This is also valid for any catalogue listed items. An option might be that any company that offers products through EFPF catalogues etc. must confirm during registering process that all the offered products are manufactured (in case mentioned minerals are part of them) with a supply chain that uses these minerals and metals from responsible and conflict-free sources only.	IAI
Customer Regulation (e.g. Airbus)	It describes the process and environmental requirements for the manufacturing of the components. It sets limit values.	3DI
Cybercriminality regulations in NL – Wet Beveiliging Network – en	Each of the EU countries has to follow Directive (EU) 2016/1148. In NL, this means that suppliers of a digital marketplace cloud service (if they have a certain size or relevance) need to ensure the security of their service against cyber-attacks and need to report incidents to the	ALM

Regulation	How does this regulation affect EFPF	Partner
Informatiesystemen (Wbni)	National Cyber Security Centre (NCSC) and the CSIRT-DSP from the ministry of economic affairs.	
Digital Markets Act (DMA) [14]	The Digital Markets Act (DMA) establishes a set of narrowly defined objective criteria for qualifying a large online platform as a so-called “gatekeeper”. This allows the DMA to remain well targeted to the problem that it aims to tackle as regards large, systemic online platforms.	SRFG
Directive of the European parliament and of the council on corporate due diligence with regard to sustainability and amending Directive (EU) 2019/1937	EU companies operate in a complex environment and large companies in particular rely on global value chains. As EU companies, including large ones, work with a significant number of suppliers in the Union and in third countries, and value chains as a whole are very complex, it can be difficult for them to identify and mitigate risks related to human rights or environmental impacts in their value chains. Identifying these negative impacts in value chains will become easier as more companies engage in due diligence and thus more data becomes available on negative impacts on human rights and the environment from companies' operations. The EFPF platform must enable appropriate supply chain transparency information to be collected and presented by companies.	HAW
EASA Certification Specification and Acceptable Means of Compliance for Large Aeroplanes CS-25/EASA Part 21G, Section A, Subpart G “Production Organisation Approval”/ EASA Part 21J, Section A, Subpart J “Design Organisation Approval”/EASA Part 145 “Approved Maintenance Organisation”	EASA CS25 is a basic technical requirement for aerospace suppliers who develop, manufacture and maintain parts and equipment in the scope of mentioned chapter “Large Aeroplanes”. EASA 21G, 21J and Part 145 could be important for products and services offered from a company in EFPF catalogues etc. as the available certification might deemed mandatory from customers/OEM in the supply chain. This regulation might also be an important information for company profiles whether these certificates are available or not.	IAI
EN 9100	General quality management requirements for aviation Assuring a certain level of quality/ reliability/ working standards contribute to EFPF. EN9100 certification can be seen as a requirement for products and services in EFPF.	3DI, IAI
Ethical Trading Initiative (ETI)/ business ethics www.ethicaltrade.org	This is a candidate regulation to be revised, adapted or re-introduced as an enabler and a safeguard in the context of digital business ethics; see ETI’s guide to support companies uphold the right to freedom of associations within their supply chain [11]. It should be extended to include digital avatars (AI-driven, human-like robots) and other covert systems).	SRFG
Ethically Aligned Design (EAD) [13]	EAD is an initiative created by the IEEE Standards Association. It covers many topics of interest to EFPF development, including e.g. general (ethical) principles; how to embed values into autonomous intelligent systems; methods to guide ethical design; safety and beneficence of artificial general intelligence and artificial superintelligence; personal data and individual access control; reframing autonomous weapons systems; economics and	SRFG

Regulation	How does this regulation affect EFPF	Partner
	humanitarian issues; law; affective computing; classical ethics in AI; policy; mixed-reality, and well-being.	
Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI set by the EC [12]	This Guidelines set out a framework for achieving trustworthy AI. It offers an assessment list - “Trustworthy AI Assessment List (Pilot Version)” which includes (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) societal and environmental well-being, and (7) accountability. This framework will be tried out in EFPF before operationalizing the EFPF platform for Open Calls and public usage.	SRFG
EU regulation 185/2010, laying down detailed measures for the implementation of the common basic standards on aviation security	<p>Since April 28 2013, companies who are wishing to have their cargo considered “secure” must be certified as “known consignors” by the respective national aviation security authority pursuant to chapter 6.4.1.1 of Commission Regulation (EU) 185/2010. The authority in Germany is the Luftfahrtbundesamt (LBA – Federal Aviation Office). Companies can only be certified if they have submitted an air cargo security program and have been audited by the relevant authority. As part of the air cargo security program, companies are required to describe their compliance with a wide range of security standards. These requirements also include that air cargo must be protected against interference by third parties. This can be achieved by ensuring that the facility itself is secure and that technical and staffing measures (security controls) are in place.</p> <p>For EFPF this might become relevant for tracking parcels/cargo using blockchain technology. Furthermore, in terms of the EFPF Risk Assessment Tool there might be an option to implement camera technology with applicable software which detects non-authorized personnel in secured areas.</p>	IAI
EU regulation No. 428/2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items	Dual-use items are such items (also software and technology) that can be used both for civil and military purposes. As a worldwide operating company INNOVINT has to consider export control regulations in terms of listed dual-use items (e.g. https://www.zoll.de/EN/Businesses/Movement-of-goods/Export/Goods/Dual-use-items/dual-use-items_node.html). For EFPF this might become important as soon as order and delivery processes are available and performed via the platform, indicating that the applicable goods do not violate any regulation. This is also valid for any catalogue listed items.	IAI
GDPR	<p>Privacy and data protection, privacy by design need to be applied including the right to be forgotten</p> <p>This regulation affects ICE and EFPF during the project and in the post-project phase, since the project will be collecting data from the users of EFPF Portal and also the visitors of the EFPF website (maintained by ICE). This data will be used for analysis and contacting purposes.</p> <p>T5.2 Portal and T4.3 Secure Data Storage require to be adapted to the GDPR requirements.</p> <p>The data collected will be relevant and limited to the purposes of the use cases to be implemented in EFPF. In case that any personal data is collected it will be stored and processed only internally, encrypted or hashed.</p>	AAM, AID, ALM, ASC, ASI, CERTH, CNET, ELD, ELN, FIT, FOR, HAW, IAI, ICE, LINKS, KLE, NXW, SRDC,

Regulation	How does this regulation affect EFPF	Partner
	<p>The adopted security measures prevent unauthorised access to personal data and to the equipment used for processing of the data.</p> <p>All data provided by ELDIA through the EFPF portal will be used in a way that is GDPR compliant. The data will be processed only by the project members and exclusively for the purposes of the EFPF project. Data collected and stored as part of the Use case pilots. In general any EFPF application processing personal identifiable data. We have to ensure that the data we receive from customers can't be accessed by anyone. We design and implement tools and services that provide security and privacy and are GDPR compliant.</p> <p>The Data Spine needs to take the integrity of the data flows into account. The Data Model Conversion tool and “HyCoDER” (Hybrid Configurable Data Extraction and Restructuring System) tool in WP4 need to take this into account regarding user access regulations and data integrity.</p> <p>The data are collected from the use cases to which FOR participate. Specific security measures and security risk assessment shall be part of the work developed in the use cases. Aspects such as identifiers and equipment, e.g., MAC addresses, shall be obfuscated.</p> <p>HAW complies with GDPR requirements through continuous monitoring of the data collection and data usage procedures in the company, reviewing and updating Privacy Policy and website adjustments, and through trainings of employees to understand the importance of data protection and GDPR procedures, key concepts and GDPR articles.</p> <p>The data analytics tools developed in T4.2 takes into account GDPR for the data management.</p> <p>Data provided by KLE through the EFPF portal should be protected. The collected data will be processed exclusively for the purposes of the EFPF project.</p> <p>GDPR will affect EFPF in terms of the data collected by its various components, including the Accountancy Service, which is about tracking and tracing user behaviour and is developed within the scope of T3.3. At the moment, this service does not collect any personal data.</p>	SRFG, VLC
Incident notification for DSPs in the context of the NIS Directive [9]	It provides guidelines on how incident notification provisions for DSP could be effectively implemented across the EU, e.g. how to identify types of incidents, parameters and thresholds.	SRFG
ISO 9001	It's a customer requirement and is important for EFPF to show its compliance to this regulation.	AAM
Machinery Directive	The Machinery Directive covers the safety aspects of machinery, but also safety components, ropes and chains (e.g. robotics, self-configuring machines/ production lines and include cybersecurity aspects). The Machinery sector is an important part of the Engineering Industry. Machinery consists of an assembly of components, at least one of which moves, joined for a specific application. The drive system of machinery is powered by energy other than human or animal effort. This regulation affects EFPF in the post-project phase, when real data will be collected.	SIE

Regulation	How does this regulation affect EFPF	Partner
Medical Device Regulation (EU) 2017/745 (EU MDR)	Applies to future CNET development in so far as EFPF components or services are used in products, applications or services that qualify as medical device systems, the MDR applies.	CNET
National Cybersecurity Strategies (NCSS) by ENISA [7]	<p>NCSS are the main documents of national states to set strategic principles, guidelines, and objectives to mitigate cybersecurity risks. NCSS are directly required by the NIS Directive and supported by ENISA's good practice guidelines, implementation guides, cyber insurance, etc.</p> <p>ENISA's "Good Practices in Innovation on Cybersecurity under the NCSS" from November 2019 [8], analysis cybersecurity- related innovation, industrialisation and collaboration, and market and policy in the EU Member States. This publication analyses innovation dimensions related to market and market regulations across the EU, which is of a remarkable importance in EFPF. For example, it lists Austria's research in the area of cybersecurity through national and EU security research programmes (e.g. National Research Development Programme KIRAS Austria) and Austrian Cyber Security Platform launched by the Federal Chancellery in 2015.</p>	SRFG
NIS Directive - Directive on security of Network and Information Security [5]	<p>The goal of the NIS Directive is to enhance cybersecurity across the EU. From 09 May 2018, the NIS Directive incorporates national legislation through e.g. national capabilities "EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc." and a national supervision of critical sectors: "EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)".</p> <p>The NIS Directive strongly promotes risk management and incidents reporting between the Operators of Essential Services (OES) and Digital Service Providers (DSP) in the EU. The scope of DSPs, in the context of NIS Directive, is limited to cloud computing services, online marketplace and online search engines, which regards EFPF as a DSP, e.g. as an online marketplace allowing business entities to share their product catalogues and business services with other consumers or businesses. Hence, EFPF must comply with the NIS Directive and provide risk management and incidence reporting.</p> <p>Article 16(4) of the NIS Directive lists the following parameters to be shared to determine any cross-border impact of an incidence: (1) the number of users affected by the incident, (2) the duration of the incident, (3) the geographical spread regarding the area affected by the incident, (4) the effect of the disruption, and (5) the extent of the impact on economic and societal activities.</p> <p>Article 16(11) defines that DSPs that are micro or small enterprises (employing fewer than 50 persons and having an annual turnover not exceeding €10 million) are excluded from the scope of the security requirements and incident notification, which shows a potential impact of the NIS Directive on EFPF after the expected growth of the EFPF platform ecosystem.</p> <p>The mandatory notification requirements of the NIS Directive are described in "Guideline on Notifications of DSP Incidents (formats and procedures)" from July 2018 [6].</p>	SRFG

Regulation	How does this regulation affect EFPF	Partner
Radio Equipment Directive (RED)	<p>The RED establishes a regulatory framework for placing radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects such as: technical features for the protection of privacy, personal data and against fraud, interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software.</p> <p>This regulation has impact in the field of IoT (devices transmitting data between themselves) and affects EFPF in the post-project phase, when real data will be collected.</p>	SIE
Reach regulations	<p>They govern the use of rare and dangerous substances that may be used in the piloting activities.</p> <p>It's a customer requirement and is important for EFPF to show its compliance to this regulation.</p> <p>This regulation has impact on whole supply chains as it is binding requirement for OEM and suppliers. EFPF should list only Reach conform products in catalogues etc.</p>	3DI, AAM, IAI
Regulation (EU) 2018/1807	<p>Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union applies to data processing in the broadest sense, encompassing the usage of all types of IT systems, whether located on the premises of the user or outsourced to a service provider. It covers data processing of different levels of intensity, from data storage (Infrastructure-as-a-Service (IaaS)) to the processing of data on platforms (Platform-as-a-Service (PaaS)) or in applications (Software-as-a-Service (SaaS)).</p>	ASI
Regulation (EU) 2019/1150	<p>Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services. This regulation specifies kind of a code of conduct to be respected when operating an online platform such as EFPF.</p>	ASI
REGULATION (EU) 2019/424	<p>COMMISSION REGULATION (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013. Since EFPF will provide a data intensive platform, energy efficiency and ecodesign aspects need to be considered</p>	ASI
Regulation (EU) 2019/881	<p>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 526/2013 (Cybersecurity Act)</p>	ASI
<p>Regulations regarding social responsibility:</p> <p>UN Global Compact, acc. to OECD, SA 8000, UN Guiding Principles on Business and Human Rights, etc.</p>	<p>All these documents are focussing on Human Rights, Working Conditions, Safety and Health, Environmental Protection, Business Ethics, Sustainable Supply Chain etc.</p> <p>For EFPF this will become important as soon as companies join the platform and become active users of platform's services. EFPF should ensure that no business is supported that violates any of the above-mentioned laws and rights.</p>	IAI

Regulation	How does this regulation affect EFPF	Partner
Restriction of Hazardous Substances (RoHS) EU regulation No. 2011/65/EU	This regulation has impact on the entire supply chain as a binding requirement for OEM and suppliers. EFPF should list RoHS conform products (e.g. no use of lead) in catalogues etc.	IAI
Royal Decree 486/1997 of April 14th [4]	As the previous ones, this Decree establishes a series of rules to guard the health and safety of workers within the workplaces. It ensures that workers have all health and safety guarantees when working in offices, etc. With the current COVID-19 crisis in Spain, working from home does not necessarily fulfil all the safety requirements of the Decree. For instance, couches, home chairs, home tables or desks are no substitute for a fully equipped office.	AID
Royal Decree 488/1997 of April 14th [3]	It defines health and safety regulations related to the work with equipment that include visualisation screens. This decree establishes a series of rules to guard the health and safety of workers that operates with such kind of devices. However, laptop screens are excluded from this regulation, providing that they are not used continuously to perform the daily work shift. With the current COVID-19 crisis in Spain, this comes into conflict with the previous Decree due to the fact that most of the employees are working from home using solely laptop screens, thus indirectly transgressing this Decree.	AID
Royal Decree 8/2020 [2]	The right to adapt the work shifts or other features related to the work. With the current COVID-19 crisis in Spain, this regulation allows workers to have ample flexibility when structuring their daily routines. At the same time, some side effects cannot be avoided, e.g. delimiting physical meetings and unsupervised work that might yield to a reduction in the quality of work, especially in junior worker profiles.	AID
Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (DSP) [10]	It provides a common baseline security objectives and measures for DSPs across the EU. In addition, it maps the security objectives against well-known industry standards, national framework and certification schemes, which is necessary to be addressed in EFPF too. For example, this document describes how the DSP establishes and maintains asset management procedures and configuration controls for key network and information systems, and many other aspects of information security.	SRFG

3 Standardisation Strategy

Based on the initial plan (D11.11) and the survey on standardisation (in Section 1), the standardisation strategy devised in the EFPF project is based on the P-D-C-A (Plan – Do – Check – Act) method. This involves pursuing the following activities:

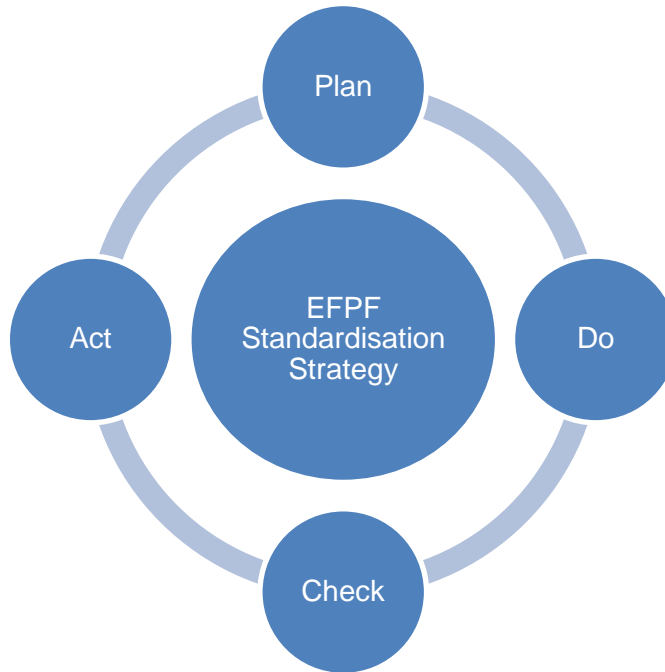


Figure 1: EFPF standardisation strategy

- **Phase Plan:** Based on the surveys from Section 1 and Section 2, a decision on standards relevant for the project is carried out.
- **Phase Do:** The project partners ensure the compatibility and interoperability of their services and technical solutions with the relevant standards.

Partners contribute towards the compliance, application, and development of standards in the areas of relevance to the EFPF as follows:

- Common communications standards and reference architecture for connections between machines (M2M) and with sensors and actuators in a supply chain environment are seen as a priority in the project
- Specific industrial needs, e.g. standards that support communications on broadband infrastructures and data formats to allow for the quick transfer of large volumes of data over networked industries
- Improving interoperability and reducing overlap, redundancy, and fragmentation of the data
- Project partners contribute to activities in Standards Development Organisations (SDOs) working on interoperability standards for security and for linking communication protocols in order to provide end-to-end security for complex manufacturing systems including the span of virtual actors (from devices and sensors to enterprise systems)
- The project partners participate towards creating a hierarchical catalogue of technical and social measures for assuring privacy protection. That implies processing of data which includes personal data within the definition of the GDPR.
- Partners participate towards the development of standards for ensuring long-term

traceability of material to enable re-use and recycling.

- **Phase Check:** Partners shall periodically review and align their standardisation activities and provide a report for internal and external awareness.
- **Phase Act:** If the new subject areas and regulations relevant to the project are planned or identified by SDOs (e.g. CEN, CENELEC, ETSI, IEC, ISO, IEEE) the partners have to create a corresponding analysis of the target status and compare it with the current status. Furthermore, the questions of what can be optimized and where lay a further potential of standardisation activities, must be clarified. If it is determined that the goal has not been reached, the cycle is run through again.

3.1 Strategic Areas of Participation

The analysis of the ongoing standardisation activities in the project and partners interests reveal the following key areas that require an active participation from a project’s strategic point of view.

81 standards (published and under development) were identified (see Section 1.2). In the following figure the number of these standards allocated to the strategic areas of participation is illustrated (multi-part standards are counted as one standard).

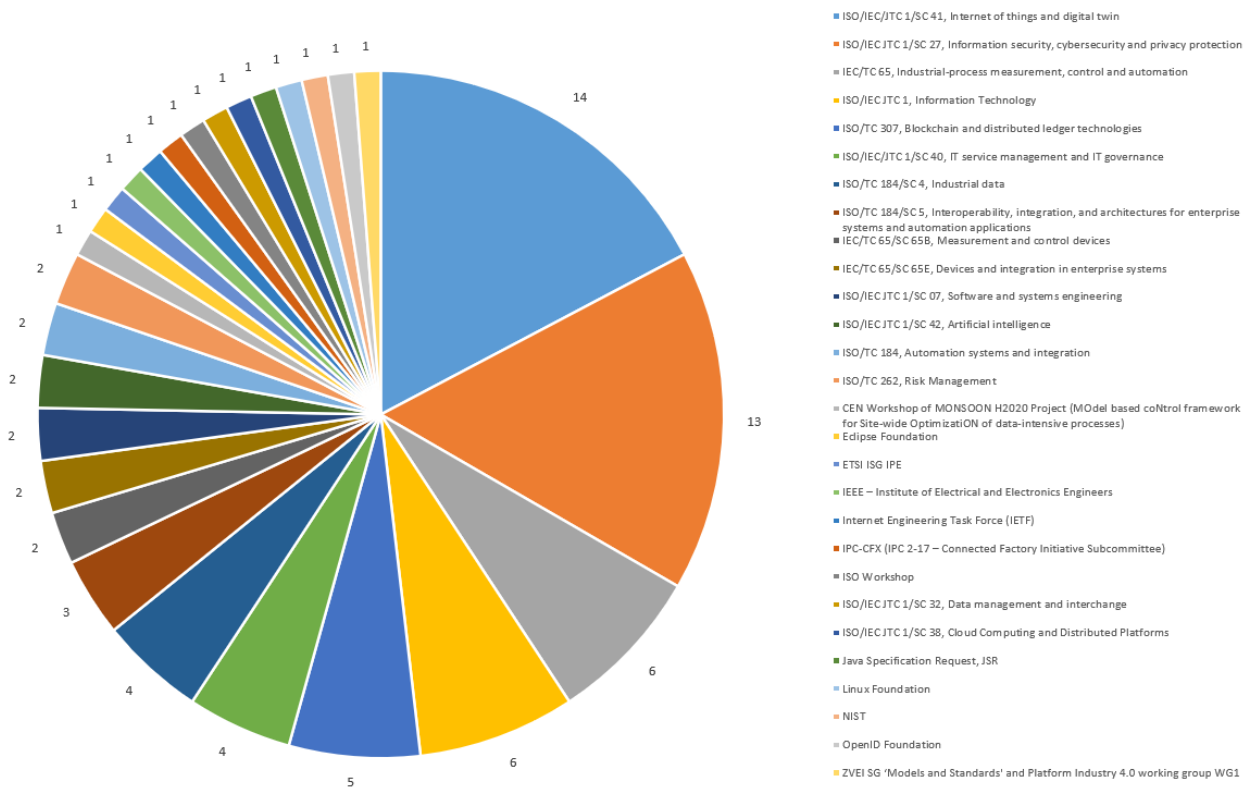


Figure 2: Strategic areas of participation with number of standards for each area

Those partners participating in the following standardisation areas are committed to report latest and important developments to the project and feed findings from the project back to standardisation using ASI as communication channel. Such two-way interaction between EFPF and standardisation communities contributes to an optimal alignment of the project activities and outcomes with standards (published and under development).

Special attention needs to be given to those standardisation projects, which support regulations. Especially New Legal Framework (NLF) directives/regulations of the European Union foresee a strong link with standards. These standards are elaborated based on a standardisation request from

the European Commission and gain the status of harmonized European Standards (hEN). Such NLF regulations are for instance the Machinery Directive and the Radio Equipment Directive.

3.1.1 CEN Workshop of MONSOON H2020 Project (MOdel based coNtrol framework for Site-wide Optimisation of data-intensive processes)

C2K has studied and implemented CWA 17492, Predictive control and maintenance of data intensive industrial processes, for the realisation of data intensive industrial processes.

ICE is investigating CWA 17942, in particular, how it can be used to support and enhance the machine learning techniques deployed within the ICEData Analytics – Anomaly Detection Tool.

3.1.2 Eclipse Foundation

ICE's Pub Sub Security Service has considered and implemented the Sparkplug specification to provide a framework for the standardised definition of topics in the EFPF Message Bus.

FOR has integrated MQTT Sparkplug into TSMatch, having developed a White paper³ on the integration aspects.

3.1.3 ETSI ISG IPE

FOR participates in the Industry Specification Group (ISG) on IPv6 Enhanced innovation (ISG IPE). The participation concerns monitoring in order to ensure alignment of the current EFPF components to the latest development of ISG IPE.

3.1.4 IEC/TC 65, Industrial-process measurement, control and automation

NXW has reviewed the scope of the IEC/TC 65 to determine the applicability to ongoing EFPF activities relating to industrial-process measurement, control and automation. Following a preliminary analysis of the published parts of the standard, NXW is considering IEC TS 62443, parts 3 and 4 in particular, to define the guidelines for the development of its next generation factory connectors. NXW has investigated the activities, in particular, IEC 62264-1:2013, IEC 61499-1:2012, and IEC PAS 63088:2017. The analysis has confirmed the validity of the current approach where RAMI 4.0 is adopted as a reference but not as a mandatory specification.

CNet monitored the standardisation activities on the device integration with IoT platforms. The analysis carried out was used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

CERTH used IDS Trusted Connector for secure connectivity of fill level sensors of industrial open top containers. This type of connectors following the ISO/IEC 27070 and IEC 62443-3 standards.

ASI promoted IEC PAS 63088 that provides a reference model for EFPF as RAMI 4.0 is at the foundation of Industry 4.0 standardisation efforts.

3.1.5 IEC/TC 65/SC 65B, Measurement and control devices

NXW has investigated the activities of this standardisation committee, in particular, IEC 62264-1:2013, IEC 61499-1:2012, and IEC PAS 63088:2017. No parts of the standard have been considered relevant for the company's products.

CNet monitored the standardisation activities on the device integration with IoT platforms. The analysis carried out was used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

³ See https://www.researchgate.net/publication/358618553_White_Paper_Applying_MQTT_Sparkplug_in_the_EFPF_Platform

3.1.6 IEC/TC 65/SC 65E, Devices and integration in enterprise systems

C2K adopted and harmonised the standards in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K did this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services.

NXW investigated models and ontologies from OPC UA, in particular IEC 62541-5:2020 OPC Unified Architecture – Part 5: Information Model at the border between building and factory concepts. NXW evaluated as well the addition of OPC-UA to its factory connector for machine-to-machine communication.

ICE investigated the OPC-UA standard, on how it will be used by the new Administration Shell standard. ICE Workflow Platform WASP (T4.6) is being tuned to support OPC UA based communication in workflows/processes that are designed to link multiple shop-floor assets. ICE has studied the support for OPC-UA in its WASP tool for enabling direct reading from factory PLC's and sensors. The intention is to use sensor data in conditional gateways for dynamic process execution flows. ICE is also studying OPC-UA in the context of the ICE Anomaly Detection tool to increase the number of communication protocols supported by the tool.

FOR is actively following OPC FLC (Field Level Communications) QoS and traffic models, thus ensuring alignment of requirements in this context towards EFPF. The TSMATCH component is currently being developed over MQTT; however, it will also be able to interface with OPC UA in order to ensure compatibility with other EFPF components.

CNET is an OPC Foundation member and has started to promote the adoption of this standard in EFPF tasks (T3.5).

3.1.7 IEEE – Institute of Electrical and Electronics Engineers

ICE is referencing IEEE 2413:2019 in its platform development initiatives and is investigating the standard as a mean to provide support for IoT based communication in the workflows and processes of its WASP tool.

CNet is promoting the uptake of this standard on IoT architecture in the development of Data Spine (T3.2). Monitoring this standard will also benefit CNet commercial activities in IoT devices.

FOR is monitoring the IEEE 2413, the standard references for Smart Cities (P2413.1). FOR has interest in the future developments of this specific part, to ensure standardisation alignment. FOR expects to apply the P2413.1 IoT architecture principles to ensure alignment in regard to Edge-based data matching services.

CERTH uses the same approach (sensors, gateways, edge IT, real time data processing and cloud/data centre) as in COMPOSITION but processing levels can provide an interface for more upper-level frameworks that integrate different IoT domains and adhere to the related standards such as the IEEE P2413 standard

3.1.8 Internet Engineering Task Force (IETF)

Based on the plan in D11.11, WASP has already implemented OpenID Connect built on top of OAuth 2.0 as a security standard to enable Single Sign-On functionality in EFPF federation. ICE also implemented OAuth 2.0 within its Anomaly Detection tool to support the integration with the EFPF security components.

3.1.9 IPC-CFX (IPC 2-17 – Connected Factory Initiative Subcommittee)

The identification of the standard provides an impetus to EFPF (T5.5) to align the relevant application development activities (through the SDK in T5.5) with the IPC-CFX standard. The associated open source “Software tools for Connected Factory Exchange SDK” (Version 1.0.5) is relevant in this regard. Relevant EFPF partners (e.g. CMS) also investigated joining the IPC-CFX movement in

order to contribute towards the further enhancement/ development of the standard e.g. for the manufacturing applications to be developed in the EFPF project.

CMS is the leader of the Connected Factory SDK group (WG-DA-05) and is developing activities towards creating requirements and a common vision for a standard, innovative and reusable SDK to be adopted by the European projects, particularly in the manufacturing area.

CMS continues working towards the standardisation of an SDK and towards the alignment of its current SDK to the new vision and suite of tools.

3.1.10 ISO/IEC JTC 1, Information Technology

AMQP, MQTT and JSON are essential standards for the application integration and the building blocks of the EFPF Data Spine and the platform. The uptake, interoperability and/or alignment of these standards has been carried out in the tasks dealing with message exchange in EFPF (T3.2 - Data Spine).

CERTH considers protocols such as ISO/IEC 19464:2014, ISO/IEC 20922:2016 and ISO/IEC 21778:2017 for the design of its components and its communication with other tools and services.

ICE has considered ISO/IEC 19464:2014 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment to the standard has taken place in T6.2 to ensure the secure transport of messages to the EFPF Message Bus via AMQP.

ICE has implemented several standards in the technical activities, such as:

- ISO/IEC 19464:2014 within in its anomaly detection, data analytics solution for the design of the component and its communication with Message Brokers.
- ISO/IEC 20922:2016 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment to the standard will take place in T6.2 to ensure the secure transport of messages to the EFPF Message Bus via MQTT.
- ISO/IEC 20922:2016 within in its anomaly detection, data analytics solution for the design of the component and its communication with other Message Brokers.
- ISO/IEC 21778:2017 as an essential standard for the implementation of the Pub Sub Security Service, Implementation and alignment to the standard will take place in T6.2 to support the communication between service components and external tools and services. This standard has also been implemented by ICE's WASP tool for the design of marketplace services and REST communication between internal components and external EFPF tools and services.
- ISO/IEC 21778:2016 within in its anomaly detection, data analytics solution for the design of the component and its communication with Message Brokers where data from devices can be pushed.
- ICE's WASP tool has been enabled to communicate with external process applications that use UBL. ICE is investigating and testing the use of UBL in the WASP platform to work towards the closed integration with UBL with an aim to ensure a closer interface with the BPMN2.0 standard.
- ICE has adopted BPMN 2.0 as a modelling notation for workflows. ICE's WASP is using BPMN for designing processes and monitoring their execution. ICE has now extended the use of BPMN in the WASP tool, implementing listeners that include functionality to generate and execute custom code.

CNet monitored the activities related to MQTT (ISO/IEC 20922:2016) due to its importance in the development of Data Spine (T3.2) and CNet's IoT applications.

In the context of T4.1 and T3.2, FOR continues the integration of MQTT and addressing interoperability issues towards other protocols, e.g., OPC-UA, CoAP. FOR is monitoring activities concerning MQTT (ISO/IEC 20922:2016) and its industrial counterpart, MQTT Sparkplug, in regard

to the TSMATCH component (T4.1), providing a publication (white paper⁴) and the evolutionary aspects concerning MQTT Sparkplug.

Considering the cross-platform data model, EFPF platform sees the UBL v2.2 (or v2.3) as a candidate. In the NIMBLE project, the UBL v2.1 version of the standard is used. In the scope of EFPF, the data model of NIMBLE were upgraded to v2.2, or v2.3 that was expected in December 2019. In the scope of EFPF standardisation activities, SRDC submitted additional user requirements and/or user usage scenarios to the UBL community in order to contribute to UBL 2.3

3.1.11 ISO/IEC JTC 1/SC 07, Software and systems engineering

ICE investigated ISO/IEC TS 33052:2016, Information technology - Process reference model (PRM) for information security management, and promoted its adoption for the development of security reference models (in T6.2)

3.1.12 ISO/IEC JTC 1/SC 27, Information security, cybersecurity and privacy protection

SRFG considered the set of Information Security standards for the design of security controls (T6.2) in EFPF. SRFG is also interested in contributing to cloud security standards, e.g. ISO/IEC 27017:2015. SRFG analysed ISO/IEC 24392 which is in an early stage of development.

CERTH used IDS Trusted Connector for secure connectivity of fill level sensors of industrial open top containers. This type of connectors following the ISO/IEC 27070 and IEC 62443-3 standards.

Regarding ISO/IEC 18033-3, ICE's Pub Sub Security Service has considered and implemented the Sparkplug specification to provide a framework for the standardised definition of topics in the EFPF Message Bus.

3.1.13 ISO/IEC JTC 1/SC 32, Data management and interchange

EFPF partners (SRFG, CERTH, VLC, C2K) have investigated ISO/IEC 6523 that provides information on how to identify organisations and organisational parts in data interchange. EFPF tasks on matchmaking (T4.5) and marketplace framework (T3.3) are currently analysing the use of this standard at company registration phase or when exchanging business messages. Some implications on domain specific aspects are being investigated

VLC along with other partners is actively investigating the use of these standards for data sharing between platforms. The approach for Business and Networking Intelligence follows the matchmaking task which uses a combination of standard including the ones mentioned here and others such as eClass and UBL.

3.1.14 ISO/IEC JTC 1/SC 38, Cloud Computing and Distributed Platforms

ISO/IEC 17788:2014, Information technology -- Cloud computing -- Overview and vocabulary, provides a comprehensive vocabulary that is relevant to all types of organisations. There is little potential to further enhance this standard and therefore the activities in EFPF project will focus on the use of this standard terminologies across project documents and dissemination channels.

FOR is actively involved in the development of the GAIA-X initiative to strengthen Europe's data infrastructure. In addition to being one of the members of GAIA-X AISBL, FOR is involved on the Data Interoperability and Interconnection working groups. Concrete contributions relate with a better support of Edge computing-based services on the GAIA-X catalogue, and contributions to the overall network service composition approach of GAIA-X.

⁴ See https://www.researchgate.net/publication/358618553_White_Paper_Applying_MQTT_Sparkplug_in_the_EFPF_Platform

3.1.15 ISO/IEC/JTC 1/SC 40, IT service management and IT governance

SRFG implemented the ISO/IEC 38500 and assured that the data accountability map and associated matrix of considerations from ISO/IEC 38505-1 are fully adopted in EFPF. The data governing principles in EFPF are implemented according to the IT governance methods presented in these standards.

3.1.16 ISO/IEC/JTC 1/SC 41, Internet of Things and digital twin

NXW has reported internally about the activities of ISO/IEC/JTC 1/SC 41. As regards ISO/IEC 21823, ISO/IEC 30141, ISO/IEC 30161, ISO/IEC 30162, ISO/IEC 30164, ISO/IEC 30168, ISO/IEC 30172, ISO/IEC 30173, and PWI JTC1-SC41-5, even though there are currently no plans to adopt them, they will still be monitored in the future. As regards ISO/IEC 30144, ISO/IEC 30147, ISO/IEC 30149, ISO/IEC 30163, and ISO/IEC 30165, there are currently no plans to adopt them as well.

CNet has monitored the standardisation activities in the realm of IoT and this has informed the design and development of integration and interoperability mechanisms for IoT sensors and devices in the EFPF platform (T3.2, T4.4).

SRFG has monitored the ongoing development of the Trustworthiness framework in the ISO/IEC 30149 - Internet of things (IoT). A possible cooperation with the ISO/IEC JTC 1/SC 41 was investigated in the context of the EFPF task related to trust (T5.3).

3.1.17 ISO/IEC JTC 1/SC 42, Artificial intelligence

ICE followed the framework of ISO/IEC 23053 to provide a comprehensive functionality of AI/ML systems in its Anomaly Detection Component.

ICE studied ISO/IEC DTR 24372 to identify the state-of-the-art computational approaches that are applicable to anomaly detection and how to add new algorithms in its Anomaly Detection Component ML powered systems

3.1.18 ISO/TC 184, Automation systems and integration

CNet monitored the standardisation activities on the device integration with IoT platforms. The analysis carried out was used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

3.1.19 ISO/TC 184/SC 4 – Industrial data

C2K adopted and harmonised the standards from ISO/TC 184/SC 4 in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K done this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services.

CNet studied the activities on Product Data representations and Digital Twin standardisations which are relevant to CNet's commercial activities related to the equipment manufacturing.

3.1.20 ISO/TC 184/SC 5, Interoperability, integration, and architectures for enterprise systems and automation applications

C2K adopted and harmonised the standards such as IEC 62264 in relation to the Factory Connector Architecture (T4.1) to support the building blocks of the EFPF platform. C2K done this by considering the format of data at all levels of the automation model and how this will support interoperability for the platform tools and services.

CNet monitored the standardisation activities on the device integration with IoT platforms. The analysis carried out was used to inform the design of Data Spine (T3.2) and align the development of Data Spine with latest standards on IoT integration.

ISO 11354-1 is implemented in T4.4 (WG 1) / INTEROP Enterprise interoperability framework.

3.1.21 ISO/TC 262, Risk Management

Although a working group has been setup by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to focus on the Risk Management topic, there is no current activity in this area. This represents an opportunity for EFPF (particularly the partners involved in the development of Risk Management Tool in T4.4) to support and collaborate with BSI towards the development of standards in this area. One area of interest for EFPF will be to facilitate the exchange of knowledge between BSI and NIST's Risk Management Framework. ASI will facilitate the investigation and collaborations in this area.

3.1.22 ISO/TC 307, Blockchain and distributed ledger technologies

CNET and CERTH both monitored the standardisation activities for application in the blockchain, distributed ledger and smart contracting efforts.

3.1.23 Java Specification Request, JSR

ICE's WASP has now implemented the standard Java portlet's as pluggable user interfaces. A portlet container runs the portlets with the run time environment.

3.1.24 Linux Foundation

ICE's WASP has investigated and started to implement OAS 3.0 for the provision of the tools REST interface which will enable standardised communication between tool components such as camunda process engine, liferay, the process designer and forms editor.

ICE's Pub Sub Security Service has implemented OAS 3.0 to provide a rest interface for communication between backend and front-end components.

3.1.25 OpenID Foundation

Based on the plan in D11.11, WASP has already implemented OpenID Connect (built on top of OAuth 2.0 as a security standard to enable Single Sign-On functionality in EFPF federation.

ICE investigated the OpenID Connect standard as a means for authentication between RabbitMQ (Message Bus) and Keycloak (EFS). OpenID Connect proved insufficient for the use case, only providing support for a UAA server and not a Keycloak sever.

ICE has also implemented OAuth 2.0 within its Anomaly Detection tool to support the integration with the EFPF security components.

3.2 Participation in Strategic Groups

The key EFPF participation in strategic groups resulted in the creation of the **CEN-CLC-ETSI Coordination Group on Smart Manufacturing**, in 2019. The objectives of this Coordination Group are the following:

- To advise the CEN and CENELEC Technical Boards (BTs) and ETSI Board on the standardisation needs in the Smart Manufacturing sector and initiate appropriate actions
- To advise the CEN and CENELEC BTs and ETSI Board on political issues concerning smart manufacturing
- To establish a synchronisation model for the various standardisation activities among CEN, CENELEC, ETSI and SDOs
- To advise the CEN and CENELEC BTs and ETSI Board on ways and means to improve their

visibility and recognition in the process of industry digitalisation

Stakeholders participating in the Coordination Group are:

- European Commission DGs and the EFTA Secretariat
- Representatives of interested Technical Bodies in CEN, CENELEC and ETSI
- IEC, ISO
- National members of CEN, CENELEC and ETSI
- SDOs, consortia and alliances (of industrial partners)
- European associations representing interested stakeholders
- National initiatives
- Major European research projects, large scale pilots, test beds
- Open-source communities
- Industry, including SME
- National initiatives, including relevant National Research & Innovation Centres
- Societal stakeholders

ASI participated in the Coordination Group acting as liaison officer for EFPF. This has the strategic advantage of increasing EFPF's visibility among stakeholders represented in the Coordination Group and receiving the first-hand feedback from the Coordination Group for the project partners.

3.3 CEN-CENELEC Workshop EFPFInterOp

The strategic areas of involvement in standardisation, described in Section 3.2, include cybersecurity, IoT, AI, Big Data, etc. Taking a holistic approach on standardisation in EFPF requires creating a report like this, to help platform's users to maximise connectivity, interoperability and efficiency of their services and participation across the supply chain in the EFPF platform ecosystem.

This is in support to the Final Report of Study on "Support to the observatory for the online platform economy"⁵. In this Final Report from 2021 it is written, that gaps concerning specific types of B2B platform services, including services relating to the industrial Internet of Things, constitutes certain challenges faced by business users. In the context of T11.3 the finding in this Final Report is of importance, that there is a need for establishing standards on data interoperability because of the current lack of interoperability or data standardisation.

Being part of the Digital Manufacturing Platforms for Connected Smart Factories and interacting with other projects in this cluster (including ZDMP and QU4LITY), resulted in the initiation of the **CEN-CENELEC Workshop for EFPF**, with the aim to create a standardisation deliverable "**CEN-CENELEC Workshop Agreement (CWA)**"⁶. The CWA is a publicly available specification and a tool for the development of an interoperable EFPF platform and ecosystem.

⁵ See <https://op.europa.eu/en/publication-detail/-/publication/ee55e580-ac80-11eb-9767-01aa75ed71a1/language-en/format-PDF/source-206332284>

⁶ A CWA is a standardisation deliverable, which may take various forms such as text file or computer code, developed and agreed by the participants in a temporary working group (CEN-CENELEC Workshop). It is designed to meet an immediate need and can be quickly developed and can be used as fast track to future standardisation activities. The stakeholder involvement is limited itself to those directly interested in the subject. The development of a CWA is fast and flexible, on average between 10-12 months. For further information see <https://boss.cen.eu/developingdeliverables/CWA/Pages/default.aspx>

A proposal for creating the CEN-CENELEC Workshop for EFPFInterOp was submitted to the CEN-CENELEC Management Centre by Austrian Standards International in September 2020. The kick-off meeting for the Workshop was announced on the website of CEN-CENELEC⁷, see figure below. The information about this announcement was disseminated to the target audiences through the channels of EFPF, its individual partners as well as those of the national CEN members, e. g. social media.

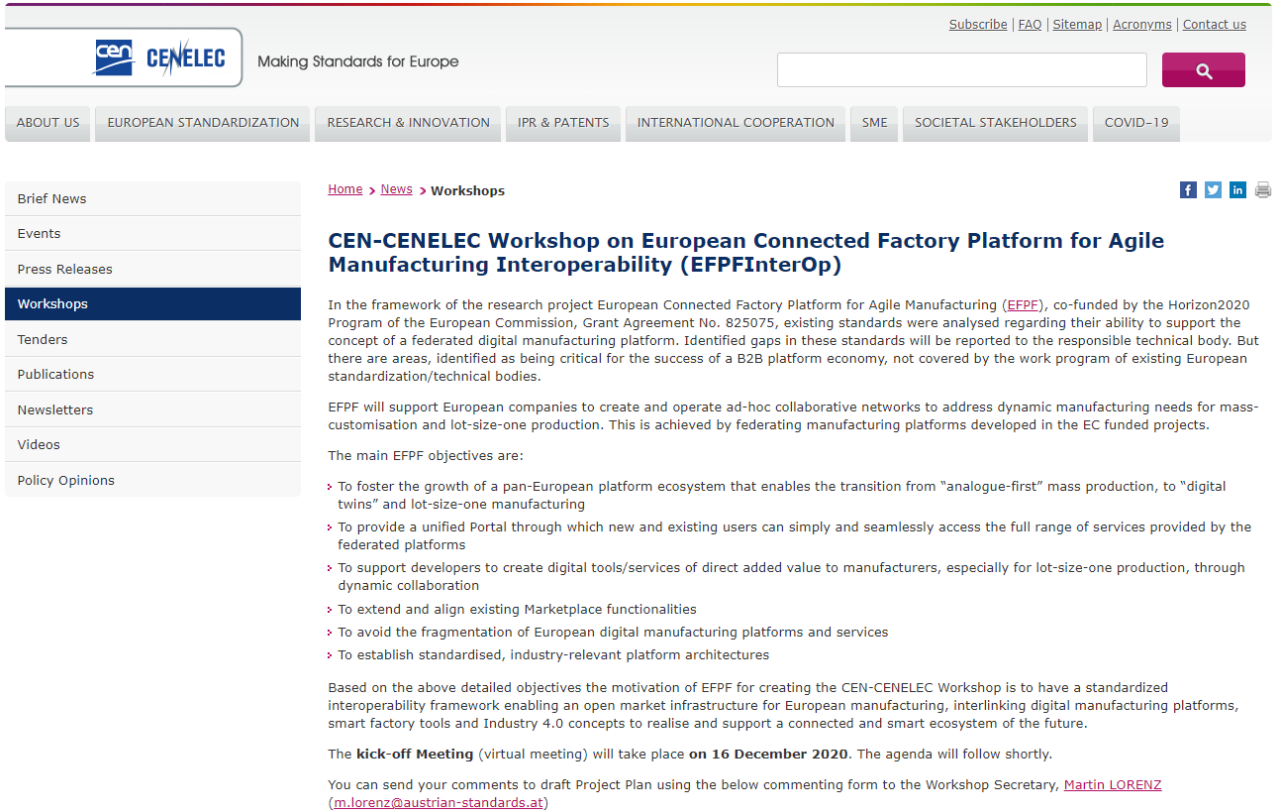


Figure 3: Screenshot of the announcement of the CEN-CENELEC Workshop EFPFInterOp from the CEN-CENELEC website

At the kick-off meeting of EFPFInterOp – which was held virtually on 16. December 2020 – the scope of the workshop and the workshop schedule were approved:

To elaborate a CEN-CENELEC Workshop Agreement (CWA) for ensuring interoperability in an ecosystem of federating manufacturing platforms, including a central portal and marketplace:

- Reference architecture for federating manufacturing platforms focusing on the interoperability on Service-Oriented Architecture (SOA), Protocol, Security and Data Model level. Additionally, a reference implementation in the form of the EFPF Data Spine and associated components will be described as well as including identified Best Practices.
- Such a federated platform having as a central Portal and Marketplace is the foundation for supporting growth and sustainability due to connecting with other platforms as well as with single enterprises.

⁷ See <https://www.cencenelec.eu/news/workshops/Pages/WS-2020-011.aspx> (due to a rebrush of the CEN-CENELEC Website the link is no longer valid)

CEN-CENELEC Workshop	M0	M1	M2	M3	M4	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
Initiation															
1. commenting on draft project plan, announcing kick-off meeting															
Development															
2. Kick-off meeting / Workshop constituted															
3. Drafting CWA															
Dissemination															
4. Public commenting on draft CWA															
5. Resolution of comments and approval of CWA															
Publication															
6. Publication of CWA															

The scope of the CEN-CENELEC Workshop EFPFInterOp and its relationship with EFPF is illustrated in the following figure:

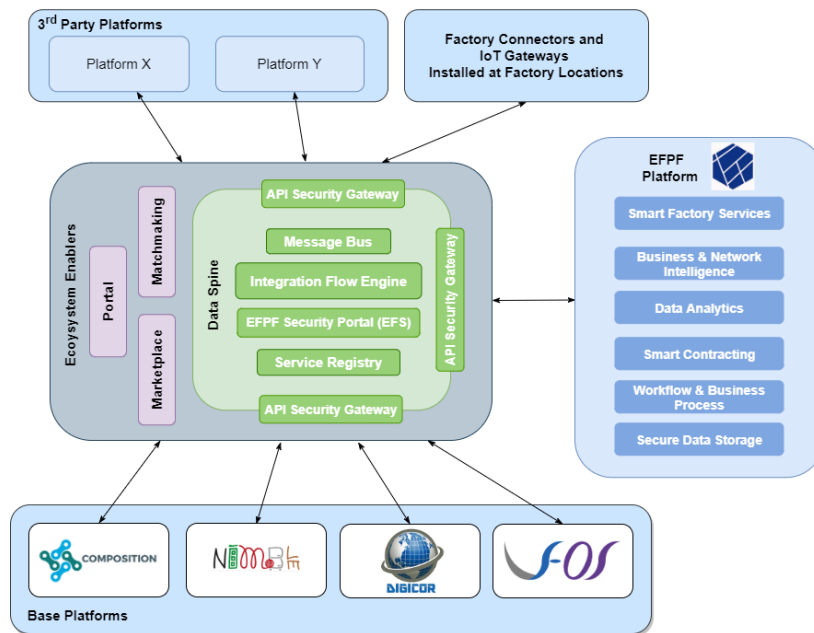


Figure 4: Scope of the CEN-CENELEC Workshop EFPFInterOp

The CEN-CENELEC Workshop EFPFInterOp is chaired by Chairperson Alexander Schneider (FIT) and Vice-chairperson Usman Wajid (ICE) with Martin Lorenz (ASI) and Andreas Feigl (ASI) as secretariat.

Next to partners from EFPF stakeholders, including representatives from DMP Cluster projects, were invited to participate in the CEN-CENELEC Workshop EFPFInterOp. The following organisations and individuals participated in the CEN-CENELEC Workshop:

1. 3D ICOM GmbH & Co. KG
2. AIDIMME, Instituto Tecnológico Metalmecánico, Mueble, Madera, Embalaje y Afines
3. AM Allied Maintenance GmbH
4. Ascora GmbH
5. Austrian Standards International
6. Brimatech Services GmbH
7. Caixa Mágica Software SA
8. Centre for Research & Technology, Hellas – CERTH
9. Change2Twin (H2020 – No 951956)

10. DIN Deutsches Institut für Normung e. V.
11. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
12. Hanse Aerospace Wirtschaftsdienst GmbH
13. Information Catalyst for Enterprise Ltd.
14. Jotne IT
15. Kyklos 4.0 (H2020 – No 872570)
16. Salzburg Research Forschungsgesellschaft m.b.H.
17. SRDC Software Research & Development and Consultancy Corp.
18. Walter Otto Müller GmbH & Co. KG
19. ZDMP Project (H2020 – No 825631)

The process of elaborating the CEN-CENELEC Workshop Agreement (CWA) EFPFInterOP is illustrated in the figure below.

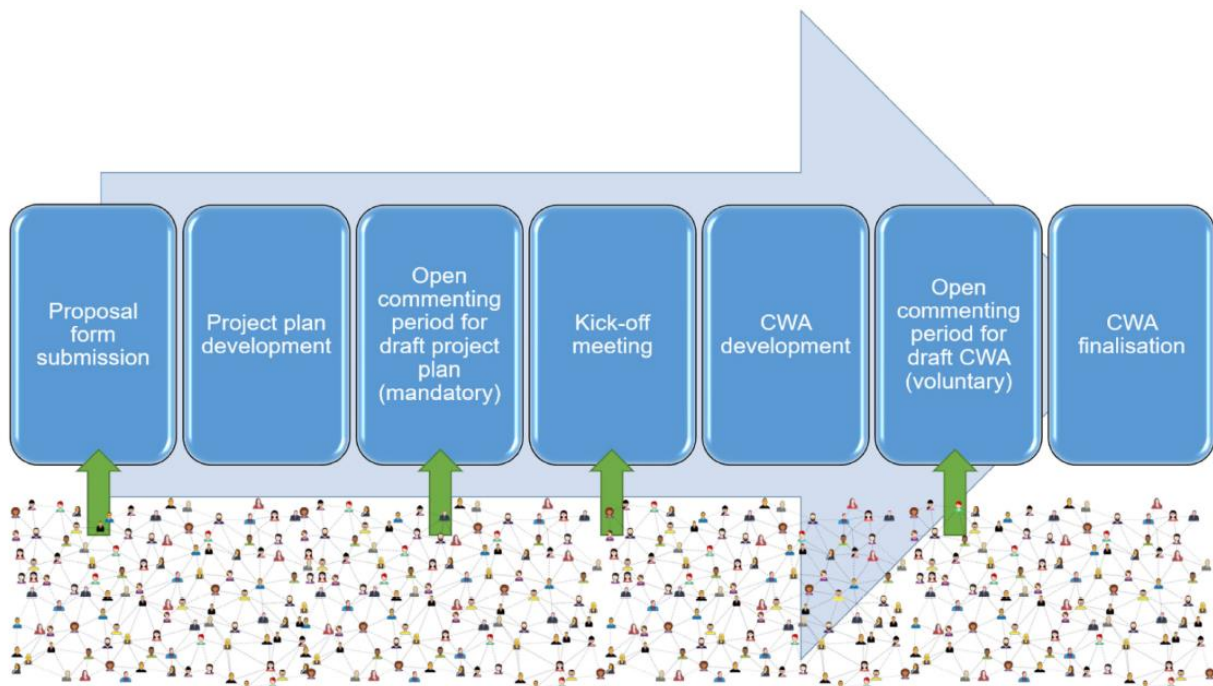


Figure 5: Illustration of the CWA process

The CWA was elaborated in twelfth CEN-CENELEC Workshop meetings and several topic dedicated focus meetings between those regular workshop meetings.

At the 11th Workshop meeting, which was held on 22. June 2022, the Workshop participants unanimously decided to forward the draft CWA, European Connected Factory Platform for Agile Manufacturing Interoperability (EFPFInterOp), due to its maturity to the open commenting phase. The start of this open commenting period was announced on the CEN-CENELEC website as illustrated in the figure below on 4. July 2022. The information about this announcement was disseminated to the target audiences through the channels of EFPF, its individual partners, EFFRA contacts as well as those of the national CEN members, e.g. social media.

The Czech Office for Standards, Metrology and Testing (UNMZ) and Hanse Aerospace Wirtschaftsdienst GmbH (HAW) provided comments on the draft CWA. These comments were resolved by unanimity at the 12th Workshop meeting, which was held on 19. October 2022.

POSTED: 2022-07-04

Draft CEN-CENELEC CWA on 'European Connected Factory Platform for Agile Manufacturing Interoperability (EFPFInterOp)'

Workshop

CEN-CENELEC

The European, as well as the global, B2B platform landscape is characterized by a high proliferation and fragmentation of diverse solutions with few signs of consolidation. Success of a B2B platform economy requires commercial platforms to be collaborative, simple, scalable, secure, and trusted.

The manufacturing industry needs interoperability, simplification, and openness to seamlessly engage with B2B platforms, to fulfil their business operations with different partners and customers in their value networks. One way to meet the needs of the manufacturing industry is a federated digital manufacturing platform with embedded intelligence and integrated tools and services to significantly reduce the burden of setting up collaborative networks, shorten the time to respond to new business opportunities and simplify the management and control of distributed processes.

To solve this issue is the primary objective of the CEN-CENELEC Workshop EFPFInterOp. The proposer of the workshop is the Horizon 2020 project EFPF. The secretariat holder of this workshop is Austrian Standards International, ASI.

This Draft CEN-CENELEC Workshop Agreement (CWA) defines a reference architecture for federating manufacturing platforms focusing on the interoperability on Service-Oriented Architecture (SOA), Protocol, Security and Data Model level. Additionally, a reference implementation in the form of the EFPF Data Spine and associated components will be described including Best Practices identified.

The draft CWA 'European Connected Factory Platform for Agile Manufacturing Interoperability (EFPFInterOp)' is now available for commenting. You are kindly invited to submit comments on the draft CWA to **Lorenz MARTIN**, using the below commenting form by **Friday, 5 August 2022**.

Download the documents:

- [Draft CWA for commenting](#)
- [Commenting Form](#)



TAGS: CWA | Digital

Figure 6: Announcement of the open commenting period for draft CWA EFPFInterOp⁸

In line with CEN-CENELEC Guide 29 the CEN-CENELEC Workshop Chair – having observed that there are no sustained objections from the CEN-CENELEC Workshop participants and all comments have been resolved – decided, the CWA is approved and can be submitted for publication. This decision was taken by unanimity.

In agreement with the CEN CENELEC Management Centre the CWA EFPFInterOp – to which the official reference number CWA 17907 was allocated by CCMC – will be made publicly available from the CEN Website <https://www.cencenelec.eu/get-involved/research-and-innovation/cen-and-cenelec-activities/cwa-download-area/> for free download following the prepayment policy of CEN-CENELEC Guide 10, Article 8.

On 23. November 2022 CWA 17907 was made available for free download from https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/RI/cwa17907_2022.pdf.

The purpose of CWA 17907 is to provide a blueprint of a federation platform and to describe components and functionalities that reduces the barrier to innovation by providing seamless access to services and solutions through an open platform. The creation of a federated ecosystem of IoT

⁸ <https://www.cencenelec.eu/news-and-events/news/2022/workshop/2022-07-04-efpfinterop/>

platforms of companies in the manufacturing domain can help companies form agile, ad-hoc collaborative networks, establish dynamic supply chains, and optimize production processes to meet such market demands as lot-size-one manufacturing.

In CWA 17907 a reference architecture for federating manufacturing platforms focusing on the interoperability on Service-Oriented Architecture (SOA), Protocol, Security and Data Model level is defined. Additionally, a reference implementation in the form of the EFPF Data Spine and associated components is described including Best Practices identified.

The Table of Content is provided in the figure below.

Contents	Page
European foreword	3
Introduction	4
4.1 Interoperability Approach	7
4.2 High-level Functional Requirements	7
5.1 Introduction	10
5.2 Data Spine	13
5.3 Marketplace	25
5.4 Portal	28
5.5 Matchmaking	29
6.1 Data Spine	34
6.2 Marketplace	37
6.3 Portal	41
6.4 Matchmaking	43
Annex A (informative) Best Practices / Lessons Learned	47
A.1 Real World Example – Furniture Pilot	47
A.2 Real World Example – Circular Economy Pilot	54
A.3 Real World Example – Aerospace Pilot	58
Bibliography	66

Figure 7: Table of Content of CWA 17907:2022

3.4 Digital Manufacturing Platforms for Connected Smart Factories

In order to ensure that EU-funded projects in the area of digital manufacturing platforms (DMP) are coordinated accordingly, EFPF is an active partner within Digital Manufacturing Platforms for Connected Smart Factories.

The aim of the DMP cluster is to identify, present and use synergies between the projects.

As a first step, a working group for standardisation activities was established and the results of the individual projects were compared in order to show which common standards are used by the projects. For a comparable overview, the standards were mapped to the Reference Architectural Model Industry 4.0 (RAMI 4.0).

The results will be published on the website of the European Factories of the Future Research Association (EFFRA), see www.effra.eu/.

3.5 Dissemination of EFPF goals in other fields of the standardisation network

ASI has raised awareness of EFPF in the standardisation communities by nominating the project for the European Standards+Innovation Awards 2021⁹ and for the Austrian Standards Living Standards Awards 2022¹⁰.

EFPF's CEN/CLC/WS *EFPFInterOp on European Connected Factory Platform for Agile Manufacturing Interoperability* is mentioned in the European Commission's 2022 Rolling plan for ICT standardisation¹¹ (Clause 3.4.6) as standardisation activity related to Digitisation of European Industry.

⁹ See <https://www.cencenelec.eu/get-involved/research-and-innovation/cen-and-cenelec-activities/standards-innovation-awards/list-of-nominees-2021/>

¹⁰ See <https://www.austrian-standards.at/de/innovation/living-standards-award>

¹¹ See <https://ec.europa.eu/docsroom/documents/49834>

4 Strategy on Regulations

It is important for all project partners to know which regulations need to be followed both, during the design and development of the platform, as well as for its operation. The following regulations were identified by the partners¹²:

- 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 (General Data Protection Regulation)
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union
- 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 526/2013 (Cybersecurity Act)
- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
- REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC
- 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
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
- COMMISSION REGULATION (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013
- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services
- DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC – Machinery directive
- DIRECTIVE 2014/53/EU - Radio Equipment Directive (RED)
- EU regulation 185/2010, laying down detailed measures for the implementation of the common basic standards on aviation security
- The Directive on security of Network and Information Security (NIS Directive) [5]
- National Cybersecurity Strategies (NCSS) by ENISA [7]
- Incident notification for DSPs in the context of the NIS Directive [9]
- Technical Guidelines for the implementation of minimum security measures for Digital Service

¹² Survey responses related to standards, which are used for contractual purposes, were omitted.

Providers (DSP) [10]

- Ethical Trading Initiative (ETI)/ business ethics
- Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI set by the EC [12]
- Ethically Aligned Design (EAD) [13]
- EU regulation No. 428/2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
- EU regulation No. 1907/2006, Reach (Registration, Evaluation, Authorisation and Restriction of Chemicals)
- EU regulation No. 2011/65/EU, Restriction of Hazardous Substances (RoHS)
- Conflict Minerals (On 1 January 2021 a new law will come into full force across the EU – the Conflict Minerals Regulation)
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 (COM/2022/71 final)
- Royal Decree 8/2020 [2]
- Royal Decree 488/1997 of April 14th [3]
- Royal Decree 486/1997 of April 14th [4]
- Benelux-verdrag inzake de intellectuele eigendom (NL)
- BGBl. I Nr. 66/2002, Federal Law on the Granting of Privileges to Non-Governmental International Organisations (national Austrian law)
- EASA Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25/EASA Part 21G, Section A, Subpart G “Production Organisation Approval”/ EASA Part 21J, Section A, Subpart J “Design Organisation Approval”/EASA Part 145 “Approved Maintenance Organisation”
- Regulations regarding social responsibility, such as UN Global Compact, OECD-Guidelines, SA 8000, UN Guiding Principles on Business and Human Rights

Special attention needs to be given to those regulations with a link to standards. Especially New Legal Framework (NLF) directives/regulations of the European Union foresee a strong link with standards. These standards are elaborated based of a standardisation request from the European Commission and gain the status of harmonized European Standards (hEN). Such NLF regulations are for instance the medical devices regulation, Machinery Directive and the Radio Equipment Directives.

On 21. April 2021 the European Commission proposed new rules and actions aiming to turn Europe into the global hub for trustworthy Artificial Intelligence (AI)¹³. The combination of the first-ever legal framework on AI and a new Coordinated Plan with Member States will guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU. New rules on Machinery will complement this approach by adapting safety rules to increase users' trust in the new, versatile generation of products. The proposed EU-Regulation on machinery products [15] – being foreseen as the revision of the Machinery Directive – is coherent with the Union policy on artificial intelligence (AI) and the upcoming Regulation on

¹³ See https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

artificial intelligence, which will address the risks having an impact on safety for high-risk AI systems embedded in a machinery or that are safety components under the future regulation on machinery products. In addition, this proposal is coherent with the Union policy on cybersecurity, making the link with the future cybersecurity schemes pursuant to Regulation (EU) 2019/881 for the purpose of demonstrating compliance with the future regulation on machinery products. Both proposed EU-Regulations – AI and Machinery products – are New Legal Framework (NLF) regulations.

5 Summary

Standardisation is of a special importance in supporting the digital transformation of industrial domains. Standardisation is the powerful tool of the technological and economic infrastructure that greatly influences competitive abilities and the strategies of companies.

Therefore, it is important for all project partners to recognise the benefits of standardisation and to address findings that could improve the European and global framework of standards.

Digital transformation of industry is not happening in a regulation-free environment. Legal compliance is a must. This is valid not only in a physical world but for digitisation of industry as well. Therefore, it is essential for all project partners to know which regulations need to be followed during the design and development of the platform as well as for its operation.

Based on the standardisation plan (D11.11) and extensive surveys, this deliverable of task T11.3 provides a detailed overview of the EFPF partners' participation in standardisation activities and on regulations that affect EFPF. The standardisation strategy is divided in three parts:

- The involvement in standardisation committees elaborating standards for strategic areas enables an optimum alignment between EFPF tools and related standards but needs to be regularly monitored and updated.
- The participation in strategic standardisation groups enhances the visibility of EFPF among key stakeholders and facilitates the access to first-hand information being highly relevant for the project.
- The concept of a CEN-CENELEC Workshop Agreement as a standardisation deliverable supports directly EFPF as a digital platform ecosystem. The concept was implemented and the work in CEN-CENELEC Workshop EFPFInterOp was completed – together with related Digital Manufacturing Cluster projects such as ZDMP. The process of elaboration a CEN-CENELEC Workshop Agreement (CWA 17907) has been proven to be successful to raise the attention of stakeholders about EFPF, to attract stakeholders – next to those being project partners – to participate in the drafting of the CWA and thereby contributing to achieve the project's overall objectives.

The subsequent work in T11.3 and the deliverable **D11.9** (final report) built on D11.11 and this deliverable, leading to a visible final impact of the EFPF project in the wider area of standardisation and to legal compliance with identified regulations.

Annex A: History

Document History	
Versions	<p>V1.0: final version of the deliverable</p> <p>V0.8: ASI draft deliverable with comments from reviewers (AID, IEC)</p> <p>V0.7: ASI draft deliverable with updated input from partners (FOR, HAW, NXW)</p> <p>V0.4: ASI draft deliverable with updated input from partners</p> <p>V0.3: ASI draft deliverable with updated list of standards and regulations</p> <p>V0.2: ASI draft deliverable with updated input from partners (CNET, FOR, HAW, ICE)</p> <p>V0.1: ASI draft deliverable with updated input from partners</p>
Contributions	<p>ASI:</p> <ul style="list-style-type: none"> • Andreas Feigl • Karl Grün • Erwin Haubert • Martin Lorenz <p>ICE:</p> <ul style="list-style-type: none"> • Usman Wajid • Cesar Marin <p>ASC:</p> <ul style="list-style-type: none"> • Norman Wessel <p>C2K</p> <ul style="list-style-type: none"> • Simon Osborne <p>FIT</p> <ul style="list-style-type: none"> • Alexander Schneider <p>NXW</p> <ul style="list-style-type: none"> • Ali Nejabati, Erin Seder <p>SRFG</p> <ul style="list-style-type: none"> • Violeta Damjanovic-Behrendt <p>SRDC:</p> <ul style="list-style-type: none"> • Yildiray Kabak <p>FOR:</p> <ul style="list-style-type: none"> • Nisrine Brouhanna, Rute C. Sofia <p>CNet:</p> <ul style="list-style-type: none"> • Mathias Axling <p>HAW:</p> <ul style="list-style-type: none"> • Ingo Martens <p>A-D:</p>

- Berend Koch

IAI:

- Lars Henschel

CERTH:

- Alexandros Nizamis

Annex B: References

- [1] GDPR: 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 (General Data Protection Regulation)
- [2] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3824
- [3] <https://www.boe.es/eli/es/rd/1997/04/14/488/con>
- [4] <https://www.boe.es/eli/es/rd/1997/04/14/486/con>
- [5] The Directive on security of Network and Information Security (NIS Directive). Online: <https://ec.europa.eu/digital-single-market/en/network-and-information-security-NIS-directive>
- [6] Guideline on Notifications of DSP Incidents (formats and procedures), 2018. Online: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675.
- [7] ENISA, National Cybersecurity Strategies (NCSS) by ENISA; <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools>
- [8] ENISA, Good Practices in Innovation on Cybersecurity under the NCSS, 2019.
- [9] ENISA, Incident notification for DSPs in the context of the NIS Directive, 2017. ONLINE: <https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive>
- [10] ENISA, Technical Guidelines for the implementation of minimum security measures for Digital Service Providers (DSP), 2017. Online: <https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>
- [11] New Guide Supports Companies in Upholding Freedom of Associations. Online: <https://www.ethicaltrade.org/blog/new-guide-supports-companies-upholding-freedom-association> (last accessed: 15-May-2020)
- [12] Ethics Guidelines for Trustworthy AI, by Independent High-Level Expert Group (HLEG) on AI. Online: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- [13] Ethically Aligned Design (EAD). Online: <https://ethicsinaction.ieee.org>
- [14] Digital Markets Act (DMA), Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
- [15] Proposal for a Regulation of the European Parliament and of the Council on machinery products, Online: <https://ec.europa.eu/docsroom/documents/45508>
- [16] White Paper: Applying MQTT Sparkplug in the EFPF Platform, Nisrine Bnouhanna, Rute C. Sofia, Edoardo Pristeri, February 2022, Online: https://www.researchgate.net/publication/358618553_White_Paper_Applying_MQTT_Sparkplug_in_the_EFPF_Platform

- [17] Study on "Support to the observatory for the online platform economy", Final report, Online: <https://op.europa.eu/en/publication-detail/-/publication/ee55e580-ac80-11eb-9767-01aa75ed71a1/language-en/format-PDF/source-206332284>
- [18] CEN-CENELEC Guide 10, Policy on dissemination, sales and copyright of CEN-CENELEC Publications, <https://www.cencenelec.eu/media/Guides/CEN-CLC/cenclcguid10.pdf>
- [19] CEN-CENELEC Guide 29, Workshop. Agreements – A rapid way to standardisation, <https://www.cencenelec.eu/media/Guides/CEN-CLC/cenclcguid29.pdf>



European Factory Platform

www.efpf.org