This project has received funding from the European's Union Horizon 2020 research innovation programme under Grant Agreement No. 957258

Architecture for Scalable, Self-human-centric, Intelligent, Secure, and Tactile next generation IoT

assist-iot

D9.4 Report on Contribution to Standardisation and International Fora - Final

Deliverable No.	D9.4	**Due Date**	31-Mar-2024
Type	Report	**Dissemination Level**	Public
Version		**WP**	WP9
Description	Report on actions undertaken by the Consortium - standardisation activities and contributions to various SDOs and international fora.		

Copyright

The ASSIST-IoT consortium consists of the following 15 partners:

UNIVERSITAT POLITÈCNICA DE VALÈNCIA	Spain
PRODEVELOP S.L.	Spain
SYSTEMS RESEARCH INSTITUTE POLISH ACADEMY OF SCIENCES IBS PAN	Poland
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	Greece
TERMINAL LINK SAS	France
INFOLYSIS P.C.	Greece
CENTRALNY INSTYUT OCHRONY PRACY	Poland
MOSTOSTAL WARSZAWA S.A.	Poland
NEWAYS TECHNOLOGIES BV	Netherlands
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	Greece
KONECRANES FINLAND OY	Finland
FORD-WERKE GMBH	Germany
GRUPO S 21SEC GESTION SA	Spain
TWOTRONIC GMBH	Germany
ORANGE POLSKA SPOLKA AKCYJNA	Poland

Disclaimer

Authors

Name	Partner	e-mail
Ignacio Lacalle Úbeda	P01 UPV	iglaub@upv.es
Alejandro Fornés Leal	P01 UPV	alforlea@upv.es
Carlos Guardiola García	P01 UPV	carguaga@upv.es
Marcin Paprzycki	P03 IBSPAN	paprzyck@ibspan.waw.pl
Evripidis Tzionas	P04 CERTH	tzionasev@iti.gr
Francisco Blanquer	P05 TL	HO.FBLANQUER@terminal-link.com
Anna Dąbrowska	P07 CIOP-PIB	andab@ciop.lodz.pl
Piotr Dymarski	P08 MOW	P.Dymarski@mostostal.waw.pl
Johan Schabbink	P09 Neways	Johan.Schabbink@newayselectronics.com
Oscar López Pérez	P13 S21SEC	olopez@s21sec.com
Zbigniew Kopertowski	P15 OPL	zbigniew.Kopertowski@orange.com

History

Date	Version	Change
18-Dec-2023	0.1	ToC closed, initial partners assignment
31-Jan-2024	0.2	First round of contributions
29-Feb-2024	0.3	Final round of contributions
4-Mar-2024	0.4	Pre-final version for review
15-Mar-2024	1.0	Final version

Key Data

Keywords	Standardization, IoT
Lead Editor	P15 OPL – Zbigniew Kopertowski
Internal Reviewer(s)	TL, FORD

Executive Summary

This deliverable is written in the framework of WP9 of **ASSIST-IoT** project under Grant Agreement No. 957258. The document presents the standardisation activities performed in the project. The deliverable includes analysis of standardisation bodies and pre-normative initiatives work, working areas, recommendations and reports regarding relevant aspects for the project and new standardisation subjects with focus on the ongoing work. The most interesting from the project point of view are **ETSI, ITU-T, IEEE SA** standardisation organisations as well as initiatives like **AIOTI, ECSO, ENISA and TIC4.0.** Next, the ASSIST-IoT standardisation activities related to the designed in the project solutions are presented. We grouped the activities in the following domains:

- Internet of Things, IoT Use Cases
- Networking and Edge Cloud,
- Cybersecurity,
- Artificial Intelligence.

According to the committed goals of WP9, the objective of T9.3 is to follow up the standardisation activities in the above domains, analyse the gaps in the standardisation documents, analyse ongoing work for selected SDOs and initiatives and contribute to selected technical subjects.

The results of the **standardisation activities per specified in the project proposal standardisation KPIs,** with detailed description of activities, standards and contributions were presented. Finally, evaluation of the activities in terms of achieved KPIs were included. **All KPIs exceeded the assumed targeted values**, where contributions to the recommendations, technical reports and white papers are more than twice larger than planned one.

Finally, at the end of the deliverable a short summary of the standardisation work is presented.

Table of contents

List of tables 6
List of figures 6
List of acronyms 7
1. About this document 11
1.1. Deliverable context 11
1.1. The rationale behind the structure 11
2. Standardisation landscape 12
2.1. ETSI: European Telecommunications Standards Institute 12
2.2. ITU-T: International Telecommunication Union Telecommunication Standardisation Sector 14
2.2.1. SG13 Future networks 15
2.2.2. SG17 Security 15
2.2.3. SG20 IoT, smart cities & communities (SC&C) 16
2.3. IEEE SA: Institute of Electrical and Electronics Engineers Standards Association 17
2.4. AIOTI: Alliance of Internet of Things Innovation 19
2.5. BDVA: Big Data Value Association 20
2.6. ECSO: European Cybersecurity Organization. 21
2.7. ENISA: European Network and Information Security Agency 21
2.8. TIC4.0: The Terminal Industry Committee 4.0 23
2.9. DG GROW - DG for Internal Market, Industry, Entrepreneurship and SMEs 24
2.10. Other standardisation organisations, forums and initiatives 25
3. ASSIST-IoT standardization activities 27
3.1. ASSIST-IoT technical domains 27
3.1.1. Internet of Things domain 27
3.1.2. Networking and edge cloud domain 28
3.1.3. Cybersecurity domain 29
3.1.4. Artificial Intelligence domain 29
3.1.5. Activities summary per technical domain 29
3.2. Standardization activities in the project 30
3.2.1. Strategy review 30
3.2.2. Communications to modify / improve existing standards used in ASSIST-IoT 31
3.2.3. Recommendations in relevant SDOs and initiatives 32
3.2.4. SDOs and pre-normative initiatives engaged 36
3.2.5. Supported standards 38
3.2.6. Identified standards 41
3.2.7. Activities summary vs KPIs 47
4. Standardization activities summary 48
5. References 50

List of tables

Table 1. Standardisation activities in technical domains 30
Table 2. Identified standards to modify/improve 31
Table 3. Activities/contributions to recommendations 32
Table 4. SDOs/Initiatives engaged 36
Table 5. Supported standards 38
Table 6. List of identified standards related to ASSIST-IoT 41
Table 7. Standardisation activities KPIs 47

List of figures

Figure 1. TIC 4.0 members 23
Figure 2. TIC 4.0 definition process 24
Figure 3. Strategy and target KPIs for standardisation activities 31
Figure 4. Estimated standardisation effort per technical domain 48
Figure 5. Estimated standardisation effort per SDO/initiative 48

List of acronyms

Acronym	Explanation
3GPP	3rd Generation Partnership Project
5G	5th Generation
5G IA	5G Infrastructure Association
5G PPP	5G Public-Private Partnership
AGVES	Advisory Group on Vehicle Emission Standards
AI	Artificial Intelligence
AIOTI	Alliance for Internet of Things Innovation
ANSI/ISA	American National Standards Institute / International Society of Automation
API	Application Programming Interface
BBF	Broadband Forum
BDVA	Big Data Value Association
CAN-Bus	Controller Area Network Bus
CEF	Connecting Europe Facility
CENELEC	European Committee for Electrotechnical Standardization)
CEN	European Committee for Standardization
CHE	Container Handling Equipment
CIS	Controls IoT Security
CNFs	Cloud-Native Network Functions
CoAP	Constrained Application Protocol
cPPP	contractual Public-Private Partnership
CPS	Cyber-Physical Systems
CSF	Cybersecurity Framework
CT	Core Network & Terminals
DAIRO	Data, AI and Robotics
DCSA	Digital Container Shipping Association
DDoS	Distributed Denial Of Service
DevOps	Development and Operations
DINRG	Decentralized Internet Infrastructure Research Group
DLT	Distributed Ledger Technology
DMT	Device Management Tree
DoA	Description of Action
DOTS	DdoS Open Threat Signalling
DSBA	Data Spaces Business Alliance

Dx.y	Deliverable No y of Work Package x
EC	European Commission
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EFRA	European Factories of the Future Research Association
EFTA	European Free Trade Association
ENI	Experiential Networked Intelligence
ENISA	European Union Agency for Cybersecurity
EOSC	European Open Science Cloud
ESCO	European Cyber Security Organisation
ETSI	European Telecommunications Standards Institute
FG-AN	Focus Group on Autonomous Networking
FG-ML5G	Machine Learning for Future Networks including 5G
FIWARE	Future Internet open-source platform
GA	General Assembly
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications
HLA	High Level Architecture
HMI	Human-Machine Interfaces
HWG	Horizontal Working Group
I2NSF	Interface to Network Security Functions
I2RS	Interface to the Routing System
IEEE	Institute of Electrical and Electronics Engineers
IEEE SA	Institute of Electrical and Electronics Engineers Standards Association
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIRA	Industrial Internet Reference Architecture
IMT	International Mobile Telecommunications
IoT	Internet of Things
IPTV	Internet Protocol Television
IRTF	Internet Research Task Force
ISG	Industry Specification Group
IT	Information Technology
ISO	International Organization for Standardisation
ITU-T	International Telecommunication Union Telecommunication
JCT	Joint Technical Committee

JIEP	Joint and Individual Exploitation Plan(s)
KPI	Key Performance Indicator
KVI	Key Validation Indicator
LoRaWAN	Long Range Wide Area Network
LWM2M	LightWeight M2M
M2M	Machine to Machine
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning
MLOps	Machine Learning Operations
MQTT	MQ Telemetry Transport
MS	Milestone
MVP	Minimum Viable Product
NGIoT	Next Generation Internet of Things
NFV	Network Function Virtualization
NGO	Non-Governmental Organisation
NIST	National Institute of Standards and Technology
NMRG	Network Management Research Group
OASIS	Organization for the Advancement of Structured Information Standards
OBM	On-Board Monitoring
OGC	Open Geospatial Consortium
ONF	Open Networking Foundation
OPC-UA	Open Platform Communications Unified Architecture
OPNVF	Open Platform Network Function Virtualization
OSGi	Open Services Gateway initiative
OSM	Open Source MANO
PC	Project Coordinator
PDL	Permissioned Distributed Ledge
PoC	Proof-of-Concept
PPP	Public Private Partnership
PROFIBUS	Process Field Bus
PROFINET	Process Field Net
RA	Reference Architecture
RAMI 4.0	Reference Architectural Model Industry 4.0
RAN	Radio Access Networks

REST	REpresentational State Transfer
RTO	Research and Technology Organisations
SA	Service & Systems Aspects
SACM	Security Automation and Continuous Monitoring
SAI	Securing Artificial Intelligence
SAREF	Smart Applications Reference Ontology
SC&C	Smart Cities & Communities
SDN	Software Defined Networks
SDO	Standardisation Organisation
SG	Standardisation Group or Study Group
SP	Special Publication
SRIA	Strategic Research and Innovation Agenda
SRIDA	Strategic Research, Innovation and Deployment Agenda
SSN	Semantic Sensor Network
STF	Standardisation Task Force
Telco	Teleconference
TF	Task Forces
TIC	Terminal Industry Committee
TLS	Transport Layer Security
TM	Traffic Management
TOS	Terminal Operating System
TSG	Technical Specification Groups
Tx.y	Task No y of Work Package x
VWG	Vertical Working Group
W3C	World Wide Web Consortium
WG	Working Group
WPx	Work Package No x
XACML	Xtensible Access Control Markup Language

1. About this document

The main objective of this document is to present the standardisation activities carried out in WP9 and T9.4 – Standardisation and pre-normative Activities.

1.1. Deliverable context

Keywords	Description
Objectives	Objective 8: Impact creation, Showcasing ASSIST-IoT, and Disrupting the current market. ASSIST-IoT will track relevant standards bodies to be compliant with them and, at further stages of the project, provide influence to standards filling the gaps they may have, which the action identifies.
Work plan	This deliverable is final in WP9 and directly linked to T9.3 – Standardisation and Pre-normative Activities.
Milestones	N/A
Deliverables	D9.4 provides a comprehensive description of standardisation activities results, analysis of work in SDOs and pre-normative initiatives, standardisation gaps analysis, achievements in the standardisation work, evaluation of the work using KPIs.

1.2. The rationale behind the structure

This document is divided into 4 sections, which present standardisation work carried out in the project. In detail:

Section 1: Introduces the reader to the objectives and scope of this document and its format.

Section 2: Presents standardisation landscape by analysis of standardisation bodies and initiatives like ETSI, ITU-T, IEEE SA, AIOTI, BDVA, ECSO, ENISA and TIC4.0, on which was focused our attention, as well other organisation.

Section 3: Describes ASSIST-IoT standardisation activities performed during the project including:

- Relevant contributions domains, which are related to technical solutions designed in the project like Internet of Things, Artificial Intelligence, Cybersecurity, Networking and Edge Cloud domain.
- Description of standardisation activities details per each KPI.
- Evaluation of performed standardisation activities using KPIs.

Section 4: This section concludes the document and summarises achieved results.

2. Standardisation landscape

In middle of the project in D9.3 the description and analysis of the different SDOs and standardisation initiatives most relevant to the project subjects were presented. Currently, we present the updated analysis of the standardisation activities with focus on main organisations most active in the subjects in different technical domains of the project scope like: IoT solutions, edge computing, data management, networking, cybersecurity, artificial intelligence as well as for use case specific subjects like: port logistics, safety at work and construction modelling. Below the analysis of the following organisations is presented:

- **ETSI -** European Telecommunications Standards Institute,
- **ITU-T -** International Telecommunication Union Telecommunication Standardisation Sector,
- **IEEE SA -** Institute of Electrical and Electronics Engineers Standards Association,
- **AIOTI -** Alliance for Internet of Things Innovation,
- **BDVA -** Big Data Value Association,
- **ECSO** - European Cybersecurity Organization,
- **ENISA -** European Network and Information Security Agent,
- **TIC4.0 -** Terminal Industry Committee 4.0,
- **Other** (ISO/IEC, 3GPP, 5G PPP, W3C, IETF).

2.1. ETSI: European Telecommunications Standards Institute

From ETSI activities analysis we selected and focused on Specification Groups most relevant to ASSIST-IoT project results areas like in IoT, AI, Networks and Security Sectors. Several **ETSI Industry Specification Groups (ISG)** were selected, either in the form of direct content for their specifications and reports, or by means of PoC-based (Proof-of-Concept) analysis of their specifications. In particular:

- **SmartM2M** (with applications in IoT, security in IoT, semantic interoperability, smart M2M communications),
- **ENI** (dedicated to exploring data-intensive, policy-based, AI-enabled network management techniques),
- **MEC** (with the goal of defining an architecture and easy cloud and IT resources at the network edge),
- **PDL** (standardizing best practices and technologies in permissioned DLT),
- **NFV** (focused on Network Function Virtualization orchestration, management, security and reliability),
- **CYBER** (market-driven cybersecurity standardization solutions, along with advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators),
- **SAI** (where security implications of applying AI are being considered) are the most promising objectives).

ETSI produces specifications, standards, reports and guides, each with its own purpose. ETSI is releasing Technical Specifications (TS), Technical Reports (TR), Group Specifications (GS), Group Reports (GR) and Special Reports (SR) in different above technical domains. The full list of the relevant ETSI documents is included in chapter 3.2.6 of this report.

In the main areas of interest in our project the following ETSI activities were most relevant to analyse:

- SmartM2M Technical Committee includes:
  - SAREF Guidelines for IoT Semantic Interoperability; EN 303 760 DEN/SmartM2M-303760
  - Use cases for cross-domain data usability of IoT devices (ASSIST-IoT contribution), ETSI TR 103 778 V1.1.1 (2021-12).
  - Develop, apply and evolve Smart Applications ontologies Smart Applications; Reference Ontology and oneM2M Mapping.
  - oneM2M deployment guidelines and best practices.

- NFV Industry Specification Group
  - Network Functions Virtualisation (NFV) Release 5; Security Assurance Specification (SCAS) for Generic NFV-MANO, GS NFV-SEC 028 DGS/NFV-SEC028ed511
  - Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification, GS NFV-IFA 040 RGS/NFV-IFA040ed511
  - Management and Orchestration; Report on Management and Orchestration Framework, GR NFV-MAN001 RGR/NFV-MAN001ed121

- ENI Industry Specification Group (see also in [1][2]) includes:
  - ENI Use Cases, GS ENI 001 RGS/ENI-001v411_Use_Cases
  - ENI Requirements, GS ENI 002 RGS/ENI-002v411_Requirements
  - ENI System Architecture, GS ENI 005 RGS/ENI-005v411_Sys_Arch
  - Evaluation of categories for AI application to Networks, GR ENI 010 RGR/ENI-0010v121 AI_App_Net
  - Definition of data processing mechanisms, GS ENI 009 RGS/ENI-009v411 Data Mechanism

- MEC Industry Specification Group includes:
  - Study on Distributed Edge Network, GR MEC 047 DGR/MEC-0047v411DistEdgeNet
  - Framework and Reference Architecture - to align the MEC architecture with the other MEC specifications, GS MEC 003 RGS/MEC-0003v321Arch
  - General principles, patterns and common aspects of MEC Service APIs, GS MEC 009 RGS/MEC-009v411ApiPrinciples
  - Study on MEC Security - cover the themes of application and platform security, Zero-Trust Networking, and security requirements for MEC Federations, GR MEC 041 DGR/MEC-0041v311MECSecurity
  - Study on MEC Application Slices - study the potential requirements and enhancements to the MEC system needed to support MEC Application Slices, GR MEC 044 DGR/MEC-0044v311MECAppSlices

- PDL Industry Specification Group includes (see also [3]):
  - PDL, Study on Utilising PDL to Standardized IoT Service Layer Platform oneM2M, GR PDL 028 DGR/PDL-0028_Study_SLP_oneM2M
  - Development of the Reference Architecture Framework, GS PDL 012RGS/PDL-0012v121 Ref Arch
  - Use of PDL to support distributed data management, GR PDL 009 DGR/PDL-009_Fed_Data_Mgmt
  - Research Landscape - the exchange of information on PDL related research projects under the EU Horizon 2020 program with focus on permissioned distributed ledgers (PDL), Distributed

digital Ledger Technologies (DLT), and Blockchain work items, GR PDL 008 DGR/PDL-008_RaI_Landscape

2.2. ITU-T: International Telecommunication Union Telecommunication Standardisation Sector

ITU-T coordinates standards for telecommunications and Information Communication Technology between its Member States, Private Sector Members, and Academia Members. During the project different Study Groups (SG) of ITU-T were analysed, followed and actively contributed (in case of SG20). There are 11 SG where most relevant groups for project purposes are:

- **SG-13 Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures**: SG works on next-generation networks, while focusing on Future Networks (FN) and network aspects of mobile telecommunications. Standardization efforts are aiming to support network virtualization, energy saving for FNs, and an identification framework. Future plans are to develop different facets of the smart ubiquitous network, requirements of network virtualization for FNs, **framework of telecom SDN** (software-defined networking) and requirements of formal specification and verification methods for SDN. **Cloud computing** is an important part of SG13 work and the group develops standards that detail requirements and functional architectures of the cloud computing ecosystem, covering inter- and intra-cloud computing and technologies supporting XaaS (X as a Service). SG13 standardization work also covers network aspects of the **Internet of Things (IoT),** additionally ensuring support for IoT across FNs as well as evolving NGNs and mobile networks. **Cloud computing in support of IoT** is an integral part of this work. The recommendations released by SG13 taking into account ASSIST-IoT scope are listed in chapter 0.

- **SG17 Security,** ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups, often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia. SG17 works on cybersecurity, security management, security architectures and frameworks, countering spam, identity management, the protection of personally identifiable information, operational aspects of data protection, open identity trust framework; and quantum-based security; and Child Online Protection. SG17 also works on the security of applications and services **for the Internet of Things (IoT),** smart grid, smartphones, software defined networking, web services, big data analytics, social networks, cloud computing, mobile financial systems, IPTV, **distributed ledger technology**, intelligent transport system, telebiometrics, the combating of counterfeiting and mobile device theft, IMT-2020/5G, cloud-based event data technology, e-health, and Radio Frequency Identification. The recommendations from this SG is X.series and most relevant are listed in chapter 0.

- **SG20 IoT, smart cities & communities**, SG20 is focused on the **standardization requirements of Internet of Things** (IoT) technologies, starting work with IoT applications in smart cities and communities (SC&C). SG20 develops international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. Main part of work are **end-to-end architectures for IoT**, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors. The list of recommendations released in this SG in relation to ASSIST-IoT interest in chapter 0 is presented.

From point of view of the ASSIST-IoT project the ongoing analysed standardisation work and new work items in the ITU-T Study Groups are presented in the next subchapters.

2.2.1. SG13 Future networks

SG13 focus on IMT-2020, cloud computing and trusted network infrastructures and is working on the following subjects so called "Questions":

- Q2/13 (WP3/13) - Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network function virtualization (NFV). The Question addresses the support of emerging services and applications in NGNs evolving in a phased network evolution approach. Based on the use cases and related ecosystem aspects, this Question will study the requirements and capabilities imposed on evolving NGNs.
- Q6/13 (WP1/13) - Networks beyond IMT2020: Quality of Service (QoS) mechanisms development to support resource control and management for softwarized/virtualized networks and AI/machine learning based QoS/QoE assurance mechanisms.
- Q17/13 (WP2/13) - Future Networks: Requirements and capabilities for computing including cloud computing and data handling, overview, ecosystem, use cases, business roles and benefits from telecommunication perspectives. Define for future computing: requirements and capabilities, interoperability and data portability as well as the applications of future computing in vertical domains.
- Q18/13 (WP2/13) - Future Networks: Functional architecture for computing including cloud computing and data handling covering the identification of architectural functions, functional components, and their inter-relation required to provide future computing based services.
- Q19/13 (WP2/13) - Future Networks: End-to-end management, governance, and security for computing including cloud computing and data handling, developing overview, framework, high level and functional requirements and capabilities, data models for end-to-end service management and orchestration of future computing, including but not limited to Development and Operation (DevOps), continuous integration / continuous delivery (CI/CD), distributed/edge computing, computing aware networking and other cloud native related technologies.
- Q20/13 (WP1/13) - Networks beyond IMT-2020 and machine learning: Recommendations on the requirements and capabilities for networks beyond IMT-2020 including AI/ML based on the emerging service scenarios. Work on the framework and architecture design of networks beyond IMT-2020 including AI/ML, based on, not limited to, the above identified requirements, capabilities and gap analysis identified by Focus Group on Machine Learning for Future Networks including 5G.
- Q21/13 (WP1/13) - Networks beyond IMT-2020: Network softwarization considering open source activities, development and maintenance of Recommendations on requirements, functional architecture and mechanisms for network softwarization including generic SDN and their profiles for intent-based networking, network virtualization, network slicing, NFV and virtualized network applications supporting service requests over versatile kinds of networks; work on the management and orchestration of homogenous/heterogeneous types of softwarized infrastructure in both public and private networks by using enhanced APIs and AI-assisted functionalities.

2.2.2. SG17 Security

SG17 focus on security subjects like network security, services security including IoT, Cloud computing and big data infrastructure security, DLT, and is working on the following subjects so called "Questions":

- Q2/17 (WP2/17) - Security architecture and network security, studies and development of security architecture and framework, a trusted telecommunication network architecture, AI/ML in supporting the building of confidence and security in the use of ICT.
- Q6/17 (WP2/17) - Security for telecommunication services and Internet of Things (IoT) for providing comprehensive security solutions. Study and identify security issues and threats in secure telecommunication services and IoT, develop interconnectivity mechanisms utilizing AI/ML based technologies.

- Q8/17 (WP4/17) - Cloud computing and big data infrastructure security to identify security requirements and threats to secure cloud computing services, to define security architecture and to organize security functions, to define a strong, flexible security architecture and implementation for cloud computing systems.
- Q14/17 (WP4/17) - Distributed ledger technology (DLT) security, to define security aspects of applications and services based on DLT, to study and identify security issues and threats in applications and services based on DLT, to develop security mechanisms, protocols and technologies for applications and services based on DLT.

2.2.3. SG20 IoT, smart cities & communities (SC&C)

SG20 focus on IoT solutions and services, architectures, protocols, data analytics and is working on the following subjects called "Questions":

- Q1/20 (WP1/20) - Interoperability and interworking of IoT and SC&C applications and services, developing Recommendations, Supplements, Reports, Guidelines, etc. as appropriate on:
  - use cases for interworking of IoT and SC&C applications and services in different verticals;
  - interworking and interoperability requirements and architectures;
  - middleware and platforms for interworking and interoperability;
  - data sets and formats to enable data interoperability and semantic interoperability among various verticals;
  - implementation, deployment, operation and maintenance.

- Q2/20 (WP1/20) - Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies, focus on developing Recommendations, Reports, Roadmaps, Guidelines etc. including:
  - use cases of IoT and SC&C services and applications across different verticals;
  - ecosystem aspects taking into account business models and use cases;
  - common and specific requirements, capabilities and architectural frameworks enhanced by emerging technologies across different verticals;
  - related implementation, deployment, operation and maintenance, as well as Proof of Concepts.

- Q3/20 (WP1/20) - IoT and SC&C architectures, protocols and QoS/QoE focus on the following subjects:
  - studies on general reference models on IoT and vertical industry needs;
  - developing frameworks to identify the basic architectural compositions and views on IoT and SC&C;
  - identifying entities, their functions, and reference points required to provide support to IoT applications and services;
  - determining the requirements that the connectivity and protocols are intended to support;
  - identifying performance requirements of connectivity technologies that will enable them to meet the IoT and SC&C requirements.

- Q4/20 (WP1/20) - Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C focus on developing Recommendations, Supplements, Reports, Guidelines, etc. covering:
  - methodology for DPM concept building based on use cases, requirements analysis;
  - data value chain, data lifecycle, capabilities and functional architectures to support DPM including big data aspects for IoT and SC&C;

- data analytics and data sharing to support data-driven intelligent services and applications for IoT and SC&C;
- tools, mechanisms and standardized interfaces for data analytics and data sharing;
- DPM, data analytics and sharing with support of emerging technologies (e.g., blockchain, artificial intelligence and digital twin, etc.) in IoT and SC&C;
- governance, security, privacy protection and risk management for IoT and SC&C;
- trusted data and data quality management for IoT and SC&C.

- Q6/20 (WP2/20) - Security, privacy, trust and identification for IoT and SC&C focus on developing Recommendations, Reports, Guidelines, etc. as appropriate on:
  - authenticity, confidentiality, integrity, non-repudiation, and availability of IoT devices, systems, applications, protocols, platforms, and services;
  - security and trust provisioning in IoT both at the ICT infrastructure and future heterogeneous converged service environments;
  - security and trust provisioning in IoT services and applications for converged environments among stakeholders of different industries;
  - requirements to mitigate the risks and threats identified in IoT and SC&C systems and services;
  - technical measures to prevent compromise, and protect the integrity and privacy of IoT systems, applications, platforms, and services;
  - technical measures needed to support the protection of privacy in SC&C applications, services, and platforms;
  - methodologies to create trustworthiness in IoT & SC&C devices, systems, applications, protocols, platforms, and services;
  - security and trustworthiness in using Application Programming Interfaces (API);
  - block-chain based technologies and mechanisms to support security and trustworthiness;
  - machine learning and artificial intelligence (AI) technologies for supporting secured interoperability and trustworthiness in IoT & SC&C.

In SG20 the contribution to Q2 was prepared to modify ITU-T Y.4478, Y.IoT-SCS with requirements and functional architecture for smart construction site services and analysed Y.IoT-Vreqs about requirements and capability framework of the internet of things for vision.

2.3. IEEE SA: Institute of Electrical and Electronics Engineers Standards Association

IEEE is the world's largest professional association dedicated to advancing technology. IEEE comprises a lot of working groups associations that are focused in different areas. The IEEE Standards Association (IEEE SA), based in US, provides editorial draft development support to more than 500 Working Groups and covers almost all of the relevant IT-related (and specially, communications) areas.

IEEE also covers subjects for the Internet of Things (IoT), as demonstrated by the many ongoing activities of the IEEE Internet of Things Initiative. IEEE has a number of existing standards (closed and under development), activities, and events that are directly related to IoT aspects. Some key standards activities are:

- Architectural framework: The focus of IEEE P2413-2019 is to develop a standard for the architectural framework for the Internet of Things, which includes descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains.
- Harmonization and security of IoT: The IEEE 1451-99 is focused on developing a standard for harmonization of Internet of Things (IoT) devices and systems. This standard defines a method for data

sharing, interoperability, and security of messages over a network, where sensors, actuators and other devices can interoperate, regardless of underlying communication technology.

- Sensor Performance and Quality: IEEE 2700 proposes a common framework for sensor performance specification terminology, units, conditions and limits is provided. IEEE P2510 defines quality measures, controls, parameters and definitions for sensor data related to Internet of Things (IoT) implementations.

List of identified IEEE standards related to IoT in chapter 0 is presented.

There are currently 26 open projects related to IoT and 46 to cloud computing subjects (in phase of working group labour). Out of those, the most interesting for ASSIST-IoT to contribute even after the project end or to follow up are:

- *P3195 - Standard for Requirements for a Mid-Level Ontology and Extensions.* This standard specifies the requirements for a mid-level ontology and for the creation of conforming extensions and modules (i.e., subsets) therefrom. ASSIST-IoT is actively participating in this working group.
- *P2989 – Standard for Authentication in a Multi-server environment*. Although ASSIST-IoT has chosen the OAuth2 approach, the architecture considering different tiers of k8s nodes might be interested in the evolution of this standard project.
- *P2986 – Recommended Practice for Privacy and Security for Federated Machine Learning:* for both T5.2 (Federated Learning) and T5.4 (privacy-DLT) of ASSIST-IoT following of this standard.
- *P2304 – Standard for Cloud Computing Shared Function Model*: ASSIST-IoT strongly endorse cloud-native concepts and bring them towards the edge-cloud computing continuum (k8s, virtualization, microservices, centralised orchestration). Following outcomes of this standard.
- STUDY GROUP for collection, record, storage, and export of motor vehicle event data recorders (MVEDRs), related to pilot 3A of ASSIST-IoT.
- *P3123- Standard for Artificial Intelligence and Machine Learning (AI/ML) Terminology and Data Formats*. Interest to follow this work for partners of ASSIST-IoT involved in T5.2 enablers and also in various pilots.
- *P3129 – Standard for Robustness Testing and Evaluation of Artificial Intelligence (AI)-based Image Recognition Service* - This standard project is related with the image recognition methods and algorithms being developed in the context of pilot 3B - to follow up the work.
- *P3652.1 - IEEE Guide for Architectural Framework and Application of Federated Machine Learning,* in ASSIST-IoT was to analyse for Federated Learning designed solution.
- *P7030 - Recommended practice for Ethical Assessment of Extended Reality (XR) technologies*. Analysed for applicability for extended reality applications in pilots 1 and 2.

In addition, the project followed the work, announcements and forthcoming project submissions by the following Standards Committees (there are currently 107 of those):

- C/AISC Artificial Intelligence Standards Committee,
- C/BDL Blockchain and Distributed Ledgers,
- C/CCSC Cloud Computing Standards Committee,
- C/CPSC Cybersecurity and Privacy Standards Committee,
- C/LT Learning Technology,
- C/S2ESC Software & Systems Engineering Standards Committee,
- COM/EdgeCloud-SC Edge, Fog, Cloud Communications with IOT and Big Data Standards Committee,
- COM/NetSoft-SC Virtualized and Software Defined Networks, and Services Standards Committee,
- CTS/BSC Blockchain Standards Committee,
- IES/IES Industrial Electronics Society Standards Committee,
- IM/ST TC9 - Sensor Technology,

- VT/ITS Intelligent Transportation Systems,
- COM/MobiNet-SC/TI Mobile Communication Networks, OM/MobiNet-S.C., Standards Committee, Tactile Internet WG,
- COM/MobiNet-SC/IOTAF Security Assessment Framework for the IoT Application Deployments WG.

2.4. AIOTI: Alliance of Internet of Things Innovation

The Alliance of Internet of Things Innovation (AIOTI) was born in March 2015 driven by the need of a unifying element in the so-far heterogeneous field of IoT influence in the European Union, specially related to the public research scope.

It is a non-for-profit organisation based in Brussels (Belgium), which main goal is to serve as a reference organisation in Europe to all IoT innovation activities, connecting public research frameworks with private initiatives and global trends in the sector. Their main role is to bring together different entities in a single collaborative framework, organising events, generating whitepapers and guidelines and, all in all, funnelling European innovation in IoT.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving standardisation activities.

AIOTI is divided in Working Groups (WG) that are two-fold:

- Horizontal working groups (HWGs), that cover wide, transversal aspects of interest for the IoT community. Nowadays, there are 8 HWGs active:
  - **Digital for Green** to define IoT and edge computing technologies, added value and role towards European Green Deal -Fit for 55- in collaboration with VWGs like Energy, Buildings and Logistics and Mobility,
  - **Distributed Ledger Technologies** allowing the testbeds and application exchange between IoT in DLT and other initiatives like INATBA or Climate Chain Coalition,
  - **Innovation Ecosystems** bringing together innovative organisations supporting circular and European cross-sectorial data economy,
  - **Policy and Strategies** to react and participate on EU directives and consultations after reflecting IoT's role on those policies,
  - **Research and partnerships** to foster research community links, to maintain the Research and Innovation Agenda -SRIA- of EOSC and to organise the large participation of AIOTI in IoT Week,
  - **Standardisation** to create and promote a High Level Architecture for IoT – HLA and the IoT identifiers to position AIOTI as relevant SDO in Europe. It is sub-divided in 5 sub-WPs: WP1: IoT & Edge Computing Landscape, WP2: HLA, WP3: Semantic interoperability, WP4: Privacy and WP5: Security,
  - **Testbeds** (to facilitate to AIOTI members to find testbeds -catalogue- where to test/validate new developments for specific use cases,
  - **Urban Society** conceived as a sort of think tank reflecting on IoT's influence to Smart Cities, connecting and engaging with other European initiatives.
- Vertical groups (VWGs) that aim at covering domain-specific areas. The goal with these groups is to release reviews and recommendations on IoT innovations to specific application fields. Up to now, 6 vertical working groups are active:

- **Agriculture** align technology, policies, research trends and standards towards Smart Farming,
- **Buildings** to become the juncture place of construction stakeholders for European innovation in applied IoT to all types of buildings towards the Smart Building,
- **Energy** supporting EC to deliver workshops related to energy efficiency through IoT, generating whitepapers and collaborating with relevant energy-related entities in Europe,
- **Health** to bring AIOTI members to the relevant health innovation fora in Europe,
- **Manufacturing** to define the value of using IoT and edge computing in supporting Manufacturing sectors to reach goal on 2021-2027 challenges,
- **Mobility and Logistics** focus of safety, on demand transport, traffic efficiency, user experience, and transport impact and innovation through IoT, ensuring connection with most recent GAIA-X activities.

In the ASSIST-IoT we actively participated in WG Standardisation in WP1: IoT & Edge Computing Landscape, WP2: HLA and followed WP3: Semantic interoperability. The list of the contributions in ch.3.2.3 is presented.

2.5. BDVA: Big Data Value Association

The Big Data Value Association (BDVA) was created in 2014 as the private counterpart of the European Commission in the Big Data Value Public Private Partnership. It has been instrumental for defining innovation agendas, roadmaps and closing the gap with policy makers. ASSIST-IoT is not a project focused on Big Data, however, the interest of the project in this association increased when it became DAIRO, extending the collaboration with other communities in order to engage at the intersection of the key disciplines of Data, AI and Robotics.

As detailed in D9.3, BDVA is structured in task forces (TF1 - Programme, TF2 - Impact, TF3 - Ecosystem, TF4 - Communications, TF5 - Policy & Societal, TF6 - Technical, TF7 - Application, TF8 - Business, TF9 - Skills & Education, and TF10 - European data sharing spaces). Among them, interest of the project is on TF2 as well as subgroups of TF6 (SG1 - data technology architectures, SG3 - Data science and AI, and SG6 - Standards) and TF7 (SG7 - Mobility and logistics, and SG11 - Automotive).

With respect to Automotive & logistics, main lines of interest were related to connectivity and energy-efficiency aspects. In the former, the project has been working to facilitate having vehicle fleets complying with EURO 7 standards, focusing on data gathering, communication (considering loss of signal and mobile aspects) and OTA calibration updates; whereas in the latter, project has fostered the sharing and process of information to optimize actions (thus, reducing emissions) when trucks and cranes are involved. All in all, the key reference documents are the following:

- BDVA Position paper: The digital decade policy programme of the European Commission (link)
- AI, Data and Robotic Partnership: Strategic Research, Innovation and Deployment Agenda (SRIDA, link).
- BDVA Position paper: Current hot topics in data protection (link).

Particularly, partners from ASSIST-IoT have participated in BDVA events, with presentations such as “Architectures and building blocks for ports and maritime logistics data platforms” by the Innovation Manager Mr. Ángel Martínez Cavero in the Data Week 2021 (link), and those from the Deputy Coordinator Dr. Ignacio Lacalle (“Edge Computing – the convergence point in the human-cloud continuum framework”, and “Mobility and Transportation: Evolving Value Chains and Market Dynamics in the Computing Continuum”) in the 2021 and 2023 editions of the European Big Data Value Forum.

2.6. ECSO: European Cybersecurity Organization.

The European Cyber Security Organisation is a fully self-financed non-for-profit organization, private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity. It unites a variety of European cybersecurity stakeholders across the EU Member States, the European Free Trade Association (EFTA) and H2020 Programme associated countries.

ECSO is structured in the following working groups:

- WG1: Standardization, certification, and supply chain management.
- WG2: Market deployment, investments, and International Collaboration.
- WG3: Sectorial demand and users committee.
- WG4: Support to SMEs, coordination with countries and regions.
- WG5: Education, training, awareness, cyber ranges.
- WG6: SRIA and Cyber Security Technologies.

AS mentioned in D9.3, the WG1 is the most relevant group for Assist-IoT and their activities and publications was followed since the beginning of the project:

- ECSO strengthens dialogue between the cybersecurity industry and the European Commission with regard to the Cyber Resilience Act. 19-10-2023. https://ecs-org.eu/ecso-strengthens-dialogue-between-the-cybersecurity-industry-and-the-european-commission-with-regard-to-the-cyber-resilience-act/
- ECSO's new NIS2 Implementation Initiative launches with its first webinar. 14-06-2023. https://ecs-org.eu/ecsos-new-nis2-implementation-initiative-launches-with-its-first-webinar/
- ECSO and ETSI renew their cooperation on cybersecurity and standardisation. 01-06-2022. https://ecs-org.eu/ecso-and-etsi-renew-their-cooperation-on-cybersecurity-and-standardisation/
- Have your say on cybersecurity certification in the EU and associated countries. 16-05-2022. https://ecs-org.eu/have-your-say-on-cybersecurity-certification-in-the-eu-and-associated-countries/
- An insight into the NIS Cooperation Group. 29-03-2022. https://ecs-org.eu/an-insight-into-the-nis-cooperation-group/
- Study on the need of cybersecurity requirements for ICT products. 21-12-2021. https://ecs-org.eu/study-on-the-need-of-cybersecurity-requirements-for-ict-products/
- Product Certification Composition Document. 14-10-2022. https://ecs-org.eu/ecso-uploads/2022/10/5fbfc8436e5a1.pdf
- System security and certification considerations. 14-12-2021. https://ecs-org.eu/ecso-uploads/2022/10/61ebc4a13b567.pdf
- European Cyber Security Certification: Challenges ahead for the roll-out of the Cybersecurity Act. 13-12-2020. https://ecs-org.eu/ecso-uploads/2022/10/5fd787e5cae1c.pdf

2.7. ENISA: European Network and Information Security Agency

ENISA is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps

Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

ENISA defines the Internet of Things (IoT) as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making". Stemming from the definition is the fact that information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision-making, and actions. IoT is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures, such as Industry 4.0, smart grid, smart transport, etc. by enabling services of higher quality and facilitating the provision of advanced functionalities.

ENISA defines a set of baseline security actions for IoT and establish good practices for IoT on different application domains such as:

- Smart cars,
- Smart cities,
- Smart hospitals,
- Smart airports,
- Industry 4.0.

ENISA has had the following recent activity that fits with Assist-IoT project regarding reports and news:

- Digital Identity Standards. 03-07-2023. https://www.enisa.europa.eu/publications/digital-identity-standards
- ENISA CSIRT Maturity Framework - Updated and improved. 23-02-2023. https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework
- ENISA Threat Landscape for DoS Attacks. 06-12-2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks
- ENISA Threat Landscape 2023. 19-10-2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- ENISA Threat Landscape 2022. 03-11-2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
- ENISA Threat Landscape 2021. 27-10-2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- How Cybersecurity Standards Support the Evolving EU Legislative Landscape. 08-02-2023. https://www.enisa.europa.eu/news/how-cybersecurity-standards-support-the-evolving-eu-legislative-landscape
- Standardisation conference explores EU cybersecurity legislation. 16-03-2022. https://www.enisa.europa.eu/news/enisa-news/standardisation-conference-explores-eu-cybersecurity-legislation
- Highlights of the Cybersecurity Standardisation Conference. 05-02-2021. https://www.enisa.europa.eu/news/enisa-news/highlights-of-the-cybersecurity-standardisation-conference

2.8. TIC4.0: The Terminal Industry Committee 4.0

Terminals Industry Committee 4.0 is a non-profit association registered in Brussels, Belgium. TIC 4.0 initiative aims to bring together representative companies from both the Terminal Operators industry and Port Equipment Manufacturers and Suppliers to collectively work on the elaboration of such standards. Its objectives are the following:

- Define and agree common Process Semantics, Language and Operational Definitions among the agents involved in the cargo handling industry.
- Make technical publications available to facilitate the standards adoption by industry players for seamless data communication.
- Promote operational Proof of Concepts to facilitate the inter-operability of different information sub-systems of cargo handling facilities.
- Foster the deployment and adoption of selected existing standards and those developed by TIC4.0 by the sector.

The above objectives are met by the membership of TIC4.0 who organized themselves into work groups and develop agreed processes, database content and use the latest publishing software to publish the definition results for the general use of the Association membership and Industry stakeholders. General Assembly is the highest ruling body of TIC4.0 on policies, content, and governance. Participation in meetings by all the member companies occurs at least three times a year. The role of the Operations Council is to govern TIC4.0 operations in accordance with decisions reached by the General Assembly. The Chief Executive Officer (CEO) of the association manages and runs TIC4.0 in accordance with the guidelines as set by the General Assembly and the Executive Council. The task forces are the core groups creating the definitions for our industry. Task forces are small groups (max. 5 persons), consisting of members and their experts, set up for specific definition and standardization assignments selected by the Operation Council. Using online virtual work meetings, the definitions and related description goals can be achieved. The task forces use guidelines and templates developed by and for TIC4.0, to ensure that the results are consistent and easy to publish. The TIC 4.0 association is currently formed by more than 50 members, and growing.

Figure 1. TIC 4.0 members

The overall process from creation to publishing of definitions is illustrated in the below diagram.

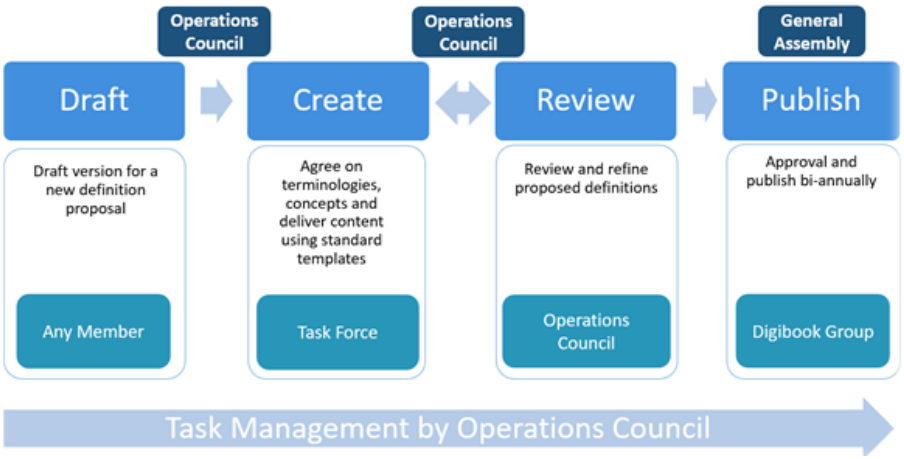

Figure 2. TIC 4.0 definition process

The schematic diagram of the definition process aims to manage the standardization of the language and vocabulary program for the years to come as follows:

Draft phase: Every member of TIC4.0 may propose work for a specific process and the concepts used in this process. Every member can create a draft version(s) of their understanding of the concept(s) to be defined.

Create phase: The Operation Council will prioritize the work and assign the draft proposal to a task force, consisting of delegates from members who are experienced in this specific concept. The task force will 'create' a definition using the TIC4.0 guidelines and templates, starting from the draft proposal.

Review phase: The results of the 'Create' process will then be submitted to the Operation Council for 'Review'. The Operation Council will check the consistency of the work with other definitions for potential overlap and overall quality. The Operation Council may ask the task force for further refinements as necessary.

Publish phase: When the Operation Council approve the definition created, it will be put on the agenda for formal approval by the General Assembly before publication

After formal approval by the TIC4.0 General Assembly, the TIC4.0 Communication Team will arrange all publication and communication of the approved material.

As it can be assumed, TIC 4.0 is very well aligned with the concepts that have been implemented in ASSIST-IoT pilot 1. Moreover, TL is the president of the Committee, so the flow of communications between project activities and standardization processes has been seamless, fluid, and very productive as can be seen in the list of collaboration activities listed in the following sections.

2.9. DG GROW - DG for Internal Market, Industry, Entrepreneurship and SMEs

The Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs is responsible for EU policy on the single market, industry, entrepreneurship and small businesses. Among its sub-groups, ASSIST-IoT has been monitoring and invited to join the "Advisory Group on Vehicle Emission Standards" (AGVES) and reporting to, the Commission expert group "Working Group on Motor Vehicles", hereafter "the expert group", with particular focus on emissions from motor vehicles, components, systems and separate technical unit. The sub-group shall:

- Assist DG Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) in the preparation of policy initiatives and implementing/delegated acts in the field of emissions in relation to the implementation of Euro 7 legislation.
- Establish cooperation/coordination between the Commission, Member States and stakeholders on questions relating to the implementation of the Euro 7 legislation.

2.10. Other standardisation organisations, forums and initiatives

For the ASSIST-IOT project also interesting are different organisations, forums and initiatives related to technological aspects of the designed solution. The aim is mainly to analyse their existing reports and to follow their current activities with possible contribution to their technical reports (in CEN WG31). Below is a short analysis of the following organisations:

- **ISO/IEC**: International Organization for Standardisation/International Electrotechnical Commission offers for experts a neutral and independent platform where they can discuss and agree on state-of-the-art technical solutions with global relevance, most relevant subcommittees are:
    - ISO/IEC JTC 1/SC6 Telecommunications and information exchange between systems,
    - ISO/IEC JTC 1/SC25 Interconnection of information technology equipment,
    - ISO/IEC JTC 1/SC27 Information security, cybersecurity and privacy protection,
    - ISO/IEC JTC 1/SC32 **Data management** and interchange,
    - ISO/IEC JTC 1/SC38 **Cloud Computing and Distributed Platforms**,
    - ISO/IEC JTC 1/SC41 **IoT** and Digital Twin,
    - ISO/IEC JTC 1/SC42 **Artificial Intelligence**.

  ISO/IEC membership is limited to national standardisation organisations and most of recommendations are not available without charging. Experts for recommendations preparations are nominated by national governmental ISO member and international organisations.

- **IETF**: Internet Engineering Task Force is open standardisation organization in the area of Internet-related technologies. In the context of 5G, the main areas that IETF is focusing on include network slicing, MEC, machine learning at network level, and security & privacy. Several **Working Groups in the IETF (DOTS, I2NSF, SACM)** have been focusing on aspects related to policy-based open security management and monitoring. In what relates to the **IRTF**, the **DINRG** is a target for contributions related to open, distributed security, as well as **NMRG** can be considered for matters related to network telemetry and intent-based network management.
- **IoT Forum** is a member based organization which aims to promote international cooperation on the Internet of Things, organize events and conferences, such as the **IoT Week** and develop activities and synergies with and among its members. IoT Forum was established by a community of research organizations and industries specialized in the Internet of Things. The founding members were developing joint activities the organizing of the IoT Week and European research projects which supported the creation of the IoT Forum as an autonomous legal organization.
- **W3C - World Wide Web Consortium** is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C is working on different aspects of Web technologies, the most interesting for ASSIST-IOT project are active groups related to Web Data and Web of Things. Regarding standardisation work W3C is focusing on Web technologies. The current and past work in the Web of Things Group is related to Technical Reports:
    - Web of Things (WoT) Architecture (W3C Recommendation);
    - Web of Things (WoT) **Thing Description** (W3C Recommendation);
    - Web of Things (WoT): **Use Cases and Requirements** (W3C Working Draft);
    - Web of Things (WoT) Discovery (W3C Working Draft);
    - Web of Things (WoT) Profile (W3C Working Draft).
- **CEN - the European Committee for Standardization,** is an association that brings together the National Standardisation Bodies of 34 European countries. CEN provides a platform for the development of European Standards and other technical documents for a variety of products, materials, services and processes. CEN supports standardisation activities in many fields and sectors including air and space, chemicals, construction, consumer products, defence and security, energy, environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging. ASSIST-IoT actively contributed to WG31 in case of safety of work.

- **CENELEC - the European Committee for Electrotechnical Standardization**, is an association of the National Electrotechnical Committees from 34 European countries. CENELEC prepares voluntary standards in the electrotechnical field, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of the European Single Market. CENELEC supports standardisation activities in many fields and sectors including: electromagnetic compatibility, accumulators, primary cells and primary batteries, insulated wire and cable, electrical equipment and apparatus, electronic, electromechanical and electrotechnical supplies, electric motors and transformers, lighting equipment and electric lamps, low voltage electrical installations material, electric vehicles railways, smart grid, smart metering, solar (photovoltaic) electricity systems, etc.

3. ASSIST-IoT standardization activities

In the project we worked on different technical subjects to develop overall common solution for different IoT use cases. Therefore, we distinguished the main interesting areas of standardisation activities to be used in our solution or to contribute to ongoing standardisation work as well as to identify the gaps in standardisation scope of work (D9.3). Below most relevant standardisation technical subjects in the project are presented. Our standardisation activities related to different technical domains are the following:

- Follow up different SDOs and initiatives activities,
- Active participation in SDOs and initiatives,
- Identification and analysis of standards used in our solutions,
- Identification of gaps in standardisation for different technical subjects,
- Contribute to standards work: recommendations, technical reports, white papers.

In order to contribute to the current standardisation landscape ASSIST-IoT has identified several standardisation goals and potentialities in several specific standardisation domains.

3.1. ASSIST-IoT technical domains

Below the following technical domains in ASSIST-IoT project are considered in relation to standardisation activities. The first analysis was included in D9.3 and here we have summary for the whole project duration.

3.1.1. Internet of Things domain

In the IoT group of subjects the following ones were considered:

1. IoT platform architecture:
    - ASSIST-IoT was focusing on the application challenges and analysis of reference architecture diversities of IOT-A RA, RAMI 4.0, ETSI MEC, and IIRA.
    - ASSIST-IoT propose a 2-D layered architecture based on the interconnection of enablers with well-defined roles. The architectural issues are currently under analysis for submission to AIOTI, we are actively participating in HLA release 6.0 with possible updates. The final changes will be discussed during 2024 year, when at the end of the year the new HLA version is planned to release.
2. IoT landscape of challenges, gaps and standardisation activities:
    - Continuous gaps analysis and standardisation work in different SDOs.
    - IoT projects landscape analysis in case of standardisation activities, ASSIST-IoT lead the analysis in AIOTI, co-editing the reports.
3. Data subjects:
    - One of the major challenges is the analysis of massive raw datasets. Some of the respective SDOs and initiatives are dedicated to this topic such as AIOTI, ISO/IEC JTC 1, ITU-T, W3C, ETSI. ASSIST-IoT was focusing on the current gaps of interoperability framework, semantic inconsistency in meta-models, and data quality.
    - The combination of the semantic repository, annotation and translation enabler will entail a connection and methodology suitable to be standardised. In ASSIST-IoT standardisation activities were focused on following up and usage of existing approaches for use cases implementation and testing in demonstrative scenarios.
    - Data spaces analysis, AIOTI/BDVA Data space position paper is under discussion. Next issues of the report are planned to release.
4. Use cases:

    Another most popular and broad domain is related to the IoT use cases. The ongoing standardisation work analyses different aspects that can be derived from use cases e.g. data spaces, semantics, human-machine

interfaces, edge computing requirements, testbed federation and many use case specific subjects like in case of ASSIST-IOT: workers' safety, logistics or autonomous vehicles aspects. The following contributions were prepared and after end of the project the use cases results are planned to be used:

- Use cases analysis where the IoT data and services require data usability specifications for machines consuming data for AI (for example machine learning), contribution with use cases specification in ETSI STF601: "Use cases for cross-domain data usability of IoT devices";
- Requirements specification for edge cloud computing optical systems, contribution with use cases specification in AIOTI WG3 for edge cloud computing gaps analysis;
- In the analysis of landscape of the IoT standardisation the contribution to AIOTI reports,
- Standardisation gaps analysis for the use cases and reference architectures, based on ASSIST-IoT use cases the identification of standardisation gaps in different technical aspects for ongoing standardisation work;
- Use case specific subjects:
    i. **Port automation –** in TIC4.0 the definition of process semantics, language and operational definitions among the agents involved in the cargo handling industry is elaborated. It is specific subjects of ASSIST-IoT Pilot 1.
    ii. **Occupational safety and health –** there are plenty of European and international standards currently in force that specify various requirements related to workers' safety. A review of the most important ones has already been included in the deliverable D3.4. Most of those documents have a status of the European standard (EN) that has been approved by CEN. The one of the specific subjects in ASSIST-IoT is related to wearable electronic devices integrated with personal protective equipment aimed at improving worker safety and comfort. Multidisciplinary (i.e. combining various disciplines such as: electronics, ICT, environmental engineering, textile and materials engineering) and niche nature of such solutions makes standardisation works in the safety area particularly challenging. It is one of the developed subjects of the ASSIST-IoT Pilot 2.
    iii. **Vehicle in-service emission diagnostics** - UPV is participating in AGVES, which is assisting the European Commission in defining and developing the Euro 7 emissions requirements, and that also includes On-Board Monitoring (OBM) requirements. ASSIST-IoT pilot 3a is aligned with the current OBM draft proposal, and the lessons learn from the project have been presented in recent AGVES meeting.

3.1.2. Networking and edge cloud domain

In networking subjects there is a lot of standardisation work in different SDOs like: ITU-T SG13, ETSI NFV, ETSI MEC, IEEE SA, AIOTI, 3GPP, 5G PPP, IETF, ISC/IEC. In ASSIST-IoT we focused on IoT networking and edge computing aspects, so among many of new and ongoing networking standardisation items the most relevant are:

- Methodology for encapsulating enablers (charts, labelling, etc.) altogether with the use of CNF to distribute service workloads, analysis and identification of possible gaps,
- Smart Orchestrator enabler and NFV subjects, ETSI activities following up and implementation in the ASSIST-IoT solutions,
- IoT Relation and Impact Beyond 5G (analysis and contribution in AIOTI WG Standardisation TF),
- Edge Computing landscape of challenges, gaps and standardisation activities:
    - Continuous gaps analysis and standardisation work in different SDOs.
    - Edge Computing projects landscape analysis in case of standardisation activities, ASSIST-IoT lead the analysis in AIOTI, co-editing the reports.

3.1.3. Cybersecurity domain

ASSIST-IoT is following both IoT, edge and cloud (multi-layer) cybersecurity standards.

The IoT landscape exhibits a confluence of hardware components such as sensors and devices, software elements including data analytics and machine learning, and connectivity solutions encompassing network protocols and cloud services.

The most common vulnerabilities in this type of systems are:

- Diverse Device Ecosystem: The IoT ecosystem encompasses a wide array of devices, resulting in a multitude of operating systems, firmware, and protocols.
- Data Privacy Concerns: The issue of data privacy arises due to the continuous collection, transmission, and storage of data by Internet of Things (IoT) devices.
- Limited Computing Resources: Numerous Internet of Things (IoT) devices are engineered with the objective of achieving cost-effectiveness and energy efficiency, resulting in inherent constraints on their processing capabilities and memory capacity.

After evaluating the vulnerabilities of the system, there is a need to find the solutions to mitigate these vulnerabilities and the cybersecurity standard that better fits the requirements.

In this way the project has been focused in granting the access to the data only to authored users and also to protect the system from attacks or incidents caused by external entities or even internal users. The most useful standards in cybersecurity are ISO-27001, NIST-800-53 and the most extended in Europe IEC-62443 that applies to IoT and OT systems, networks and devices. The primary goal of the ISA/IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. The IACS community audience for this standard is intended to be asset owners, service providers for integration or maintenance, product suppliers and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

3.1.4. Artificial Intelligence domain

Most of the SDOs and different initiatives are launching standardisation work on broad range of AI/ML subjects and applications (e.g. ITU-T SG13, ISO/IEC JTC1 SC42, ETSI ENI, SAI, IEEE SA, AIOTI, BDVA). Due to the novelty of the AI/ML domain, ASSIST-IoT was monitoring and analysing the standards development and consolidate project results (e.g. H2020 AI4EU), looking for opportunities to contribute to AI/ML framework architectures, components and use cases. In this domain the standardisation work is still in the early stage therefore the potential identified subjects for future contributions are:

- Video augmentation enabler for maritime terminal assets recognition via Machine Learning over moving objects. Although this field is rather explored, there is not an actual standard for applying current existing tools for maritime terminal assets.
- Objects recognition using AI/ML like helmets and vests of the workers in industry plants, construction sites (in case of the ASSIST-IoT).
- The architecture and schema (including steps, etc.) of the Federated Learning enablers which is one of the hot topics today and it is present (as projects) in diverse SDOs. The mechanisms and recommended technology are needed to be delivered as a standard.

3.1.5. Activities summary per technical domain

To summarise ASSIST-IoT standardisation activities according to main technical domains and SDOs the global view in the Table 1 is presented. In each domain, we identified and actively participated in standardisation working groups where our activities can be distinguished as:

- active participation in working groups (blue box),
- active participation with submitted contributions (green box),
- following up (yellow box).

Table 1. Standardisation activities in technical domains

Domain / SDO/initiative	IoT	AI	Networking/Cloud	Cybersecurity
ETSI	smartM2M	AI, ENI	NFV, MEC	SAI, PDL
ITU-T	SG-20	SG-13, SG-16	SG-13	SG-17
IEEE SA	CEC, CCSC	AISC	IEEE 802.1x	CPSC
AIOTI	WG SD	WG SD	WG SD, Testbeds	WG SD
BDVA	TF6 (SG1, SG6) TF7 (SG7, SG11)	TF6 (SG3, SG6)		TF6 (SG4)
ESCO/ENISA				Security

ASSIST-IoT Consortium members are present in most important international standardisation bodies, committees, and initiatives and have experience in contributions to published standards and in pre-normative forums in different areas. In next chapter the detailed information about ASSIST-IoT standardisation activities and evaluation in terms of planned standardisation KPIs is presented.

3.2. Standardization activities in the project

3.2.1. Strategy review

At the beginning of the project, ASSIST-IoT team has defined the plan of the standardisation activities, based on the work planned in individual Work Packages (in D9.2) and updated at D9.3. In the presented roadmap (Figure 3) the whole project duration activities are showcased, indicating through checkpoints relevant milestones (at the middle and at the end of the project).

In the first half of the project the work was concentrated on analysis of the existing standards and ongoing standardisation to select most relevant SDOs and initiatives for the project technical subjects. In the second half of the project contributions to SDOs the standardisation activities were increased according to the Work Plan. The detailed information about these activities in relation to planned KPIs is presented.

For the project, the standardisation strategy includes the following activities and their KPIs defined in D8.1:

1. **Communications to modify / improve existing standards used in ASSIST-IoT -** identification of gaps and needs for improving of existing standards – target KPI: 6,
2. **Recommendations in relevant SDOs and initiatives -** contribution to recommendations in SDOs – target KPI: 10,
3. **SDOs and pre-normative initiatives engaged -** engagement in SDOs work and pre-normative initiatives – target KPI: 40,
4. **Internationally recognized standards supported in ASSIST-IoT** – usage of standardized elements in project solutions, target KPI: 40
5. **Identified standards related to ASSIST-IoT activities -** followed and analysed standards, target KPI: 120.

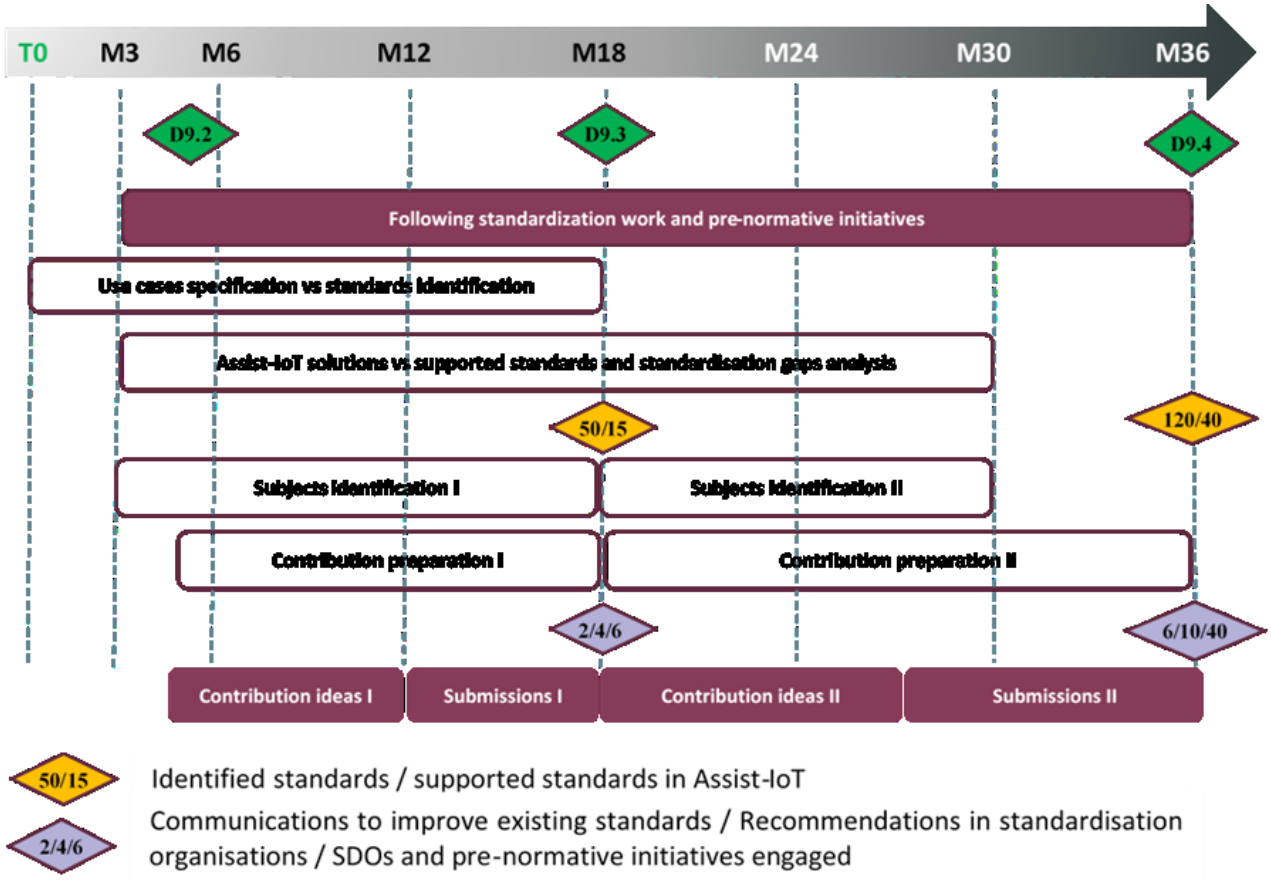

Figure 3. Strategy and target KPIs for standardisation activities

The standardisation work inside the ASSIST-IoT project according to planned strategy was realized. We followed up the standardisation work in different SDOs and initiatives and in different technical domains, analysed and identified gaps and standardisation work items and contributed in the identified subjects.

According to strategy we have defined standardisation KPIs. In next chapters our standardisation activities and its evaluation against planned values of KPIs are presented in details.

3.2.2. Communications to modify / improve existing standards used in ASSIST-IoT

The KPI.3.1.2 measures the number of **identified existing standards where the modification or improvement is required in relation to developed ASSIST-IoT components**, enablers or overall architectural design. The list of these standards in relation to ASSIST-IoT components will verify the KPI compliance. To fulfil this KPI the **number of identified standards should be 6 at the end of the project**.

Table 2. Identified standards to modify/improve

No	SDO/Standard	Description/standard title	Modification/Improvement
1	ETSI MANO	It covers the management and orchestration necessary for provisioning VNFs, along with their lifecycle management	Initially considered for VM-based VNFs, recent releases have tackled Cloud Native (i.e., container-based) ones. We suggest to explore the introduction of specifications related to hyper automation / AI-nativeness in the

			mid-/long-term, and have a close collaboration with CNCF, which hosts *de facto* standard solutions for this area.
2	ETSI SmartM2M	ETSI TR 103 778, Use cases for cross-domain data usability of IoT devices	Contributions with use cases specific to ASSIST-IoT
3	ITU-T Y.4478, Y.IoT-SCS	ITU-T SG20, Requirements and functional architecture for smart construction site services	Change in the network architecture and requirements specification for construction site use case.
4	Y.IoT-Vreqs	ITU-T SG20, Requirements and capability framework of the internet of things for vision",	Improvement with AI based vision recognition to framework of the internet of things applications.
5	IEEE SA	IEEE P3195 Ontology Standards	Improvement of ontologies for the specific use cases.
6	AIOTI WG2	HLA6.0 – High Level Architecture specification	Alignment of ASSIST-IoT architecture and HLA specification.
7	AIOTI WG1	High Priority IoT Standardisation Gaps and Relevant SDOs	Update of standardisation gaps for IoT verticals related to ASSIST-IoT.

3.2.3. Recommendations in relevant SDOs and initiatives

To measure the KPI.3.1.3 we need to count the number of **activities and performed contributions to different SDOs and initiatives for recommendations work purposes**. The contributions will be prepared according to relevant ASSIST-IoT research and development activities in different technical and non-technical subjects. The list of activities and contributions were collected. The target value of this **KPIs is 10 at the end of the project**.

Table 3. Activities/contributions to recommendations

No	Standard/SDO/initiative	Description	Partners
1	OPENCONTINUUM LANDSCAPE V1 AND PRELIMINARY RECOMMENDATIONS	This document starts the common definition for a Continuum taxonomy as well as the methodology for defining a conceptual framework to analyse the European landscaping in order to provide recommendations for future work. ASSIST-IoT worked also actively for testing the survey related to "Landscape Framework for Research Assets Evaluation", 2023.	UPV
2	Developing a Reference Architecture for the Continuum	As part of the ICT-56 projects, ASSIST-IoT worked in a document for defining common concepts, taxonomy and block of the computing continuum, 2023	UPV
3	NGIoT Roadmap and Policy Recommendations	Strategy white paper of the CSA of the ICT-56 projects, with insights extracted from the 6 flagship projects, 2023.	All
4	A Vision on Smart, Decentralised Edge Computing Research Directions	Exports the vision and future research directions of the flagship ICT-56 projects with respect to decentralised edge computing, 2023	UPV, PRO
5	D3.8: Recommendations on Research Priorities and Innovation Strategies to Standardisation	The report provides a mapping of relevant pre-normative activities and standardisation bodies, including relevant documentation and contact points, as well as its mapping based on the EU-IoT Scope Areas, and IoT European competitiveness domains. It provides a full perspective of recommendations on research priorities and innovation strategies for Standardisation derived from several activities developed in the context of WP3, 2023	UPV

6	ETSI STF601	Contribution to „Use cases for cross-domain data usability of IoT devices", Cross-domain usability of IoT devices for humans and machines, TC (Technical Committee) SmartM2M, Technical Report, 2021 https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf	OPL leading, all partners
7	ESCO	Technical Paper on Internet of Things (IoT). April 2021 v0.8. The scope of this technical paper is to identify current and foreseen challenges related to IoT cybersecurity at technical level (both from the IoT supply point of view and the IoT adopters' point of view), at regulatory level, and in relation to certification.	S21SEC
8	AIOTI	IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges Release 1.0, contribution 2021 This report highlights several IoT vertical domain use cases collected by the AIOTI and determines the specific requirements they impose on the underlying (Beyond) 5G network infrastructure.	OPL, UPV
9	AIOTI	AIOTI Report IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges R2, contribution, 2022. This report highlights several IoT vertical domain use cases collected by the AIOTI and determines the specific requirements they impose on the underlying (Beyond) 5G network infrastructure.	OPL, UPV
10	AIOTI	IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges Release 3.0, contribution, 2023. This report highlights several IoT and Edge Computing vertical domain use cases and determines the specific requirements they impose on the underlying (Beyond) 5G network infrastructure. These use cases and requirements can be used by Standards Developing Organizations (SDOs), such as 3GPP, ITU-T, ISO, and IEEE as requirements for automation in vertical domains focusing on critical communications.	OPL, UPV
11	AIOTI	Edge Computing Standard Framework Concepts Release 1.0, contribution, 2021. The main objective of this deliverable is to briefly present the global dynamics and landscapes of edge computing SDO, Alliance and OSS initiatives, which can be used: 1) to leverage on existing edge computing standardization, industry promotion and implementation of standards and protocols, and 2) to provide input to edge computing standardisation gap analysis activities.	OPL, partners
12	AIOTI	Contribution to Report Computing Continuum Scenarios, Requirements and Optical Communication enablers – use cases and requirements, 2022. This report introduces Computing Continuum use cases, requirements and KPIs on communication infrastructures, IoT and edge computing platforms. The documents finally list a set of recommendation of the evolution of the current technologies for high-end IoT system running on computing continuum platforms.	OPL, partners

13	AIOTI	High Level Architecture (HLA) next release 5.0, contribution, 2021. AIOTI WG Standardisation has developed a High Level Architecture (HLA) for IoT that should be applicable to AIOTI Large Scale Pilots.	OPL, partners
14	AIOTI	High Priority IoT Standardisation Gaps and Relevant SDOs R3, contribution, 2023. This report introduces an approach for the definition and identification of key IoT gaps in several initiatives. Based on the prioritisation of these gaps, the deliverable starts to address the work done within the relevant Standards Developing Organisations (SDOs) that need to cooperate in order to solve these gaps.	OPL, partners
15	AIOTI	Co-editor of AIOTI report „EU funded projects landscape focusing on IoT and Edge computing" Release 1.0, 2022. The main objective of this deliverable is to briefly present the EU funded projects focusing on IoT and edge computing.	OPL
16	AIOTI	IoT and Edge Computing EU funded projects landscape, Release 2, co-editor. 2023. The main objective of this deliverable is to briefly present the EU funded projects focusing on IoT and edge computing, which can be used to: 1) leverage on existing IoT and edge computing research and innovation activities in Europe, and 2) provide input to IoT and edge computing standardisation gap analysis activities.	OPL
17	AIOTI	IoT LSP Standard Framework Concepts Release 3.0, contribution, 2023. Report introduces IoT Standards Developing Organisation (SDO), Alliance and Open Source Software (OSS) landscapes to be used as input for the recommendations for Large Scale Pilots (LSPs) standard framework and gap analysis.	OPL
18	ITU-T	ITU-T Y.4478, Y.IoT-SCS, ITU-T SG20, Requirements and functional architecture for smart construction site services, contribution to work on new standards, 2023	OPL, partners
19	ESCO	Contribution to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem, 2022	S21SEC
20	TIC 4.0 2022.005 Release	Contains two main blocks: a very extensive and detailed presentation of the TIC4.0 concepts, and a set of Semantics, Data Model and Definitions	TL
21	TIC 4.0 2022.006 Release	Contains the following topics: • Guideline on how to include TIC in technical specifications. • An extensive overview of the main events and processes defined and published according to the TIC4.0 semantics. • The Job Instruction process related to the TOS data model.	TL

		• The first set of definitions directly targeting the CHE Spreader. • The principles of how to translate the dataset from the FLAT format into the JSON format, including an open-source software tool to automatically convert datasets from FLAT to JSON.	
22	TIC 4.0 2023.007 Release	Contains the following topics: • Some missing statuses have been added to the Job Instruction process, such as assigned, dispatched and not dispatched. • The "job-stepping" concepts related to cargo move steps during the "collect" and "deliver" have been added. The second set of definitions, focusing on the different modes, movements and functions that the spreader can do.	TL
23	TIC 4.0 2023.008 Release	Contains the following topics: • TIC4.0 Health White Paper which gives an overview of the health ecosystem and its relevance in the port industry. It complements the existing definitions and provides the outlook to develop a complete health ecosystem, including taxonomies for health signals, diagnosis, and root causes, to enhance maintenance operations and facilitate predictive maintenance. • Cycle: The existing definition Cycle 2022.004 was updated and reviewed with the following changes: the new definition "deliver" was included and the context between "deliver" and "end of cycle" was clarified. The links of related TIC4.0 standards were updated. • Carrier Visit: The definition of "FirstTimeCarrierReadyforDeparture" was added to the extensive overview of events of the 2022.006 Release. • Job instruction: The definition of the events "collect" and "deliver" in relation to moving cargo have been added. A third set of definitions for the topic spreader, identifying the unique position of devices located on a spreader in relation to a reference mark.	TL
24	TIC 4.0 2023.009 Release	Contains the following topics: • "Maintenance ensuring Health" White Paper: After defining what Health means, this white paper was focused on the subject Maintenance (group of actions that take place to preserve the asset's Health). • Maintenance Data Model: A new Data Model for Maintenance has been developed to reflect the	TL

		processes, concepts and definitions that concern this area of interest. • "KPI" White paper: intends to create an understanding of the methodology of how any KPI (standard or exotic) may be calculated and represented using the TIC4.0 semantic. • The definition of "Cargo" has been expanded to reflect and cover Reefer-Cargo characteristics 'TypeReefer'. • New concepts related to different parts of the spreader (tools, extensions) have been the focus of this latest release. General concepts like On, Off and Powered were already defined in the previous releases for the "Container Handling Equipment (CHE)", now they have been updated for "reefer" as well.	
25	AGVES	The UPV is participating in AGVES, which is assisting the European Commission in defining and developing the EURO7 emissions requirements, and that also includes On-Board Monitoring (OBM) requirements. ASSIST-IoT pilot 3a is aligned with the current OBM draft proposal, and the lessons learn from the project have been presented in recent AGVES meeting.	

3.2.4. SDOs and pre-normative initiatives engaged

The KPI.3.1.4 is collecting the number of different engagements in SDOs, and pre-normative initiatives described in D9.3. **All activities will be counted regarding participation in different SDOs, initiatives and forums for different standardisation subjects**. The active participation in different standardisation working groups, study groups, task forces and their working subjects were included.

To fulfil this KPI we need to have activities **at least in 40 engagements** at the end of the project.

Table 4. SDOs/Initiatives engaged

No	SDOs/Initiatives	Description	Partners
1	AIOTI	Active participation in AIOTI Standardisation WG with sub-WPs: WP1: IoT & Edge Computing Landscape. Contributions to the white papers and technical reports in WP1.	OPL, UPV
2	AIOTI	WP2: HLA. Contributions to the white papers and technical reports in WP2.	UPV, OPL
3	AIOTI	WP3: Semantic interoperability.	UPV
4	BDVA	Participation in SG3: Data science and AI.	UPV
5	BDVA	Participation in SG6: Big data - HPC.	UPV
6	BDVA	Participation in SG6: Standards.	UPV
7	EUCEI	Participation in EUCEI TF1 (Strategic Liaisons),	UPV, PRO, SRIPAS, INF
8	EUCEI	Participation in EUCEI TF2 (Open source engagement)	UPV, PRO

9	EUCEI	Participation in EUCEI TF3 (Architecture)	UPV, OPL
10	EUCEI	Participation in EUCEI TF6 (Impact)	INF, OPL, UPV
11	EU-IoT	Participation on the working groups of the CSA	UPV, PRO, INF
12	CEN TC248 WG31 PG	Active participation in CEN Standardisation WG31: Testing the impact of smart textile elements in clothing on the user cognitive load (reported as preliminary work)	CIOP-PIB
13	ESCO	Active participation in ESCO with contributions to technical reports.	S21SEC
14	ITU-T SG20 Q1	SG20 IoT, smart cities & communities, Work item 1: Interoperability and interworking of IoT and SC&C applications and services	OPL
15	ITU-T SG20 Q2	SG20 IoT, smart cities & communities, Work item 2: Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies	OPL
16	ITU-T SG20 Q3	SG20 IoT, smart cities & communities, Work item 3: IoT and SC&C architectures, protocols and QoS/QoE	OPL
17	ITU-T SG20 Q4	SG20 IoT, smart cities & communities, Work item 4: Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C	OPL
18	IEEE SA	IEEE Standard Ontology Working Group, member	OPL, SRIPAS
19	IEEE SA	IEEE Common Core Cyber Ontology subgroup, member	OPL
20	IEEE SA	IEEE Testbeds working group, member	OPL
21	IEEE SA	C/CCSC Cloud Computing Standards Committee, member	OPL
22	IEEE SA	Artificial Intelligence Standards Committee, member	OPL
23	IEEE SA	COM/EdgeCloud-SC Edge, Fog, Cloud Communications with IOT and Big Data Standards Committee, member	OPL
24	IEEE SA	COM/NetSoft-SC Virtualized and Software Defined Networks, and Services Standards Committee, member	OPL
25	ETSI MANO	ETSI MANO working group participation	UPV
26	ETSI NFV	ETSI NFV working group participation	OPL
27	TIC4.0	TL leader of committee, actively working on standardisation	TL
28	ISO/IEC SC32	Following up Data management and interchange working group	OPL
29	ISO/IEC SC38	Following up Cloud Computing and Distributed Platforms	OPL
30	ISO/IEC SC41	Following up IoT and Digital Twin	OPL
31	5GIA	Participation in the standardisation working groups	OPL, ICSS
32	3GPP	OPL representatives in the organisation	OPL
33	ENISA	Members in the organisation	S21SEC, OPL
34	FIWARE	UPV participates in the organisation	UPV
35	EFFRA	UPV participates in the organisation	UPV
36	ITU-T SG 13	SG 13 Future networks participation	OPL
37	ITU-T SG 17	SG 17 Security	OPL
38	ETSI MEC	ETSI MEC working group participation	OPL
39	ETSI IOT	ETSI IOT working group participation	OPL
40	IETF	Following up and participation on IoT subjects	UPV, OPL
41	IEEE SA Open	Gitlab, following up	UPV, OPL
42	AGVES	EURO7 standard	UPV

3.2.5. Supported standards

The KPI.3.1.1 (Internationally recognized standards supported in ASSIST-IoT solutions) measures the number of **applied existing**, well-renowned and market-applied **standards in the different components** of the ASSIST-IoT. To identify the compliance of this KPI a list of supported standards in different components was prepared. The fulfilment of this KPI is positive, when the number of **standards supported by all software components are over 40** at the end of the project.

Table 5. Supported standards

No	Standard	Description	Purpose
1	ISO/IEC/IEEE 42010	Addresses the creation, analysis and sustainment of architectures of systems through the use of architecture descriptions	Alignment of the information provided in the ASSIST-IoT Reference Architecture
2	ITU-T Rec. Y.2060/4000	Overview of the Internet of things (IoT). It clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model.	Alignment of the characteristics/ features of the horizontal planes of the ASSIST-IoT reference architecture. More than embracing the standard, works over parts of it.
3	IEEE standard 1471	Addresses the activities of the creation, analysis, and sustainment of architectures of software-intensive systems, and the recording of such architectures in terms of architectural descriptions	The concept of "concern" is introduced in the ASSIST-IoT Reference Architecture following the taxonomy of the standard.
4	ETSI NFV	Requirements and architecture for virtualization for various functions within telecoms networks	Considered in the Smart orchestrator solution, base of the virtualization stack of the project
5	ETSI MANO	It covers the management and orchestration necessary for provisioning VNFs, along with their lifecycle management	Considered in the Smart orchestrator solution, base of the orchestration of the workloads of the project
6	W3C Web standards	Set of web standards related to HTML, CSS, DOM, SVG, PNG, etc.	Development of user web interfaces
7	MEF 70	It standardizes SD-WAN service attributes and uses standard IPv4 and IPv6 routing protocols	Applied as using the Akraino SD-EWAN as base for the design of the SD-WAN enablers of the project
8	RFC 6071	Document of IP Security (IPsec) and Internet Key Exchange (IKE)	IPSec is considered in the SD-WAN solution
9	IEEE 802.1ad, IEEE 802.3ad	Two standards related to networks bridges and aggregation of network connections	Considered for designing and implementing the Multi-link enabler solution – adapted to wireless links
10	OpenAPI 3.1.0	The OpenAPI Specification (OAS) defines a standard, programming language-agnostic interface description for HTTP APIs	Used for defining the enablers' exposed APIs and making them usable by the OpenAPI enabler
11	ITU-T Y.4212	Requirements and capabilities of network connectivity management in the Internet of things	Network connectivity in the pilot 2 (you can describe more if needed)
12	ITU-T Y.4478, Y.IoT-SCS	Requirements and functional architecture for smart construction site services	Pilot 2 construction site, network architecture

13	A09:2021-Security Logging and Monitoring Failures	Returning to the OWASP Top 10 2021, this category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected.	Part of the architecture, serving security purposes.
14	A08:2021-Software and Data Integrity Failures	Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations.	Pilot 2 construction site, network architecture
15	IDS RAM 3.0	An industry standard for building IDS ecosystems, products and services.	Part of the architecture, serving interoperability purposes.
16	ISO/IEC 29119-1: Concepts & Definitions	Defines key software testing concepts and vocabulary, serving as the foundation for IEEE software testing standards.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.
17	ISO/IEC 29119-2: Test Processes	Establishes a generic testing process model applicable to any software development lifecycle, focusing on risk mitigation and key product attributes.	
18	ISO/IEC 29119-3: Test Documentation	Provides standardized testing documentation templates customizable to an organization's software development lifecycle requirements.	
19	ISO/IEC 29119-4: Test Techniques	Offers dynamic software testing techniques based on industry standards like BS-7925-2, including equivalence partitioning and boundary value analysis.	
20	ISO/IEC 29119-5: Keyword Driven Testing	Supports keyword-driven testing approaches using predefined action-based keywords for easier test case understanding and implementation.	
21	EN 14255-2:2005	Measurement and assessment of personal exposures to incoherent optical radiation Visible and infrared radiation emitted by artificial sources in the workplace	Determination of the UV exposure coefficient of construction workers – Pilot 2
22	EN ISO 13688:2013	Protective clothing - General requirements	Compatibility of used wearable devices with protective clothing – Pilot 2
23	EN ISO 20471:2013+A1:2016	High visibility clothing - Test methods and requirements	Compatibility of used cooling clothing with protective clothing (High visibility clothing) – Pilot 2
24	EN 361:2002	Personal protective equipment against falls from a height – Safety harnesses	Compatibility of equipment used in tests with an anthropomorphic mannequin (Fall-related incident identification) – Pilot 2
25	EN 358:2018	Personal protective equipment for positioning during operation and prevention of falls from a height – Safety belts and lanyards for positioning during operation or restriction of movement	
26	EN 813:2008	Personal protective equipment against falls from a height – Sit harnesses	
27	EN 12277:2015+A1:2018	Mountaineering equipment - Harnesses - Safety requirements and test methods	
28	EN 360:2002	Personal protective equipment against falls from a height – Retractable type fall arresters	

29	EN 362:2004	Personal protective equipment against falls from a height – Connectors	
30	EN 353-2:2002	Personal protective equipment against falls from a height – Self-locking arrester on flexible anchorage line	
31	EN 355:2002	Personal protective equipment against falls from a height – Energy absorbers	
32	EN 354:2002	Personal protective equipment against falls from a height – Lanyards	
33	EN 397:2012+A1:2012	Industrial safety helmets	Compatibility of AR glasses used with PPE – Pilot 2
34	Regulation (EU) 2016/425	Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC	Compatibility of used wearable devices with protective clothing – Pilot 2
35	Council Directive 89/391/EEC	Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work	Compatibility of used wearable devices with the requirements for ensuring safety during work – Pilot 2
36	EN ISO 9886:2004	Evaluation of thermal strain by physiological measurements	Measurement of physiological parameters that are monitored to detect dangerous situations (such as heart disruptions) – Pilot 2
37	ITU-T Y.4212	Requirements and capabilities of network connectivity management in the Internet of things	Network connectivity in the pilot 2
38	ITU-T Y.4478, Y.IoT-SCS	Requirements and functional architecture for smart construction site services	Pilot 2 construction site, network architecture
39	OAuth 2.0	Provides specific authorization flows for web applications, desktop applications, mobile phones, and living room devices	Used in IdM and authzserver enablers
40	ANSI SQL	It is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS)	Used in the DDBB of the enablers.
41	IEC-62443	Define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).	Considered for the design and the implementation of the cybersecurity enablers
42	XACML	It is an XML-based standard markup language for specifying access control policies	Used in authzserver enabler for the evaluation of the authorization rules
43	NIST 800-53	Provides a catalogue of security and privacy controls for all U.S. federal information systems except those related to national security	Considered for the design and the implementation of the cybersecurity enablers
44	ISO 19650-6	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 6: Health and safety information	Pilot 2 – safety of workers, health monitoring

45	TIC4.0 Release 2023.009	Semantics, Dataset, Data Model and Definitions	Pilot 1 - port logistic, dataset specification
46	A09:2021-Security Logging and Monitoring Failures	Returning to the OWASP Top 10 2021, this category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected.	Part of the architecture, serving security purposes.
47	A08:2021-Software and Data Integrity Failures	Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations.	Pilot 2 construction site, network architecture
48	IDS RAM 3.0	An industry standard for building IDS ecosystems, products and services.	Part of the architecture, serving interoperability purposes.
49	ISO/IEC 29119-1: Concepts & Definitions	Defines key software testing concepts and vocabulary, serving as the foundation for IEEE software testing standards.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.
50	ISO/IEC 29119-2: Test Processes	Establishes a generic testing process model applicable to any software development lifecycle, focusing on risk mitigation and key product attributes.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.
51	ISO/IEC 29119-3: Test Documentation	Provides standardized testing documentation templates customizable to an organization's software development lifecycle requirements.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.
52	ISO/IEC 29119-4: Test Techniques	Offers dynamic software testing techniques based on industry standards like BS-7925-2, including equivalence partitioning and boundary value analysis.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.
53	ISO/IEC 29119-5: Keyword Driven Testing	Supports keyword-driven testing approaches using predefined action-based keywords for easier test case understanding and implementation.	Considered in the corresponding software testing phases throughout the ASSIST-IoT's software testing lifecycle.

3.2.6. Identified standards

The KPI.3.1.5 measures the **identified standards related to different subjects** of ASSIST-IoT solutions (components, enablers, architecture) besides supported standards listed below. The analysis of the standards from different SDOs and initiatives in D9.3 was presented and later updated until end of the project. Based on this analysis we can count the number of identified standards and technical reports to evaluate planned KPI value. To fulfil this KPI we need **to identify at least 120 standards** at the end of the project. The list of identified standards is presented in table below.

Table 6. List of identified standards related to ASSIST-IoT

No	Standard	Title/Description
1	ETSI TR 103 621 V1.1.1 (2022-03)	SmartM2M, Guide to Cyber Security for Consumer Internet of Things.
2	ETSI SR 003 680 V1.1.1 (2020-03)	SmartM2M. Guidelines for Security, Privacy and Interoperability in IoT System Definition;
3	ETSI TS 103 264 V3.1.1 (2020-02)	SmartM2M, Smart Applications; Reference Ontology and oneM2M Mapping
4	ETSI TR 103 527 V1.1.1 (2018-07)	SmartM2M, Virtualized IoT Architectures with Cloud Back-ends

5	ETSI TR 103 529 V1.1.1 (2018-08)	SmartM2M, IoT over Cloud back-ends: A Proof of Concept
6	ETSI TR 103 675 V1.1.1 (2020-12)	SmartM2M, Artificial Intelligence and the oneM2M architecture
7	ETSI TR 118 501 V1.0.0 (2015-05)	oneM2M Use Case collection
8	ETSI GR ENI 004 V2.2.1 (2021-12)	Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI
9	ETSI GS ENI 001 V3.1.1 (2020-12)	Experiential Networked Intelligence (ENI); ENI use cases
10	ETSI GS ENI 005 V2.1.1 (2021-12)	Experiential Networked Intelligence (ENI); System Architecture
11	ETSI GS MEC 009 V1.1.1 (2017-07)	Mobile Edge Computing (MEC); General principles for Mobile Edge Service APIs
12	ETSI GS MEC 003 V3.1.1 (2022-03)	Multi-access Edge Computing (MEC); Framework and Reference Architecture
13	ETSI GR MEC 031 V2.1.1 (2020-10)	Multi-access Edge Computing (MEC) MEC 5G Integration
14	ETSI GR MEC 024 V2.1.1 (2019-11)	Multi-access Edge Computing (MEC); Support for network slicing
15	ETSI GS MEC-IEG 004 V1.1.1 (2015-11)	Mobile-Edge Computing (MEC); Service Scenarios
16	ETSI GS MEC-IEG 005 V1.1.1 (2015-08)	Mobile-Edge Computing (MEC); Proof of Concept Framework
17	ETSI GS NFV 003 V1.1.1 (2013-10)	Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV
18	ETSI GS NFV-IFA 010 V4.2.1 (2021-05)	Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification
19	ETSI GR NFV-MAN 001 V1.2.1 (2021-12)	Network Functions Virtualisation (NFV); Management and Orchestration; Report on Management and Orchestration Framework
20	ETSI GS NFV-PER 001 V1.1.1 (2014-06)	Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises
21	ETSI GS NFV-EVE 005 V1.1.1 (2015-12)	Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework
22	ETSI GS NFV-SWA 001 V1.1.1 (2014-12)	Network Functions Virtualisation (NFV); Virtual Network Functions Architecture
23	ETSI GS NFV 002 V1.1.1 (2013-10)	Network Functions Virtualisation (NFV); Architectural Framework
24	ETSI GS NFV-REL 001 V1.1.1 (2015-01)	Network Functions Virtualisation (NFV); Resiliency Requirements
25	ETSI GS NFV 004 V1.1.1 (2013-10)	Network Functions Virtualisation (NFV); Virtualisation Requirements
26	ETSI GS NFV-SEC 003 V1.1.1 (2014-12)	Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance
27	ETSI GS NFV-TST 001 V1.1.1 (2016-04)	Network Functions Virtualisation (NFV); Pre-deployment Testing; Report on Validation of NFV Environments and Services
28	ETSI GS NFV-SOL 003 V2.3.1 (2017-07)	Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; RESTful protocols specification for the Or-Vnfm Reference Point
29	ETSI GR PDL 008 V1.1.1 (2021-09)	Permissioned Distributed Ledger (PDL); Research and Innovation Landscape

30	ETSI TS 138 424 V15.0.0 (2018-07)	5G; NG-RAN; Xn data transport (3GPP TS 38.424 version 15.0.0 Release 15)
31	ETSI TS 123 502 V15.2.0 (2018-06)	5G; Procedures for the 5G System (3GPP TS 23.502 version 15.2.0 Release 15)
32	ETSI TS 136 101 V14.5.0 (2017-11)	LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101 version 14.5.0 Release 14)
33	ETSI TS 123 501 V15.2.0 (2018-06)	5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)
34	ETSI TS 138 331 V15.3.0 (2018-10)	5G; NR; Radio Resource Control (RRC); Protocol specification (3GPP TS 38.331 version 15.3.0 Release 15)
35	ETSI TS 102 690 V2.1.1 (2013-10)	Machine-to-Machine communications (M2M); Functional architecture
36	ETSI TS 133 185 V14.0.0 (2017-07)	LTE; 5G; Security aspect for LTE support of Vehicle-to-Everything (V2X) services (3GPP TS 33.185 version 14.0.0 Release 14)
37	ETSI TS 124 386 V14.1.0 (2017-07)	LTE; User Equipment (UE) to V2X control function; protocol aspects; Stage 3 (3GPP TS 24.386 version 14.1.0 Release 14)
38	ETSI TS 138 101-1 V15.2.0 (2018-07)	5G; NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone (3GPP TS 38.101-1 version 15.2.0 Release 15)
39	ETSI TS 138 421 V15.0.0 (2018-07)	5G; NG-RAN; Xn layer 1 (3GPP TS 38.421 version 15.0.0 Release 15)
40	ETSI TS 138 413 V15.0.0 (2018-07)	5G; NG-RAN; NG Application Protocol (NGAP) (3GPP TS 38.413 version 15.0.0 Release 15)
41	ETSI TS 123 502 V15.3.0 (2018-09)	5G; Procedures for the 5G System (3GPP TS 23.502 version 15.3.0 Release 15)
41	ETSI TS 133 501 V15.1.0 (2018-07)	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.1.0 Release 15)
43	ETSI TS 138 401 V15.2.0 (2018-07)	5G; NG-RAN; Architecture description (3GPP TS 38.401 version 15.2.0 Release 15)
44	ETSI TS 138 473 V15.3.0 (2018-10)	5G; NG-RAN; F1 Application Protocol (F1AP) (3GPP TS 38.473 version 15.3.0 Release 15)
45	ETSI GR MEC 018 V1.1.1 (2017-10)	Mobile Edge Computing (MEC); End to End Mobility Aspects
46	ETSI TS 102 689 V1.1.1 (2010-08)	Machine-to-Machine communications (M2M); M2M service requirements
47	ETSI TR 103 290 V1.1.1 (2015-04)	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
48	ETSI TR 102 857 V1.1.1 (2013-08)	Machine-to-Machine communications (M2M); Use Cases of M2M applications for Connected Consumer
49	ETSI TS 102 689 V2.1.1 (2013-07)	Machine-to-Machine communications (M2M); M2M service requirements
50	ETSI TR 101 584 V2.1.1 (2013-12)	Machine-to-Machine communications (M2M); Study on Semantic support for M2M Data
51	ETSI TS 118 102 V3.1.2 (2021-01)	oneM2M Requirements (oneM2M TS-0002 version 3.1.2 Release 3)
52	ETSI TS 118 101 V4.15.0 (2022-09)	oneM2M; Functional Architecture (oneM2M TS-0001 version 4.15.0 Release 4)
53	ETSI TS 103 780 V1.1.1 (2022-08)	SmartM2M; SAREF: oneM2M usage guidelines
54	ETSI TR 103 675 V1.1.1 (2020-12)	SmartM2M; AI for IoT: A Proof of Concept

55	ETSI TS 118 130 V4.0.1 (2023-06)	oneM2M; Ontology based Interworking (oneM2M TS-0030 version 4.0.1 Release 4)
56	ETSI TS 118 114 V4.0.1 (2023-11)	oneM2M; LWM2M Interworking (oneM2M TS-0014 version 4.0.1 Release 4)
57	ETSI TR 103 375 V1.1.1 (2016-10)	SmartM2M; IoT Standards landscape and future evolutions
58	ETSI TS 118 110 V4.0.1 (2023-08)	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 4.0.1 Release 4)
59	ETSI TS 118 120 V3.0.1 (2021-01)	oneM2M; WebSocket Protocol Binding (oneM2M TS-0020 version 3.0.1 Release 3)
60	ETSI TR 118 568 V5.0.1 (2023-08)	AI enablement to oneM2M (oneM2M TR-0068 version 5.0.1)
61	ETSI TR 103 536 V1.1.2 (2019-12)	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms
62	ETSI TS 118 108 V4.4.1 (2023-08)	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 4.4.1 Release 4)
63	ETSI TR 103 839 V1.1.1 (2023-09)	SmartM2M; Scenarios for evaluation of oneM2M deployments
64	ETSI TR 103 535 V1.1.1 (2019-10)	SmartM2M; Guidelines for using semantic interoperability in the industry
65	ETSI TS 118 112 V2.2.2 (2020-03)	oneM2M; Base Ontology (oneM2M TS-0012 version 2.2.2 Release 2A)
66	TSI TS 103 410-5 V1.1.2 (2020-05)	SmartM2M; Extension to SAREF; Part 5: Industry and Manufacturing Domains
67	ITU-T Y.4100	Y.4100: Common requirements of the Internet of things
68	ITU-T Y.4101	Y.4101: Common requirements and capabilities of a gateway for Internet of things applications
69	ITU-T Y.4102	Y.4102: Requirements for Internet of things devices and operation of Internet of things applications during disasters
70	ITU-T Y.4103	Y.4103: Common requirements for Internet of things (IoT) applications
71	ITU-T Y.4104	Y.4104: Service description and requirements for ubiquitous sensor network middleware
72	ITU-T Y.4111	Y.4111: Semantics based requirements and framework of the Internet of things
73	ITU-T Y.4113	Y.4113: Requirements of the network for the Internet of things
74	ITU-T Y.4114	Y.4114: Specific requirements and capabilities of the Internet of things for big data
75	ITU-T Y.4115	Y.4115: Reference architecture for IoT device capability exposure
76	ITU-T Y.4122	Y.4122: Requirements and capability framework of the edge-computing-enabled gateway in the Internet of things
77	ITU-T Y.4200	Y.4200: Requirements for the interoperability of smart city platforms
78	ITU-T Y.4201	Y.4201: High-level requirements and reference framework of smart city platforms
79	ITU-T Y.4203	Y.4203: Requirements of things description in the Internet of things
80	ITU-T Y.4208	Y.4208: Internet of things requirements for support of edge computing
81	ITU-T Y.4210	Y.4210: Requirements and use cases for universal communication module of mobile IoT devices
82	ITU-T Y.4112	Y.4112: Requirements of the plug and play capability of the Internet of things

83	ITU-T Y.4117	Y.4117: Requirements and capabilities of the Internet of things for support of wearable devices and related services
84	ITU-T Y.4118	Y.4418: Gateway functional architecture for Internet of things applications
85	ITU-T Y.4471	Y.4471: Functional architecture of network-based driving assistance for autonomous vehicles
86	ITU-T Y.4472	Y.4472: Open data application programming interfaces (APIs) for IoT data in smart cities and communities
87	ITU-T Y.4500.1	Y.4500.1: oneM2M – Functional architecture
88	ITU-T Y.4500.2	Y.4500.2: oneM2M – Requirements
89	ITU-T Y.4500.3	Y.4500.3: oneM2M – Security solutions
90	ITU-T Y.4500.10	Y.4500.10: oneM2M – MQTT protocol binding
91	ITU-T Y.4000	Y.4000: Overview of the Internet of things
92	ITU-T Y.4050	Y.4050: Terms and definitions for the Internet of things
93	ITU-T Y.3500	Y.3500: Information technology – Cloud computing – Overview and vocabulary
94	ITU-T Y.3501	Y.3501: Cloud computing – Framework and high-level requirements
95	ITU-T Y.3505	Y.3505: Cloud computing – Overview and functional requirements for data storage federation
96	ITU-T Y.3506	Y.3506: Cloud computing - Functional requirements for cloud service brokerage
97	ITU-T Y.3510	Y.3510: Cloud computing infrastructure requirements
98	ITU-T Y.3512	Y.3512: Cloud computing - Functional requirements of Network as a Service
99	ITU-T Y.3513	Y.3513: Cloud computing - Functional requirements of Infrastructure as a Service
100	ITU-T Y.3531	Y.3531: Cloud computing - Functional requirements for machine learning as a service
101	ITU-T Y.3535	Y.3535: Cloud computing – Functional requirements for a container
102	ITU-T Y.3536	Y.3536: Cloud computing – Functional architecture for cloud service brokerage
103	ITU-T Y.3540	Y.3540: Edge computing – Overview and high-level requirements
104	ITU-T Y.3550	Y.3550: Cloud computing – Requirements for artificial intelligence based cloud service development and operation management
105	ITU-T Y.3600	Y.3600: Big data – Cloud computing based requirements and capabilities
106	ITU-T Y.3605	Y.3605: Big data - Reference architecture
107	ITU-T Y.3650	Y.3650: Framework of big-data-driven networking
108	ITU-T Y.3651	Y.3651: Big-data-driven networking - mobile network traffic management and planning
109	ITU-T Y.3652	Y.3652: Big data driven networking – requirements
110	ITU-T Y.3653	Y.3653: Big data driven networking – functional architecture
111	ITU-T Y.3654	Y.3654: Big data driven networking – Machine learning mechanism
112	ITU-T Y.3655	Y.3655: Big data driven networking - Management and control mechanisms
113	ITU-T Y.3656	Y.3656: Big data driven networking-mechanism of network service provisioning
114	ITU-T X.1601	X.1601: Security framework for cloud computing
115	ITU-T X.1602	X.1602: Security requirements for software as a service application environments

116	ITU-T X.1604	X.1604: Security requirements of Network as a Service (NaaS) in cloud computing
117	ITU-T X.1641	X.1641: Guidelines for cloud service customer data security
118	ITU-T X.1642	X.1642: Guidelines for the operational security of cloud computing
119	ITU-T X.1643	X.1643: Security requirements and guidelines for virtualization containers in cloud computing environments
120	ITU-T X.1644	X.1644: Security guidelines for distributed cloud
121	IEEE P2413	Standard for an Architectural Framework for the Internet of Things
122	IEEE P1935	Standard for Edge/Fog Manageability and Orchestration
123	IEEE P2302	Standard for Intercloud Interoperability and Federation (SIIF)
124	ISO/IEC 30179:2023	Overview and general requirements of IoT system for ecological environment monitoring
125	ISO/IEC 30141:2018	Internet of Things (IoT) Reference Architecture
126	ISO/IEC TR 30176:2021	Internet of Things (IoT) - Integration of IoT and DLT/blockchain: Use cases
127	ISO/IEC 30161-2:2023	Internet of Things (IoT) Data exchange platform for IoT services. Part 2: Transport interoperability between nodal points
128	ISO/IEC 21823-3:2023	Internet of things (IoT) Interoperability for IoT systems. Part 3: Semantic interoperability
129	ISO/IEC 21823-4:2022	Internet of things (IoT) Interoperability for IoT systems. Part 4: Syntactic interoperability
130	ISO/IEC TR 30164:2020	Internet of things (IoT) Edge computing
131	ISO/IEC TR 30166:2020	Internet of things (IoT) Industrial IoT
132	ISO/IEC TR 22417:2017	Information technology, Internet of things (IoT) use cases
133	ISO/IEC 27400:2022	Cybersecurity, IoT security and privacy, Guidelines
134	ISO/IEC 21558-3:2022	Telecommunications and information exchange between systems - Future network architecture, Part 3: Networking of everything
135	TIC4.0 Release 2023.009	Semantics, Dataset, Data Model and Definitions
136	TIC4.0 Release 2022.003	Semantics, Dataset Roadmap, Data Model and Definitions of Cycle (new update), Carrier Visit, Cargo Visit, Health, Drive and Movement, CHE Data Model (new update) and TOS Data Model (new update)
137	TIC4.0 Release 2021.001	Container Handling Equipment Activity and Power Source Concepts and Definitions
138	IEEE P1912	Standard for Privacy and Security Architecture for Consumer Wireless Devices
139	IEEE P1931.1	Standard for an Architectural Framework for Real-time Onsite Operations Facilitations (ROOF) for the Internet of Things
140	IEEE P1934	Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing
141	IEEE P2301	Guide for Cloud Portability and Interoperability Profiles (CPIP)
142	IEEE P2303	Standard for Adaptive Management of Cloud Computing Environments
143	IEEE P2557	Standard for Ambient Genetics Frameworks
144	IEEE P2558	Standard for Ambient Objects
145	IEEE P2668	Standard for Maturity Index of Internet-of-things: Evaluation, Grading and Ranking
146	ISO 19650-1	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 1: Concepts and principles

147	ISO 19650-2	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 2: Delivery phase of the assets
148	ISO 19650-3	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 3: Operational phase of the assets
149	ISO 19650-4	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 4: Information exchange
150	ISO 19650-5	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 5: Security-minded approach to information management
151	ISO 19650-6	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM), Part 6: Health and safety information
152	CEN/TR 17920	BIM in infrastructure - Standardization need and recommendations
153	CEN/TR 17945:2023	Textiles and textile products - Textiles with integrated electronics and ICT - Definitions, categorisation, applications and standardisation needs
154	CEN ISO/TR 23383:2020	Textiles and textile products - Smart (Intelligent) textiles - Definitions, categorisation, applications and standardization needs (ISO/TR 23383:2020)

3.2.7. Activities summary vs KPIs

ASSIST-IOT standardisation activities started around different technical subjects to analyse, follow up, identify gaps and contribute in different SDOs but focus on main SDOs and initiative that are most active currently in our technical domains. To evaluate these activities, the KPIs were defined. In table below, the targeted and achieved KPIs values in the project are presented. **All KPIs exceeded the assumed targeted values**, where contributions to the recommendations, technical reports and white papers are more than twice larger than planned one.

Table 7. Standardisation activities KPIs

KPI	Achieved	Target M41
Communications to improve existing standards	**7**	**6**
Recommendations in relevant SDOs including Technical Reports, White Papers and Position Papers	**25**	**10**
SDOs and pre-normative initiatives engaged	**42**	**40**
Supported standards in ASSIST-IoT	**53**	**40**
Identified standards related to ASSIST-IoT	**154**	**120**

4. Standardization activities summary

ASSIST-IoT standardisation activities was related to different technical domains. Estimated effort per technical domain in the figure 4 is presented. Most of the standardisation work was devoted to IoT and use cases subjects, next for the cloud computing and networking subjects, then on security, AI and other use case specific issues.

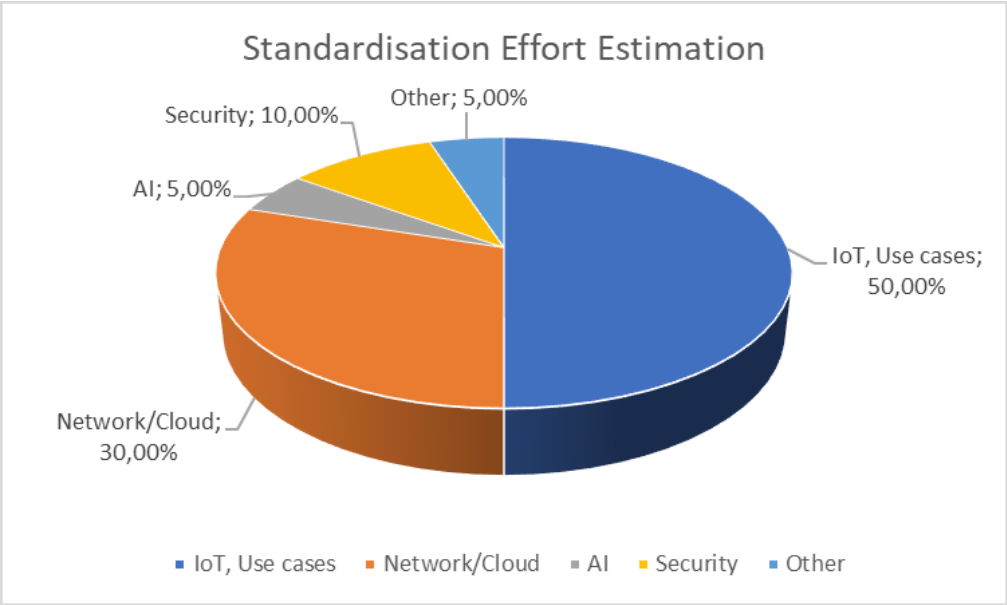

Figure 4. Estimated standardisation effort per technical domain

The summary of different activities in the standardisation areas in ASSIST-IoT project is presented for each of SDOs and initiatives. The main focus was on 3 SDOs and 2 initiatives. Estimated effort per SDO/initiative in the Figure 5 is presented. The effort was divided mostly among ETSI, ITU-T, AIOTI and IEEE SA.

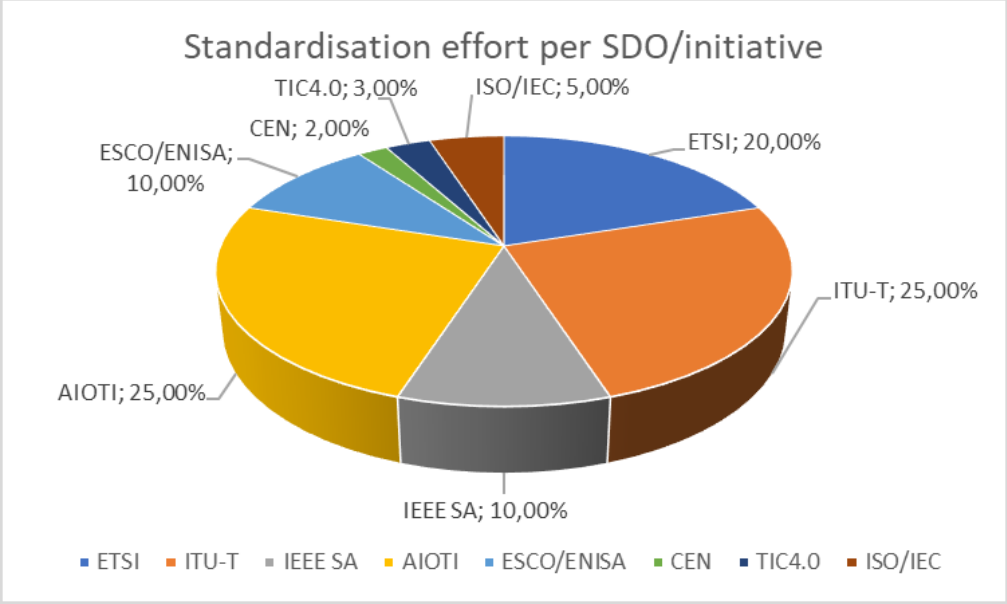

Figure 5. Estimated standardisation effort per SDO/initiative

Below the short summary of the activities per SDO/initiative is collected.

1. *Short summary of the work done with **ETSI** (by ASSIST-IoT):*
   - Active participation in the ETSI standardisation work using membership and cooperation through AIOTI.
   - Following the standardisation work and contribution to Technical Reports (use cases for human interfaces in IoT services).
   - Potential contributions after completed project for SmartM2M and NFV subjects.

2. *Short summary of the work done with **ITU-T** (by ASSIST-IoT):*
   - Active participation in the ITU-T standardisation work using OPL partner membership.
   - Following up the standardisation work items and contribution to SG20: IoT, smart cities & communities.
   - Following up the SG13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure
   - Participation in ITU-T meetings: SG13 and SG20.

3. *Short summary of the work done with **IEEE SA** (by ASSIST-IoT):*
   - Active participation in the selected Working Groups: Collaborative Edge Computing, C/AISC/CEC.
   - Following up the selected Working Groups: Tactile Internet, COM/MobiNet-SC/TI, Security Assessment Framework for the IoT Application Deployments, COM/MobiNet-SC/IOTAF, Federated Machine Learning, C/AISC/FML.
   - IEEE SA Training + Development programs – the course has been passed.
   - Publishing in IEEEXplore Digital Library

4. *Short summary of the work done with **AIOTI** (by ASSIST-IoT):*
   - Active participation in the AIOTI Standardisation WG.
   - Contributions to white papers, position papers and technical reports in different technical subjects: HLA, data spaces, edge computing, IoT and edge computing landscape and gaps analysis.
   - Align technical architecture of ASSIST-IoT with the specifications of HLA release 5.0 (see deliverable D3.6).

5. *Short summary of the work done with the **ESCO/ENISA** (by ASSIST-IoT):*
   - Active participation in the working groups and follow up by S21SEC.
   - Identification of gaps in cybersecurity domain.
   - Contribution to cybersecurity white papers and best practices.

6. *Short summary of the work done in use case specific aspects (by ASSIST-IoT):*
   - Active participation in TIC4.0 initiative and activities regarding Pilot 1 Port automation.
   - CENLEC organisation activities in case of Pilot 2 related to safety of workers.

5. References

[1] "Artificial Intelligence and future directions for ETSI", ETSI White Paper No. #34, 1st edition – June 2020, ISBN No. 979-10-92620-30-1, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp34_Artificial_Intellignce_and_future_directions_for_ETSI.pdf

[2] "ENI Vision: Improved Network Experience using Experiential Networked Intelligence", ETSI White Paper No. 44, 1st edition – March 2021, ISBN No. 979-10-92620-38-8, https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44_ENI_Vision.pdf

[3] "An Introduction of Permissioned Distributed Ledger (PDL)", ETSI White Paper No. #48, 1st edition – January 2022, ISBN No. 979-10-9262036-6, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf

[4] "ENISA Good practices for IoT and Smart Infrastructures tool, November 2017" [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT. [Accessed 14 2022]

[5] "ENISA IoT Security Standards Gaps Analysis. January 2019". [Online], Available https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis/at_download/fullReport [Accessed 14 2022]

[6] MeliCERT Cyber Security Platform https://github.com/melicertes/csp