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

D9.3 Report on Contribution to Standardisation and International Fora

Deliverable No.	D9.3	**Due Date**	30-Apr-2022
Type	Report	**Dissemination Level**	Public
Version	1.0	**WP**	WP9
Description	Report on actions undertaken by the Consortium, standardisation activities and contributions to various international fora.		

Copyright

Copyright © 2020 the ASSIST-IoT Consortium. All rights reserved.

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

This document contains material, which is the copyright of certain ASSIST-IoT consortium parties, and may not be reproduced or copied without permission. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The information contained in this document is the proprietary confidential information of the ASSIST-IoT Consortium (including the Commission Services) and may not be disclosed except in accordance with the Consortium Agreement. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the Project Consortium as a whole nor a certain party of the Consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is subject to change without notice.

The content of this report reflects only the authors' view. The Directorate-General for Communications Networks, Content and Technology, Resources and Support, Administration and Finance (DG-CONNECT) is not responsible for any use that may be made of the information it contains.

Authors

Name	Partner	e-mail
Ignacio Lacalle Úbeda	P01 UPV	iglaub@upv.es
Marcin Paprzycki	P03 IBSPAN	paprzyck@ibspan.waw.pl
Francisco Blanquer	P05 TL	HO.FBLANQUER@terminal-link.com
Anna Dąbrowska	P07 CIOP-PIB	andab@ciop.lodz.pl
Grzegorz Owczarek	P07 CIOP-PIB	growc@ciop.lodz.pl
Piotr Dymarski	P08 MOW	P.Dymarski@mostostal.waw.pl
Oscar López Pérez	P13 S21SEC	olopez@s21sec.com
Zbigniew Kopertowski	P15 OPL	zbigniew.Kopertowski@orange.com

History

Date	Version	Change
23-Dec-2021	0.1	ToC closed , initial partners assignment
15-Mar-2022	0.2	Second version
7-Apr-2022	Prefinal	Ready to Internal review
30-Apr-2022	Final	Final version

Key Data

Keywords	Standardization
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 in the first half of the project. Deliverable includes analysis of standardisation bodies and pre-normative initiatives, their structure, 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, BDVA, ECSO, ENISA and TIC4.0. Next, the ASSIST-IoT potential contribution areas related to the designed in the project solutions are presented. We grouped the activities in the following domains:

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

According to the committed goals of WP9, T9.3 objective is to follow up the standardisation activities in the above domains and analysis of the gaps in the standardisation documents and ongoing work for selected SDO's and initiatives. Then, such analysis allows for identification of possible and required contributions in the relevant technical subjects and SDO's. Such approach is one of the elements of our standardisation work strategy in the project. In this strategy we planned set of actions according to defined KPI's.

For the first period of the project, the assumed KPI's for the standardisation activities are being achieved.

The list of already performed and planned contributions and actions is also presented in this report.

Finally, at the end the summary of the standardisation work and future plans are presented.

Table of contents

List of tables

List of figures

List of acronyms

Acronym	Explanation
3GPP	3rd Generation Partnership Project
5G	5th Generation
5G IA	5G Infrastructure Association
5G PPP	5G Public-Private Partnership
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
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 T9.3 – 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 one of the deliverables in WP9 and directly linked to T9.3 – Standardisation and Pre-normative Activities.
Milestones	N/A
Deliverables	D9.3 provides a comprehensive description and analysis of SDO's and pre-normative initiatives, standardisation gaps analysis, achievements and planned activities in the standardisation work.

1.1. The rationale behind the structure

This document is divided into 8 sections, which present standardisation work carried out in the project and future plans. In detail:

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

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

Section 3: Describes ASSIST-IoT relevant contribution domains, which are related to technical solutions designed in the project like Internet of Things domain, Artificial Intelligence, Cybersecurity, Networking and Edge Cloud.

Section 4: Contains the analysis of standardisation gaps in different technical domains.

Section 5: Presents updated standardisation strategy assumed in the project.

Section 6: Includes the description about standardisation contributions already performed and planned for the future.

Section 7: Shows the achievements in the standardisation work and KPI's related to the standardisation activities.

Section 8: This section concludes the document and summarises future plans.

2. Analysis of Standardisation Bodies and Initiatives

According to deliverable D9.2 where the first short analysis of the relevant standardisation organisations and initiatives for the project was conducted, we are focusing 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

ETSI was set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) in response to proposals from the European Commission. Currently, in ETSI 900+ member organizations are drawn from over 60 countries and five continents.

ETSI provide recommendations in different key global technologies, with most relevant to ASSIST-IoT project results areas like in IoT, AI, Networks and Security Sectors. Several **ETSI Industry Specification Groups (ISG)** are target for future project contributions, 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) and the recently launched),
- **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).

The process of creating and issuing the standards, specifications and reports with possible entry points for ASSIST-IoT project are shown in the Figure 1.

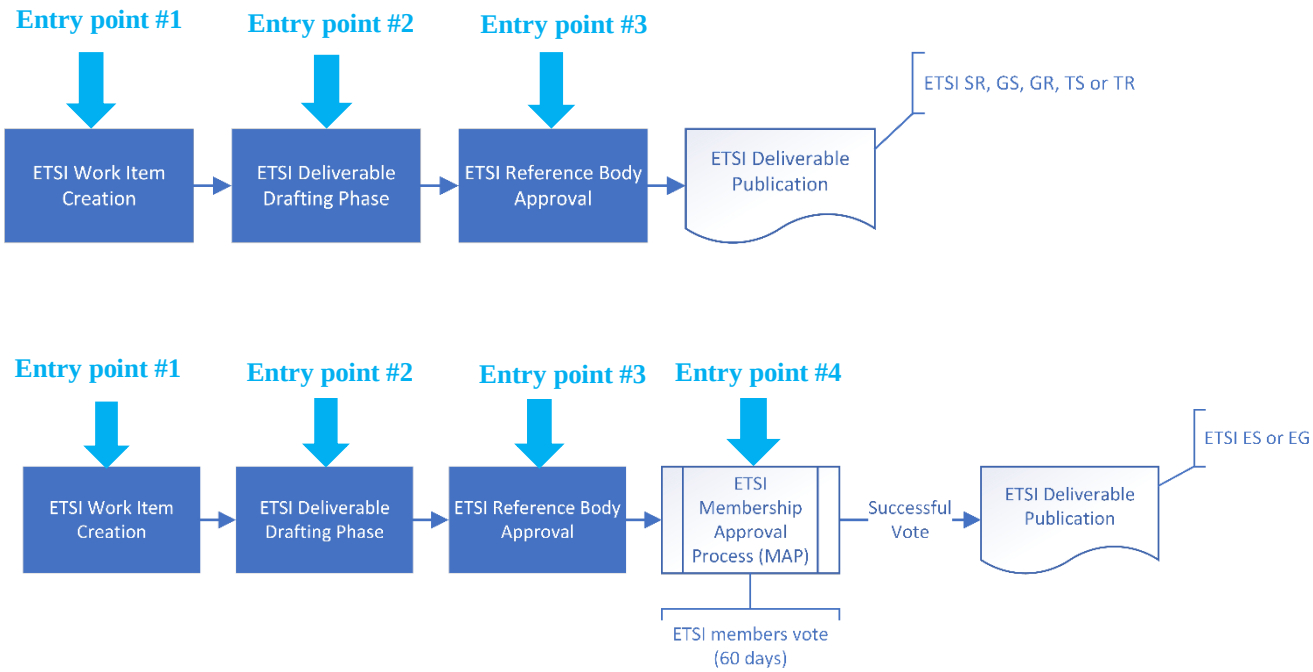

Figure 1. ETSI documentation process with ASSIST-IoT entry points.

The process of creating and publication of ETSI documents consists of 3 or 4 stages:

1. Work item creation – with entry point #1 for ASSIST-IoT using project partners as a members of ETSI or AIOTI (AIOTI cooperates with ETSI).
2. Deliverable drafting phase – with entry point #2 – project partners as members of ETSI or AIOTI.
3. Reference body approval – with entry point #3 – project partners as members of ETSI technical group.
4. Approval with voting – project partners as members of ETSI.

ETSI is a key player on the international standards scene and publishes between 2,000 and 2,500 standards every year. 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 most project relevant specifications (one contributed by ASSIST-IoT) are the following:

- ETSI TR 103 778 V1.1.1 (2021-12) SmartM2M, Use cases for cross-domain data usability of IoT devices **(ASSIST-IoT contribution**). The objective of the present document is to identify, select and describe use cases where the IoT data and services require data usability specifications for machines consuming data for AI (for example machine learning). Enabling data usability with AI approach will also be considered.
- ETSI TR 103 621 V1.1.1 (2022-03) SmartM2M, Guide to Cyber Security for Consumer Internet of Things. Guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices.
- ETSI SR 003 680 V1.1.1 (2020-03) SmartM2M. Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach. It is introducing, in a relatively non-technical manner, to some of the main issues that individuals and organizations should address when they face the development of an IoT system. A strong emphasis is put on interoperability, security, privacy and standards in support.
- ETSI TS 103 264 V3.1.1 (2020-02) SmartM2M, Smart Applications; Reference Ontology and oneM2M Mapping, standardized framework for the Smart Applications Reference ontology based on the results

of a European Commission Study Group on Smart Appliances ontologies and of different Specialist Task Forces that have supported the maintenance and evolution of the ontology taking into account all the interest of the relevant stakeholders.

- ETSI TR 103 527 V1.1.1 (2018-07) SmartM2M, Virtualized IoT Architectures with Cloud Back-ends, addresses the rationale and requirements for the use of virtualization - and of the cloud in general - in support of IoT systems. It also introduces some features that will be key for the definition and further implementation of virtualized IoT systems such as microservices; provides the identification of new architectural elements (components, mappings, Application Programming Interfaces (API), etc.) that are required to address IoT on a cloud back-end.
- ETSI TR 103 529 V1.1.1 (2018-08) SmartM2M, IoT over Cloud back-ends: A Proof of Concept, Recalls the main elements of the Proof-of-Concept (PoC) in support of IoT Virtualization: use case description, high-level architecture of the application developed, main technical choices. Presents the main implementation choices. Outlines the lessons learned and the possible impact of future IoT Virtualization implementations
- ETSI TR 103 675 V1.1.1 (2020-12) SmartM2M, AI for IoT: A Proof of Concept. Description of the implementation: architecture, oneM2M platform used, open source support, etc.
- ETSI TR 103 674 V1.1.1 (2021-02) SmartM2M, Artificial Intelligence and the oneM2M architecture. document is addressing the issues related to the introduction of AI into IoT systems and, as first priority, into the oneM2M architecture.
- ETSI GR ENI 004 V2.2.1 (2021-12) Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI. Document provides terms and definitions used within the scope of the ETSI ISG ENI. The purpose is to define a common lexicon for use across all deliverables of ENI.
- ETSI GS ENI 001 V3.1.1 (2020-12) Experiential Networked Intelligence (ENI); ENI use cases. Document specifies a collection of use cases from a variety of stakeholders, where the use of an Experiential Networked Intelligence (ENI) system can be applied to the fixed network, the mobile network, or both, to enhance the operator experience through the use of network intelligence.
- ETSI GS ENI 005 V2.1.1 (2021-12) Experiential Networked Intelligence (ENI); System Architecture. Document specifies the functional architecture of an ENI System, which is a high-level decomposition of an ENI System into its major components, along with a characterization of the externally visible behaviour (e.g. as defined by a set of reference points) of the components.
- ETSI GS MEC 003 V3.1.1 (2022-03) Multi-access Edge Computing (MEC); Framework and Reference Architecture. Document provides a framework and reference architecture for Multi-access Edge Computing. It describes a MEC system that enables applications to run efficiently and seamlessly in a multi-access network.
- ETSI GR MEC 031 V2.1.1 (2020-10) Multi-access Edge Computing (MEC) MEC 5G Integration. Document describes the key study areas in the MEC 5G integration.
- ETSI GR MEC 024 V2.1.1 (2019-11) Multi-access Edge Computing (MEC); Support for network slicing. Document focuses on identifying the MEC functionalities to support network slicing.
- ETSI GS NFV-IFA 010 V4.2.1 (2021-05) Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Functional requirements specification. Document specifies functional requirements for NFV management and orchestration, and general guidelines and requirements for NFV management and orchestration interface design.
- ETSI GR NFV-MAN 001 V1.2.1 (2021-12) Network Functions Virtualisation (NFV); Management and Orchestration; Report on Management and Orchestration Framework. Document describes the management and orchestration framework for the provisioning of Virtualised Network Function (VNF), and the related operations, such as the configuration of the virtualised network functions and the infrastructure these functions run on.
- ETSI GR PDL 008 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Research and Innovation Landscape, document shows the current research and innovation programmes related to permissioned

distributed ledgers, distributed digital ledger technologies and blockchain with the goal of identifying advanced technologies and innovative research results relevant or essential to PDL standardization.

In the main areas of interest in the project the ongoing work and future planed subjects are the following:

- SmartM2M Technical Committee includes:
  - Smart Applications; Reference Ontology and oneM2M Mapping.
  - oneM2M deployment guidelines and best practices.
  - SAREF: AI Support for ontologies.
  - Study for SAREF ontology patterns and usage guidelines.
  - Among others Smart Cities Domain and Automotive Domain - major revision of ontology extension, using updated reference ontology patterns.
- ENI Industry Specification Group (see also in [1][2]) includes:
  - System architecture information and data models.
  - Evolution of use cases, requirements, and how they relate to the system architecture.
  - System architecture intent policy model and its scope within policy management.
  - System architecture ontologies, semantics and an intent description language.
  - Evaluation of categories for AI application to networks.
  - ENI requirements update - how intelligence is applied to the network and applications in different scenarios to improve experience of service provision and network operation.
- MEC Industry Specification Group includes:
  - Framework and Reference Architecture - to align the MEC architecture with the other MEC specifications.
  - Study on MEC Security - cover the themes of application and platform security, Zero-Trust Networking, and security requirements for MEC Federations.
  - Study on MEC Application Slices - study the potential requirements and enhancements to the MEC system needed to support MEC Application Slices.
- PDL Industry Specification Group includes (see also [3]):
  - Development of the Reference Architecture Framework.
  - Use of PDL to support distributed data management.
  - Research Landscape - the exchange of information within ETSI ISG PDL 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.

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. From inception of ITU-T in 1865, the work on standardisation in broad range of domains is conducted in Study Groups (SG). There are 11 SG where most relevant groups for contributions 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 are the following series (taking into account ASSIST-IoT scope):

- **X series**: Data networks, open system communications and security
  - **X.200-X.299**: Open Systems Interconnection
- **Y series**: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
  - **Y.2000-Y.2999**: Next Generation Networks
  - **Y.3000-Y.3499**: Future networks
  - **Y.3500-Y.3599**: Cloud Computing
  - **Y.3600-Y.3799**: Big Data
  - New recommendations:
    - Y.3654 - Big data driven networking - Machine learning mechanism,
    - Y.3535 - Cloud computing – Overview and functional requirements for data storage federation,
    - Y.3536 - Cloud computing - Functional architecture for cloud service brokerage,
    - Y.3115 - AI enabled cross-domain network architectural requirements and framework for future networks including IMT-2020,
    - Y.3116 - Traffic typization IMT-2020 management based on an artificial intelligent approach.

- **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:
  - **X.1500-X.1599**: Cybersecurity information exchange
  - **X.1600-X.1699**: Cloud computing security
  - **X.1750-X.1799**: Data security
  - **X.1800-X.1819**: IMT-2020 Security

- **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 recommendations released in this SG in relation to ASSIST-IoT interest are the following:

- **Y series**: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
  - **Y.2000-Y.2999**: Next Generation Networks
    - **Y.2000-Y.2099**: Frameworks and functional architecture models
    - **Y.2200-Y.2249**: Service aspects: Service capabilities and service architecture
    - **Y.2250-Y.2299**: Service aspects: Interoperability of services and networks in NGN
  - **Y.4000-Y.4999**: Internet of things and smart cities and communities
    - **Y.4100-Y.4249**: Requirements and use cases
    - **Y.4250-Y.4399**: Infrastructure, connectivity and networks
    - **Y.4400-Y.4549**: Frameworks, architectures and protocols
    - **Y.4550-Y.4699**: Services, applications, computation and data processing
    - **Y.4700-Y.4799**: Management, control and performance
    - **Y.4800-Y.4899**: Identification and security
    - **Y.4900-Y.4999**: Evaluation and assessment
    - New recommendations:
      - Y.4122, Y.IoT-EC-GW, Requirements and capability framework of edge computing-enabled gateway in the IoT,
      - Y.4212 , Y.IoT-NCM-reqts, Requirements and capabilities of network connectivity management in the Internet of things,
      - Y.4478, Y.IoT-SCS Requirements and functional architecture for smart construction site services,
      - Y.4563, Y.DPM-interop, Requirements and functional model to support data interoperability in IoT environments,
      - Y.4810 , Y.Data.Sec.IoT-Dev Requirements of data security for the heterogeneous IoT devices.

Beside SG there are Focus Groups where two groups are interesting for the scope of ASSIST-IoT:

- **FG-AN** (Focus Group on Autonomous Networking): This group pursues the definition (and publication of reference documents) of future autonomous real-time networks and the delivery of an open platform to test pre-standards technologies. It is sub-divided in 3 working groups (requirements, architecture and enablers and proof of concept), and the contributions can be made only by members (Orange Poland as a partner in the ASSIST-IoT project) before the scheduled group meetings via the description of the contribution using a public template. This focus group is of interest for the scope of WP4 of ASSIST-IoT, in particular for the works to be conducted under task T4.2.
- **FG-TBFxG** (Focus Group on Testbeds Federations for IMT-2020 and beyond): this group will serve as a platform to harmonize testbeds specifications across SDOs/Fora and play a role in providing a platform to share views, to develop a series of deliverables and it will also offer a platform to different stakeholders to share their initiatives and projects aligned with the outlined vision and the desired Ecosystem on Testbeds Federations.

The process of creating and issuing the standards, specifications and reports with possible entry points for ASSIST-IoT project are shown in the Figure 2.

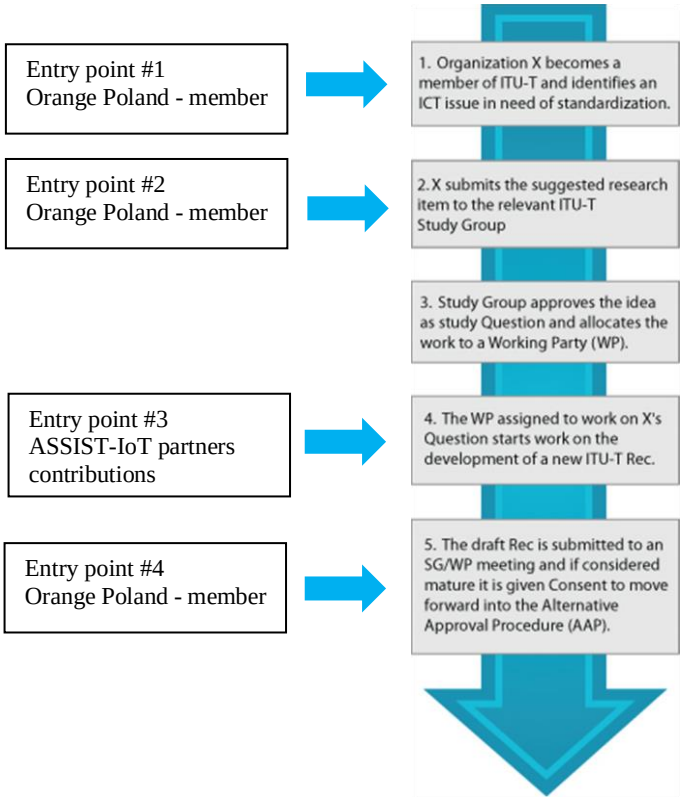

Figure 2. ITU-T standardisation process with ASSIST-IoT entry points.

The process of developing of ITU-T recommendations consists of 5 stages:

1. Member of ITU-T propose need of standardisation – entry point #1, Orange Poland as a member of ITU-T can issue the standardisation need (in cooperation with ASSIST-IoT project partners).
2. Member of ITU-T submit the suggested research item to the relevant ITU-T Study Group – entry point #2 – Orange Poland as a member of ITU-T can submit the standardisation subject (in cooperation with ASSIST-IoT project partners).
3. Study Groups approves submission.
4. Work on Recommendation – entry point #3 – Orange Poland as a member of ITU-T with project partners cooperation can work on submitted subject or contribute to any other standardisation work in different subjects.
5. Approval of recommendation – Orange Poland as a member of ITU-T is attending in approval process.

From point of view of the ASSIST-IoT project the ongoing standardisation work and new planed subjects in the ITU-T Study Groups are the following:

- **SG13 Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures:**
  - Y.Supp-AN-Use Cases "Use Cases for Autonomous Networks", requirements and potential use cases.
  - Y. IMT2020-CNC-req “Requirements of computing and network convergence in IMT2020 network and beyond”.

- Y. IMT2020-AINDO-req-frame "Requirements and framework for AI-based network design optimization in future networks including IMT-2020".
- Y. CNC-MO "Framework of management and orchestration for computing and network convergence in IMT-2020 networks and beyond".
- Y.REQCAP-NACC: "Requirements and capability of network awareness based on cloud computing".

- **SG17 Security**:
  - X.srdidm, "Security requirements for decentralized identity management systems using distributed ledger technology", describes security requirements for decentralized identity management systems using distributed ledger technology.
  - X.gecds, "Guideline on edge computing data security", analyses the edge computing data security and provides relative data security challenges and threats as well as data security guidelines for Edge Computing.
  - X.sa-ec, "Security architecture of edge cloud", to guide operator to implement a uniformed security management for multi-vendor environment.
  - X.sa-dsm, " Security architecture of data sharing management based on the distributed ledger technology", to specify the security architecture of data sharing management based on in distributed ledger technologies. Based on the architecture, it specifies the interfaces between the functional entities and the procedures of data sharing management based on DLT.
  - X.5Gsec-ecs, "Security framework for 5G edge computing services", analyses the potential deployment scheme and typical application scenarios of edge computing services, specifies the security threats and requirements specific to the edge computing services.

- **SG20 IoT, smart cities & communities:**
  - Y.IoT-MCSI : "Metadata for camera sensing information of autonomous mobile IoT devices", defines the metadata elements and format for autonomous mobile IoT devices and describes metadata characteristics of camera sensing-based information on IoT devices.
  - Y.IoT-Vreqs "Requirements and capability framework of the internet of things for vision", aims at developing a clear capability framework to accommodate newly developed vision-based internet of things applications.
  - YSTR.SemComm.IoT "Architectural Framework for Semantic Communication Services in IoT and Smart City & Community", to promote smooth, feasible and standardized solutions for the IoT and SC&C relevant services and applications to use and deploy semantic knowledge bases and semantic-aware communication in supporting highly efficient and scenario/domain-oriented networking services.

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

IEEE is the world's largest professional association dedicated to advancing technology. It is a widely accepted format for writing and submitting research papers commonly used in technical fields. 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 publishes more than 100 standards a year. Some of them are so accepted and sound that everyone uses them daily (e.g., IEEE 802.11b WiFi). Being active since 1963, IEEE SA covers almost all of the relevant IT-related (and specially, communications) areas.

According to their structure, an IEEE Standards Board (formed of Governors) must approve all the standard projects that are worthy to be promoted to actual standards. For this to take place, considering the vast amount of initiatives started yearly, a clockwork mechanism was designed and is currently used to guarantee successful preparation of the standards. As per today, the different steps and timings are very well defined, starting by an idea that is consecutively validated by different governance structures to become an approved project (in a maximum of 4 years) and then an actual standard (in a maximum of 10 years). This is illustrated in Figure 3.

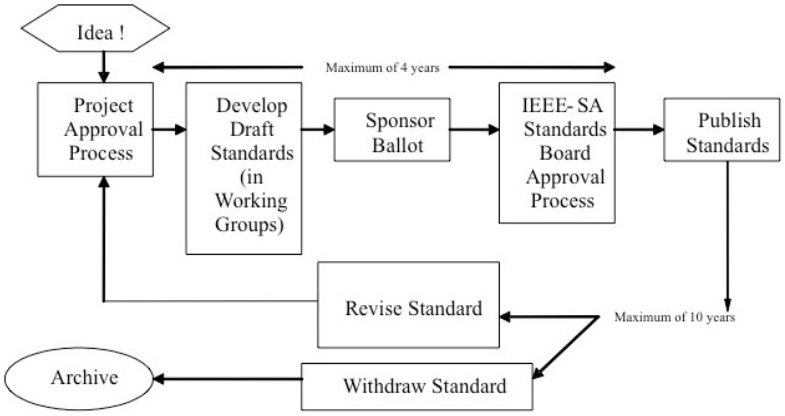

Figure 3. IEEE SA standardisation mechanism (reduced) – image from IEEE SA.

However, the underlying mechanisms are far more complex (see Figure 4). In order to contextualise how ASSIST-IoT can participate and contribute to IEEE SA standardisation (see Figure 5), find a summary below.

The procedure is initiated by the creation of a "Standards project". These projects are initiated by an IEEE Sponsor, that usually is one (or more) IEEE Society (there are 42). This sponsor initiates such action whenever a new interesting technological proposal could have the consideration of potential standard. For a project to advance as a standard candidate, it needs to be approved by the IEEE Standards Board. This first approval procedure materialises in a meeting that takes place once per month (NesCom), in which a committee (see below) validates (or not) a list of proposed candidate projects that are afterwards ratified by the IEEE Standards Board. At that point, the elaboration of a draft standard starts, supervised by the aforementioned Standards Committee. The elaboration process has also its inner rules: first, a Working Group must be established that is usually composed of the study group members and external individuals/corporations. For the external elements to join, the committee issues a call for members. Once the WG is formed, the WG chair organises the work by planning and hosting meetings that generate minutes over an agreed agenda. At the same time, the formal documents to convert a short PAR into a standard draft are also completed (following a set of established templates). Once the Standards Committee considers that the working version is stable, an Initial Ballot Draft is generated. By then, the Standards Committee should have composed a balloting group, that meet to vote whether the draft should advance or not. This process, that lasts 60 days (with potential extension to 120) goes in parallel to a Public Consultation in which anyone can express concerns and questions about the standard-to-be. The voting must be positive in a 75%. If this is achieved, the draft advances and gets confirmed by a RevCom committee meeting, that recommends the approval to the IEEE Standards Board for ratification. Afterwards, the IEEE Editors generate final standard that last 10 years.

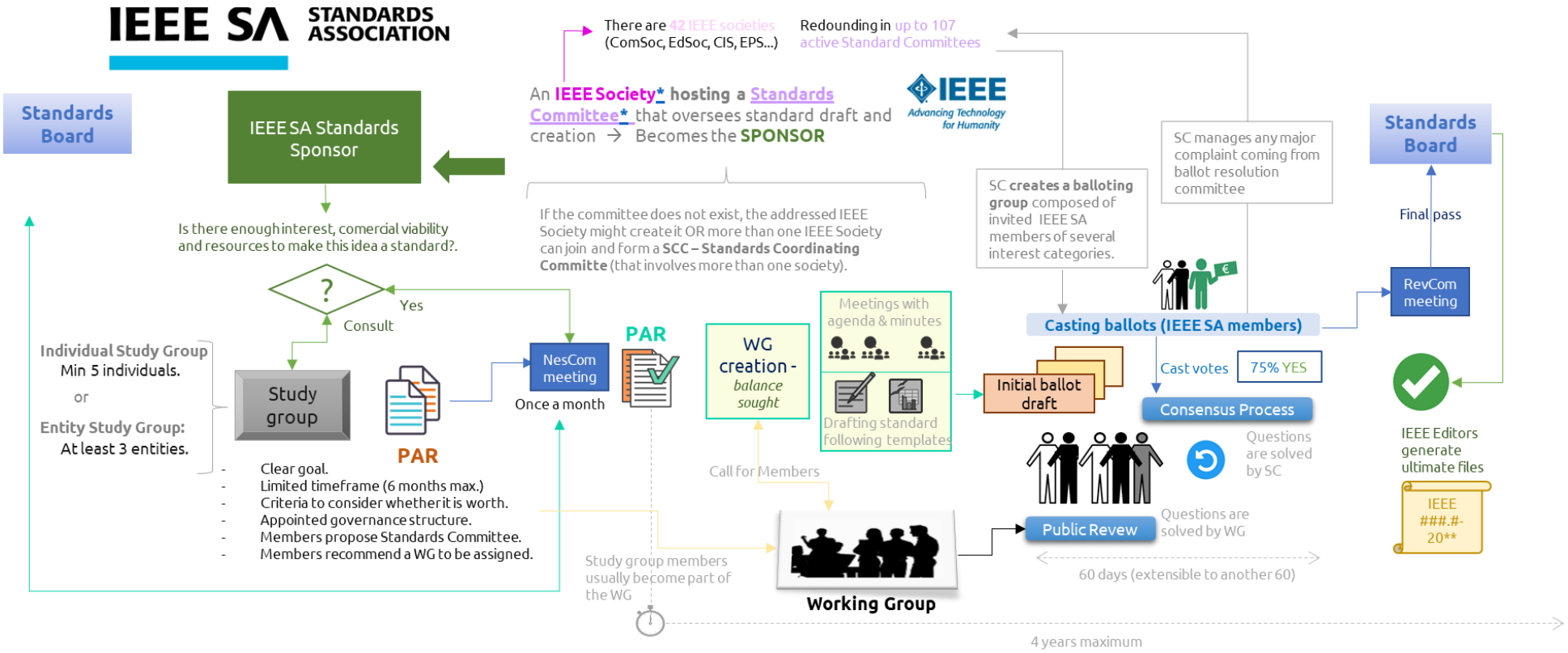

Figure 4. IEEE SA standardisation mechanism (complete).

Entry points for ASSIST-IoT:

Analysing the previous explanation and flow, the ASSIST-IoT team has realised that the contribution of the project could be materialised in 5 points of the procedure. Those have been called "entry points". It is the goal of the participants of task T9.4 (among others) to actively explore the possibilities opening in any of those entry points to guarantee enough presence of ASSIST-IoT in relevant/interesting IEEE SA standards. The entry points are as follows:

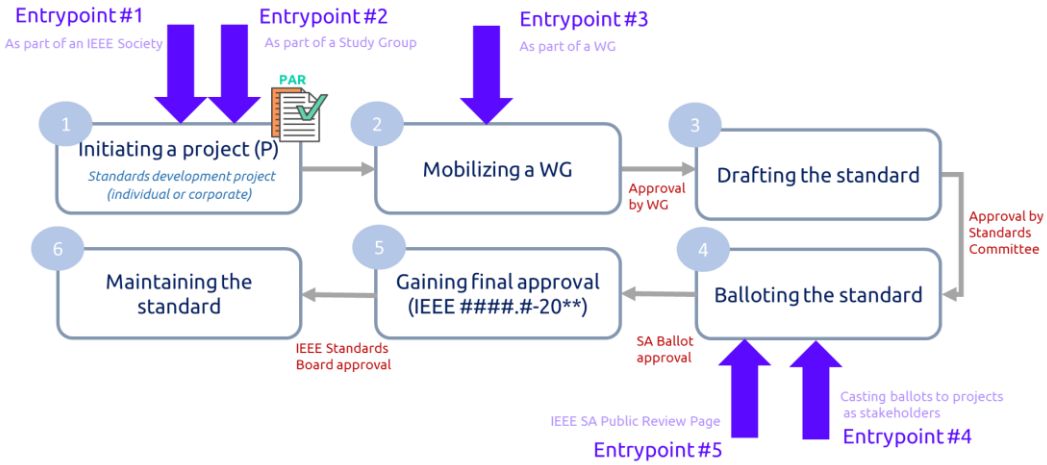

Figure 5. IEEE SA Standardisation procedure entry points for ASSIST-IoT to contribute.

- **Entry point #1**: *As part of an IEEE Society*: ASSIST-IoT partners belonging to any of the IEEE Societies will explore potential request to the Standardisation Head in the entity to start a project request procedure. In addition, ASSIST-IoT will also explore joining additional Societies to be better positioned for this task.
- **Entry point #2**: *As part of a Study Group*: In the moment of generating a draft PAR, the Standardisations Committees look for the creation of study groups to assess the viability of standardising a project idea. In that regards, ASSIST-IoT will join some lists of interest that could be cover in order to be eligible to be summoned as potential study group members.
- **Entry point #3**: *As member of a Working Group (preferred slot)*: In an individual standard project Working Group, anyone can freely participate. (IEEE SA membership not required to participate). For corporate standards projects, IEEE SA corporate membership is required. Agendas for Working Group meetings are distributed beforehand and the results of the group's deliberations are publicly available, usually through meeting minutes. Call for participation is managed through IEEE SA Media Contact.
- **Entry point #4**: *As a balloting stakeholder:* A balloting group consists of a balance of a variety of interests and works by invitation from Standards Committee members. This is normally done using lists where IEEE SA members include themselves as "experts", "interested", "consumers" or "producers. In ASSIST-IoT, partners being members to IEEE SA will enrol into some of those lists to be eligible.
- **Entry point #5**: *As a public reviewer*: ASSIST-IoT partners will be continuously monitoring relevant standardisation procedures in IEEE SA and will propose questions and comments to balloting drafts so that ASSIST-IoT technical perspective on those fields is taken into account.

Every participation is performed through a suite of online tools: https://standards.ieee.org/develop/etools/

There are currently 84 open projects that are open to participate (in phase of working group labour). Out of those 84, the following are the most interesting for ASSIST-IoT:

- *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.

- *P2976 – Standard for XAI – eXplainable Artificial Intelligence*: This is a statement (from the Grant Agreement) that ASSIST-IoT may explore potential synergies in the ML/AI methods to be developed (both within structural enablers and in additional functionalities).
- *P2986 – Recommended Practice for Privacy and Security for Federated Machine Learning:* Both T5.2 (Federated Learning) and T5.4 (privacy-DLT) of ASSIST-IoT will be interested in following the evolution of this standard, most likely participating as external public reviewers.
- *P2994 - Standard for Security Assessment Framework for Internet of Things (IoT*) Application Deployments: This project is interesting for ASSIST-IoT. Although there is a specific task within the project to tackle security (T5.3), the directives in this standard might guide some interoperability decisions and compatibilities during ASSIST-IoT deployment in pilots.
- *P2418.10 – Standard for Blockchain-based Digital Asset Management*: In ASSIST-IoT, a blockchain tool (Hyperledger Fabric) is being used to build enablers related to monitoring, security and auditing. Even though the concept of "assets" has not been introduced in the project yet, this might be extremely useful if deciding to move forward with DLT and apply it in broader aspects of the architecture.
- *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). Some outcomes of this standard might be relevant. Working Group participation in consideration.
- 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*. There is a current request for Working Group, that could be of interest to some partners of ASSIST-IoT involved in T5.2 enablers and also in various pilots of the project.
- *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.
- *P3652.1 - IEEE Guide for Architectural Framework and Application of Federated Machine Learning*, in ASSIST-IoT federated Learning solution is design and under developing.
- *P7030 - Recommended practice for Ethical Assessment of Extended Reality (XR) technologies*. Of applicability for extended reality applications in pilots 1 and 2.

In addition, the project will closely follow 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.

Finally, ASSIST-IoT will tackle the membership/close contact with the following relevant IEEE Societies (there are currently 42 of those):

- IEEE Communications Society (ComSoC),
- IEEE Computational Intelligence Society (CIS),
- IEEE Computer Society (CS),
- IEEE Intelligent Transportation Systems Society (ITSS),
- IEEE Vehicular Technology Society (VTS).

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. In addition, since 2021, AIOTI is part a Digital Innovation Hub (SCoDIHNet) that embarks 82 entities from 23 European countries in the quest for innovation in 5G/6G with IoT including AI and cybersecurity.

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 convergence of standards and interoperability and defining policies.

According to their principles, the added value provided by AIOTI to the IoT continental arena roots in:

1. Leadership and connection to policy-makers, which is clearly visible considering the high-level participation of EC units heads (DGGROW, DGGONNECT, among others) in AIOTI conferences and organised events. This influence also materialises in issuing whitepapers and pre-normative documents that hugely feed EU policies, strategies and research frameworks.
2. Collaboration, via the participation in PPP (public-private partnerships), fostering joint actions between different actors and also promoting innovation hubs like ScoDIHNet. The pivotal point here is the research and innovation agenda followed by the Alliance which is continuously revised and improved.
3. Matchmaking, as AIOTI members are always active in organising webinars, workshops, special sessions and other type of events to exchange knowledge and opportunities related to IoT innovation. This is also emphasised as AIOTI tends to collaborate closely with the CSAs (Coordination and Support Actions) funded by the EC that aim at clustering various research initiatives.

AIOTI has designed a contribution path aiming to create a dynamic European IoT ecosystem, where activities focus on well-defined areas of development. In particular the organisation has been recently 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 AIOIT in IoTWeek,
  - **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.

The following list compiles the most relevant and recent documents issued by AIOTI that have influence/are influencing ASSIST-IoT in one way or another. It has been also the starting point to reflect what ASSIST-IoT contributions to the SDO might look like:

- **High Level Architecture - HLA** (release v5.0): This is, by far, the most relevant document for ASSIST-IoT coming from AIOTI. It observes the different NGIoT architectures being proposed by projects and companies and devises a global, well-detailed, technical-closed architecture specification.
- **High Priority IoT Standardisation Gaps and Relevant SDOs** (deliverable of WG Standardisation WP3): This document listed the different gaps and relevant standardisation organisations that have a role in the IoT field in Europe. It has served as a beautiful reference document for elaborating D9.2 and D9.3 and has helped ASSIST-IoT orient efforts during the last few months.

- **IoT and Edge Computing impact on Green Deal**: Although not being a specific goal of ASSIST-IoT, the fact of reducing the environmental impact of IoT and edge solutions should be a priority for all innovative actions. This document sets the ground for some ways how IoT and edge could contribute to improve businesses reducing footprint and energy consumption.
- **AIOTI input to Europe Digital Decade**: This document created before ASSIST-IoT draws a roadmap about how key technical gaps should be covered in line with the Europe Digital Decade – the common European digital plan towards 2030.
- **AIOTI Contribution to Recovery and Renovation Wave in Europe**: This document, delivered by the VWG Buildings, outlined how IoT and next generation technologies must play a role towards the Smart Building, emphasizing in the connection with BIM systems.

2.5. BDVA: Big Data Value Association

The Big Data Value Association (BDVA) – known since 2020 as DAIRO: Data, AI and Robotics - is an industry-driven international non–for-profit organisation with more than 200 members all over Europe, to develop the Innovation Ecosystem for the data and AI-driven digital transformation in Europe delivering maximum economic and societal benefit. The most relevant aspect of BDVA's offering is to be aware of the advances in the field of Industrial Data Spaces (mentions in the GA to ensure exploration and alignment).

According to their own definition: "*The mission of the BDVA is to develop the Innovation Ecosystem that will enable the data and AI-driven digital transformation in Europe delivering maximum economic and societal benefit, and, achieving and sustaining Europe's leadership on Big Data Value creation and Artificial Intelligence.*"

BDVA produces a good quantity of position papers during a year, so ASSIST-IoT is following actively their recommendations to align internal work of the project with those whitepapers and reviews.

The BDVA/DAIRO is structured in task forces (TFs), each of them tackling a set of objectives of the association under the authority of the Board of Directors. Every TF focuses on specific sector or cross-sectorial concerns:

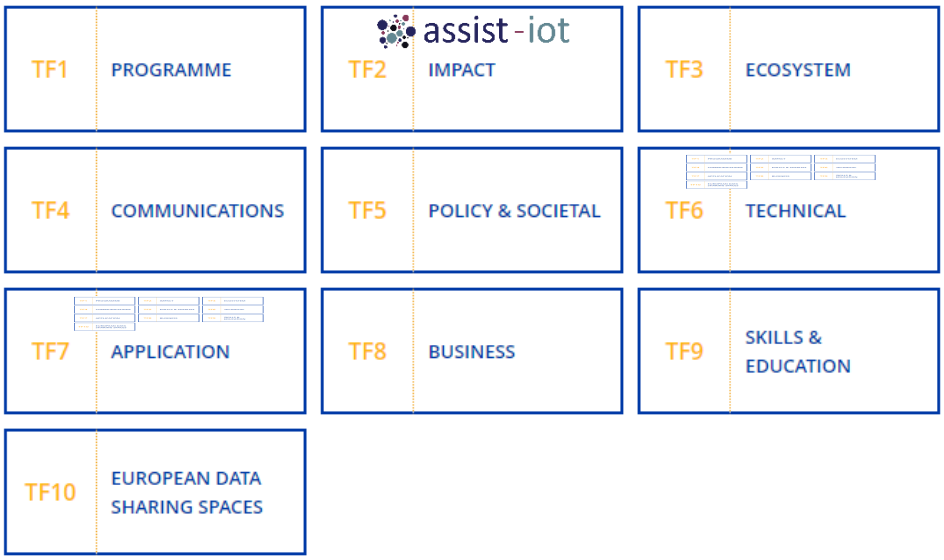

Figure 6. BDVA task forces

Figure 6 illustrates all task forces of BDVA, including those that are being relevant for ASSIST-IoT.

TF2 (Impact) is a task force aiming at updating the main guiding document of the association (the SRIDA – Strategic Research, Innovation and Deployment Agenda), reviewing the KPIs and reporting advances and modifications, aligning those with the European Commission vision as well. It also organises the work of all members vis-à-vis the SRISA. This is only observed by ASSIST-IoT.

However, those that are being followed with more attention are TF6 and TF7.

TF6 focuses on monitoring and collecting information about ongoing and emerging technical trends in technical priority areas (according to the SRIDA), create a wiki documentation with the findings and contribute to update the SRIDA. The work in this TF is organised in sub-groups, according to technical division:

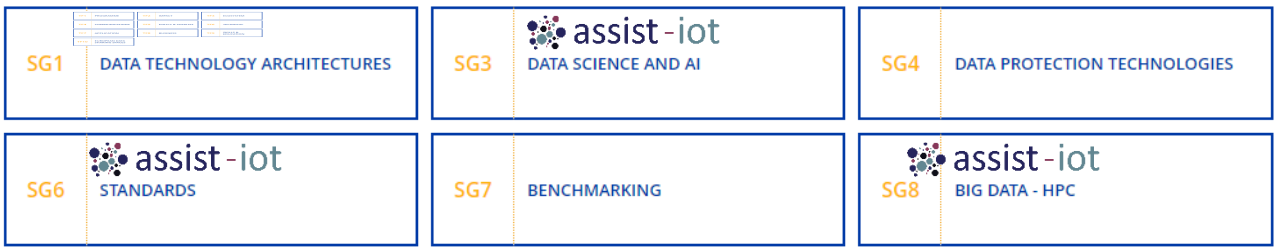

Figure 7. TF6 subgroups (BDVA)

Within those, Figure 7 illustrates those that entail more interest for ASSIST-IoT, corresponding to technical goals of the project. The most relevant out of those are described below (ordered by importance):

- *TF6-SG6: Standards*: This group intends to serve as one-stop-shop for acknowledging the current status of AI and Big Data standardisation in Europe, mapping advances to the European Commission's Digital Strategy. It analyses results of various PPPs, ISO/IEC, CEN-CENELEC, etc. ASSIST-IoT follows the documents issued by this SG and will aim to be member in the future.
- *TF6-SG1: Data technology architectures*: Compiles advances in all related data management aspects from an EU perspective, generating a relevant state of the art and providing input to European policies while enhancing the SRIDA. It is the SG in charge of delivering the White Paper in AI and the EU Strategy for Data. ASSIST-IoT will aim at actively contributing to this work.
- *TF6-SG3: Data Science and AI:* Gathers status of data and monitoring technologies to deliver recommendations to BDVA members and to enhance the SRIDA.

On the other hand, TF7 aims at supporting selected industrial sectors and other areas of interest with Big Data technologies, identifying needs, promoting skills and reviewing trending languages, technologies, etc. It also contributes to SRIDA and generate sectorial reports. Same as for TF6, TF7 is divided in sub-groups targeting specific Big Data-intensive sectors. Those most relevant for ASSIST-IoT are TF7-SG7: Mobility and logistics and TF7-SG11: Automotive.

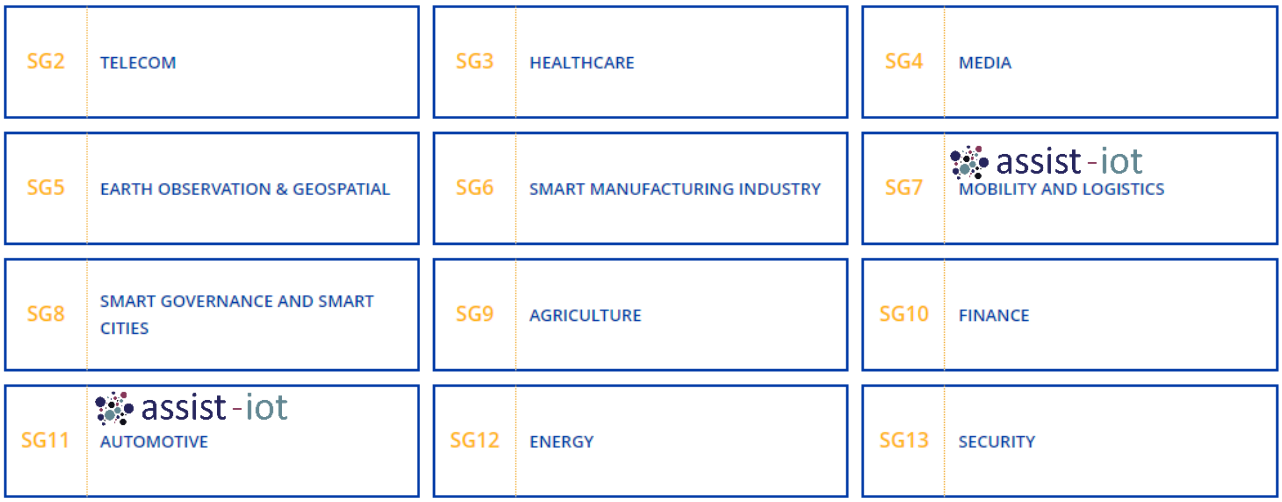

Figure 8. TF7 subgroups (BDVA)

The following list compiles the most relevant and recent documents issued by BDVA:

- **Strategic Research Innovation and Deployment Agenda**,
- Speeding up Industrial AI and Trustworthiness - Position Paper,
- Towards a European AI regulation: a perspective from our community.

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.

For ASSIST-IoT and in the scope of this report is relevant the work done under WP1: Overview of existing Cybersecurity standards and certification schemes v2.

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 proposes a consolidated web format with all baselines and security measures also available as an excel sheet also referenced to technical measures and Relevant References.

- ENISA Good practices for IoT and Smart Infrastructures tool [1],
- ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures [5].

2.8. TIC4.0: The Terminal Industry Committee 4.0

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. Terminal Link (partner of ASSIST-IoT) is the president of the Committee. One of the objectives is promote the deployment and adoption of selected existing standards and those developed by TIC 4.0 by the sector. The list of publications is the following:

- TIC4.0 White Paper: "An Introduction to the Terminal Industry Committee 4.0 (TIC4.0)" released in March 2021.
- TIC4.0 Release 2021.001 "Container Handling Equipment Activity and Power Source Concepts and Definitions" released in May 2021.
- TIC4.0 Release 2021.002 "Move and Cycle: Definitions, Dataset Roadmap and Data Model" released in October 2021.
- 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)" released in January 2022.

Standards related to the cargo:

EDI (Electronic Data Interchange) is the electronic exchange of business documents such as orders, delivery notes and invoices. These documents are exchanged between business partners in the form of structured data and without manual intervention.

Source: https://www.seeburger.com/info/what-is-edi/

UN EDIFACT Messages stands for Electronic Data Interchange For Administration, Commerce and Transport. This is a global set of rules defined by the UN for the inter-company electronic data exchange between two or more business partners via EDI.

reference: https://unece.org/fileadmin/DAM/trade/edifact/untdid/d424_s1.htm

Standards related to the equipment :

It is about all the standards around the vehicles, cranes, equipment in general. In our case we are only interested in the control system of the machine.

For this we only have some standard interfaces : CAN-BUS; PROFIBUS, PROFINET, OPC-UA. But except CAN-BUS, the rest doesn't the find the "information model". They are just the communication protocol

Data sharing:

Recently has appear several indicatives to share data in the port industry, the most famous are DCSA https://dcsa.org/ and TIC 4.0 https://tic40.org/ for sure are other initiatives for the logistic chain. These standards are not about the protocol but only about the content. Usually are designed to describe a process not just an equipment status or a cargo metadata.

2.9. Other standardisation organisations, forums and initiatives

For the ASSIT-IOT project also interesting are different organisations, forums and initiatives related to technological aspects of the designed solution. The aim is to analyse their existing reports and to follow their current activities without major involvement of contributing to their technical reports. Below is 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 includes 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.

- **3GPP**: The 3rd Generation Partnership Project (3GPP) unites telecommunications standard development organization of current and future generations of mobile communications technologies. The standards development work in 3GPP is organized in Technical Specification Groups (TSGs), namely: Radio Access Networks (RAN), **Service & Systems Aspects** (SA) and Core Network & Terminals (CT). For ASSIST-IoT most relevant is the TSG SA group.

- **5G PPP:** The 5G Public-Private Partnership brings together cross-project work groups focused on common issues as the basis for convergence on technical and strategic aspects of 5G at the EU programme level. The Work Groups stem from the 5G-Infrastructure Association activities and the 5G PPP projects themselves. The relevant WG is working on the **5G security** and pre-standardisation, and R&D topics to be standardized.

- **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 ASSIT-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.
- **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 Contributions Domains

In the project we are working on different technical subjects to develop overall common solution for different IoT use cases. Therefore, we can distinguish the main interesting areas of standardisation to be used in our solution or to contribute to ongoing standardisation work as well as to see the gaps in standardisation scope of work and propose new standardisation subjects. Here below there are explained some hints (extracted from the experience of technical partners in collaboration with standardisation task members) about which parts of ASSIST-IoT would be more suitable to be considered as a potential standard project. It is not the intention of this section to list all technical components that are affected or interested by/in current standardisation procedures. It is understood that all elements of the architecture and the project, to varying extents, rely on standards or standards-to-be, therefore this is not covered in the text below.

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. Internet of Things domain

The following subjects are considered:

1. IoT platform architecture:
    - ASSIST-IoT is specifically focusing on the application challenges and analysis of reference architecture diversities of IOT-A RA, RAMI 4.0, ETSI MEC, and IIRA.
    - The architecture is the main and foremost candidate for standardisation. ASSIST-IoT propose a 2-D layered architecture based on the interconnection of enablers with well-defined roles. This architecture will be brought to AIOTI HLA release 6.0 and later would be suitable for a standardisation project submission.
2. 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 is 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. This line will be explored by ASSIST-IoT standardisation team as soon as the software will deliver results and will be tested in demonstrative scenarios.
    - Data spaces analysis, AIOTI Data space position paper, the contribution is under preparation.
    - Interoperability for data spaces, BDVA position paper, the contribution is under preparation.

3.2. Artificial Intelligence domain

Most of the SDO's 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 is 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. The potential subjects 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.
- The architecture and schema (including steps, etc.) of the Federated Learning enablers will be considered for standardisation. As it is mentioned in previous sections, Federated Learning is one of the hot topics today and it is present (as projects) in diverse SDOs. The mechanisms and recommended technology will be studied to be delivered as a standard.

3.3. Cybersecurity domain

ASSIST-IoT is following both IoT, edge and cloud (multi-layer) cybersecurity standards, particularly for the secure exchange and processing of data (e.g. ISO/IEC 27001 and 27002, IETF and ETSI TR 103 305-3, Critical Security Controls, including a chapter for IoT Security). In the project we look for opportunities to close the gaps in the existing standards as well as in the area of application security for ecosystem interoperability. In the field of cybersecurity, it is also worth mentioning other initiatives and best practices published by ENISA on IoT security and other market-oriented initiatives like IoT security testing framework by ICSA labs and standards and schemas developed by IoT device vendors, such as: BITAG Internet of Things (IoT) Security and Privacy Recommendations, Cloud Security Alliance IoT Working Group, GSMA IoT Security Guidelines, and CIS Controls IoT Security Companion [4][5][6].

ASSIST IoT will contribute on enhancing cybersecurity and paving the path to accomplish different cybersecurity standards and best practices on the following activities:

- Dynamic and context-based access control policies using OASIS XACML;
- Combination of tools and for gaining awareness on cybersecurity incident detection;
- Design and implementation of suitable tools and solutions for cybersecurity incident response.

3.4. 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. Among many of new and ongoing networking standardisation items the most relevant is related to Smart Orchestrator enabler:

- Methodology for encapsulating enablers (charts, labelling, etc.) altogether with the use of CNF to distribute service workloads might be considered as a candidate for standardisation,
- Network slicing architecture and specification (planned contribution to ITU-T SG13),
- IoT Relation and Impact Beyond 5G (analysis in AIOTI WG Standardisation TF),

3.5. Use cases domain

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 ASSIT-IOT: workers safety, logistics or autonomous vehicles aspects. The following contributions are prepared and planned:

- 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;
- Use cases and testbeds. SDOs are working on federated testbed standardisation (IEEE, ITU-T, ETSI);
- The current 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: **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 Legal and Regulatory Constraints Analysis and Specification in sub-section 3.3.4. Taking into account ASSIST-IoT pursuits, the following thematic categories of the identified standards for occupational safety and health can be distinguished: (a) occupational risk management, (b) hazards and exposures specific for the construction site, (c) ergonomics, and (d) personal protective equipment. Most of those documents have a status of the European standard (EN) that has been approved by CEN. Unfortunately, besides the widespread interest in the application of information and communication technologies (ICT) for Industry 4.0 vision in the work environment, the standardised testing methods and evaluation criteria of the safety-related ICT systems to be used in the work environment are still limited. This issue also concerns 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.

4. Standardisation gaps analysis

As mentioned in D9.2 and throughout this document, several EU and international bodies such as ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS or OGC are proposing standards to cover many of the most relevant IoT aspects. However, due to its relatively new emergence, the Industrial adoption and global-wide inclusion of those is not a reality yet. In contrast, the sector still seems to be driven by de-facto standards (specially, technology-wise) notwithstanding the SDO behind. Thus, interoperability and compatibility across IoT deployments is still far from being achieved.

In January 2020, the WG3 of AIOTI published a document [12] in which, drawing from the work by ETSI STF and others, identified 49 standardisation gaps related to IoT domains and knowledge areas. In that study (fed by a selected survey), out of the 49, here below there is a short selection of those which (according to ASSIST-IoT team) should be considered (still) relevant standardisation gaps:

- **Connectivity**: There is a large number of heterogeneous and competing communication and networking technologies at various levels (from a OSI layered reference model perspective): MQTT, OPC UA, CoaP, LoraWAN, Sigfox, Zigbee, WiFi, in many cases, not compatible between each other.
- **Data interoperability**: This is one of the main holes in standardisation. There is a lack of translation mechanisms between different data models, being currently very dependent on the use-case, application domain and even on the predominant device/service provider. Although there are several initiatives that have tried to tackle this issue, such as the Smart Applications Reference Ontology (SAREF) by ETSI, the ETSI ISC GIM working group's NGSI-LD API (and, for instance, the SmartDataModels initiative within) or the Semantic Sensor Network (SSN) ontology from W3C, none of them is the **one reference neutral data model**. Therefore, seamless inter-working between data systems is not yet achieved. Related with the previous, there is also a lack of standards on how to interpret the sensor data in an identical manner across heterogeneous platforms.
- **Safety**: The Industrial world introduced, via IEC 61508, a Safety Integrity Levels for hardware and system integrity, but this is not close to the actual reality of IoT sector, where the potential damages and negative impacts of malfunctioning devices/elements in the environment is not much explored.
- **Interoperability between IoT HLAs**, platforms and discovery mechanisms. A lot of platforms co-exist in the IoT landscape, but architectures and schemas (even to the least minimum expression) are different, therefore interoperability is very difficult to be envisioned. Many initiatives have tackled this topic (projects like SerIoT, INTER-IoT, LSPs) and also the Web of Things (WoT), which describes a thing, security and payload data schemes and protocol binding for achieving so. However, the sector has not yet reached an agreement upon this.
- **Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms**. The Open Mobile Alliance through its Broadband Forum (BBF) proposed TR-069 and TR-369 for Device and Service management (but focused on mobile applications) and also delivered a management/communication protocol in LWM2M. On another note IETF proposed COMI and SUIP to serve as deployment managers while OSGi exposed DMT Admin API. However, this is another of the main points where heterogeneity outstands.
- **Secure permissions, access control and the need to regulate trust relationships** among the main entities (ISO TC 204 and CEN 278). Some protocols and technologies have become de-facto standards (such as TLS-based REST APIs and OAuth2 for identification and authentication), but there is here, again, another aspect that is not standardised and that keeps preventing IoT from being a fully trusted, centralised, powerful Industrial reference.
- **IoT devices identifiers**. This was considered a major gap by AIOTI's report, which signalled URNs proposed in ISO/IEC 29161 as a potential solution, but with little expectations of convergence. To ASSIST-IoT authors, this gap is considered as not-so-relevant as most use-cases will be focused on connecting devices via other networking features (e.g., IP LANs, SD-WAN, etc.), avoiding the need of world-wide unique identification.

In addition, the team of ASSIST-IoT in T9.4 has been able to identify other gaps in the current IoT standardisation landscape:

- Gaps in NG-IoT, including edge computing:
  - IoT and edge computing systems are unbreakable elements where the cooperation in different technological fields are required, therefore main challenge in standardisation work is from the point of **interoperability** for interfaces, data models and ontologies.
  - Standardised methods to distribute software components to devices across a network. Although cloud-native approach is gaining traction in the IoT field as it contemplates deployment of functions (network and non-network) over edge equipment, there is not yet a clear reference on how to tackle this paradigm. Distributed cloud-oriented ETSI MANO architecture is usually assumed as feasible (coming from the radio access networks world), but, again, the software components distribution to computing equipment in a network is still a matter of case-per-case decision. **ASSIST-IoT may play a substantial role here** as it proposes a way for deploying such functions (CNFs – through containers) for NGIoT scenarios leveraging an ETSI MANO orchestrator (OSM).
  - A single market for IoT/IIoT **edge computing** is required. Currently, there are many initiatives (open source and private) targeting the edge computing market (including devices, computing equipment, platforms, software solution, workload distribution, inference, training, federation…). It is the believe of ASSIST-IoT partners that there should be an open standard instructing how to achieve edge computing, performing seamless plug and play for the edge-to-cloud continuum.
  - There is the need to standardise a strategy for data management. Up to know, further than GDPR obligations, every NGIoT deployment devises and applies their own data management policies and technologies. There have been some efforts in different SDOs (ISO, ETSI, IEEE SA, DSBA) but none of them has covered all of the aspects that should be standardised (according to ASSIST-IoT team):
    - Data anonymization/aggregation technologies,
    - Deliver a solid data privacy management methodology (ETSI STF547 in TR 103 591 explored it), devising a sound way to keep data privacy and preservation,
    - Blockchain technology and methodology for IoT, including smart contracts negotiation. IEEE P2418 initiative and the Blockchain Community Group of W3 have worked on this aspect, not reaching adopted standards yet. The goal here for European initiatives should be to develop, deploy and operate an European blockchain-based infrastructure that is green and compliant with EU values and framework,
    - Alignment with Common European Data Spaces, DSBA and other open initiatives aiming at secure, trustable, robust data sharing in Europe.
  - Lack of a reference for business cases and value chain model to guide choices for deployment. This is a point that ASSIST-IoT will aim at contributing to, as one of its goals is to deliver sustainable business models to let sectors leverage technological IoT innovations.
  - In IoT and edge computing platforms it is required to work on federation of platforms, their interoperability which allow for resources optimisation, improvement of service quality and reducing costs.
  - New IoT Distributed and Federated Reference Architectures integrated with the 5G architecture and AI are under investigation for addressing the convergence of Tactile Internet, Digital Twin edge processing, AI and distributed security based on ledger. It is the field of new standardisation needs where ASSIT-IOT is dealing with most of the above issues.
- Gaps in AI and Big Data:
  - Embedded and frugal AI (see [15]),
  - Explainable AI,
  - Metrics for defining data quality, accuracy, and other relevant information [16]. Some of these definitions are too wide and misleading, preventing different use-cases to leverage each other (even when eager to) due to those misconceptions. According to BDVA/DAIRO, this is paramount.

    - DevOps and, in particular, MLOps for data training, sharing, inference, etc.
- A non-technical gap has also been identified in some sources that has been considered relevant for ASSIST-IoT. Measuring risks is a common task throughout IoT and AI deployments. However, there is not a current standard guiding the definition, classification, assessment, etc. In contrast to the project management field (where this aspect is well covered), technical risks do not have regulation or guidelines and would definitely be of use.
- Cybersecurity standardization - in general, there is a gap on building a European Cybersecurity Community, also within the IoT domain. There are different initiatives on cybersecurity like MeliCERT Cyber Security Platform [6] which are oriented to coordinate actions form Service Operation Centres SOCs and Computer Security Incident Response Teams CSIRTs and Computing Emergency Response Teams CERTs. Nevertheless, cooperation and sharing of information among different industry sectors and even countries are still in a very early stage, and there is also a strong need on building related trust circles for sharing and collaborating on cybersecurity incidents. The foreseen gaps in cybersecurity area are in:
    - Identifying the intended use and environment of a given IoT device,
    - Implementation of regular monitoring to verify the devices behaviour, to detect cyberthreats and to discover integrity errors,
    - Cybersecurity monitoring on IoT standardization landscape, establishing procedures for analysing and handling security incidents,
    - participating in information-sharing platform to report vulnerabilities and receive timely and critical information about cyber threats and vulnerabilities.
- Gaps in networking and beyond 5G solutions:
    - There is a lot of ongoing standardisation works as well as existing recommendations for networking subjects and 5G technology, anyway we can find still open and newly appeared fields for standardisation also relevant for ASSIST-IoT project related to **network resources management** (network orchestration), **AI/ML empowered network** solutions for resources management, security or energy consumption.
    - One of the key gaps related to networking is **connectivity interoperability** in IoT systems. We have a lot of different wireless and wireline technologies used in IoT ecosystem without perspective for convergence to single technology, so it implies difficulties in standardisation single connectivity mechanism. The new challenges and gaps in wired and wireless infrastructure is related e.g. to gateway – be able to manage different technologies, QoS differentiation for IoT services, security risks with different stakeholders.

5. Standardisation strategy

ASSIST-IoT team has defined the plan of the standardisation activities, based on the work planned in individual Work Packages. In the presented roadmap (Figure 9) 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. Beside the analysis the first contributions were submitted to SDOs as well as already published. It is also expected that contributions to SDO's will increase over time in direct relation with the technical development of the project in the second half of the project. According to the Work Plan, now in this deliverable the analysis of standardisation landscape work of different SDO's, technical domains and standardisation gaps are outlined. It will be updated by the end of the project via D9.4 report.

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

1. **Internationally recognized standards supported in ASSIST-IoT** – usage of standardized elements in project solutions, target KPI: 15,

2. **Communications to modify / improve existing standards used in ASSIST-IoT -** identification of gaps and needs for improving of existing standards – target KPI: 2,
3. **Recommendations in relevant SDO's and initiatives -** contribution to recommendations in SDO's – target KPI: 4,
4. **SDOs and pre-normative initiatives engaged -** engagement in SDO'S work and pre-normative initiatives – target KPI: 6,
5. **Identified standards related to ASSIST-IoT activities -** followed and analysed standards, target KPI: 50.

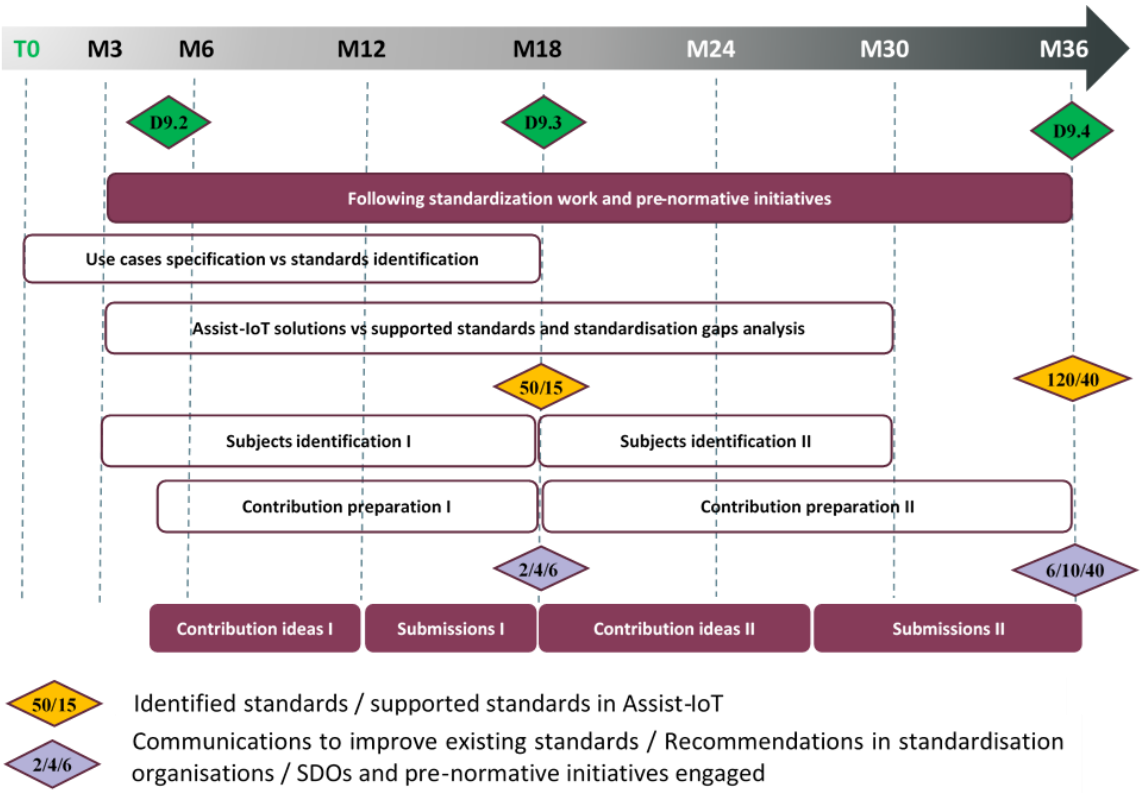

Figure 9. Project standardisation activities roadmap with target KPI's.

Strategy for the second half of the ASSIST-IoT project is focused on the main technical areas mentioned above in the context of the developed solution and analysis of the standards with identified standardisation gaps:

1. Main technical domains in the project:
    a. **IoT domain** in case of reference architecture, DLT and semantic interoperability, use cases specification.
    b. **AI solutions** with federated machine learning, governance and practice of artificial intelligence as related to computational approaches to machine learning, algorithms and related data usage.
    c. **Cybersecurity domain** with focus on enhance technical guides on IoT related security controls Influence, define or propose new security blocks on the reference architecture.
    d. **Networking and edge cloud systems** with focus on smart networking, 5G, SDN/NFV and testbeds based on open-source solutions, Fog/Edge Computing solutions.
2. Main SDO's and standardisation initiatives identified as most relevant for the project:
    a. ITU-T - active partners involvement, full membership,
    b. ETSI - partner delegates with active participation in WG's,
    c. IEEE SA - three partners active involvement, corporate member (Orange),
    d. AIOTI – two active members, especially in WG3,

e. BDVA – one active partner,
f. ESCO/ENISA – active members in cybersecurity area.

3. Secondary interest SDOs: beside main standardisation SDO's it is foreseen to potentially contribute to TIC4.0, IETF and others.

The standardisation work inside the ASSIST-IoT project and our strategy is aligned to EU Strategy on Standardisation presented in [7] by European Commission. EC emphasises the important role of standardisation and its development. For the 2022 the main polices relevant to the project among others are:

- the twin green and digital transitions;
- the digital single market;
- the single market for services;
- energy efficiency and climate.

From current annual EU work programme most important priorities relevant to the project are:

- Review existing standards to identify needs for revisions or development of new standards to meet the objectives of the European Green Deal and Europe's Digital Decade and support the resilience of the EU single market.
- Smart contracts for data spaces.

Moreover, what is important for our work and we will follow up the different activities planned by the Commission:

- Set up a mechanism to monitor, share information, coordinate and strengthen the European approach to international standardisation (ISO, IEC, ITU and other relevant international fora), supported by the EU Excellence Hub on Standards.;
- Foster the development and deployment of international standards for a free, open, accessible and secure global internet and establish an EU internet standard monitoring website.
- Promote international cooperation on standardisation and EU standards with the Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI-GE) and Horizon Europe, also with a view to support stakeholder participation in international standardisation (SMEs, civil society, academics) – ASSSIT-IoT is cooperating with different SDO's and pre-normative initiatives;
- Launch the 'Standardisation Booster' to support researchers under Horizon 2020 and Horizon Europe to test the relevance of their results for standardisation;
- Develop a Code of Practice for researchers on standardisation to strengthen the link between standardisation and research/innovation through the European Research Area (ERA), by mid 2022;
- Organise Standardisation University Days to promote standardisation awareness among academics and students;
- Deploy initiatives for young researchers and networks from Horizon Europe and the Euratom Research and Training programme, including the COST Association, for the valorisation of research and innovation through standardisation and pre-normative research.

6. Contributions performed by ASSIST-IoT

In table below the submitted, started and planned for second half of the project standardisation activities according to main technical domains and SDO's are presented. In each domain, ASSIST-IoT has identified and actively participates (green box) in working groups specified in the table.

In each domain ASSIST-IoT has identified possible contributions and activities: started active participation in working groups (green box), plan to contribute (yellow box) and already submitted contributions (blue box).

Table 1. Submitted and planned activities in summary.

Domain/SDO	IoT	AI	Networking/Cloud	Cybersecurity
ETSI	**smartM2M, PDL**	**AI, ENI**	**NFV, MEC**	**SAI**
ITU-T	**SG-20**	**SG-13, SG-16**	**SG-13**	**SG-17**
IEEE SA	**CEC, CCSC**	**AISC**		**CPSC**
AIOTI	**WG SD, DLT**	**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 table below the current list of submitted (released) and planned contributions in standardisation work is presented.

Table 2. List of submitted and planned contributions.

SDO, Forums, Initiatives	Partner	Report/recommendation contribution	Type	Release/ Planned Date
ECSO	S21SEC	Technical Paper on Internet of Things (IoT). April 2021 v0.8	White Paper	Q2 2021
AIOT	OPL, UPV	IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges Release 1.0	Technical Report	Q3 2021
AIOT	OPL, partners	Edge Computing Standard Framework Concepts Release 1.0	Technical Report	Q3 2021
ETSI	OPL, WP3 partners	STF601 Cross-domain usability of IoT devices for humans and machines, TC (Technical Committee) SmartM2M, Technical Report „Use cases for cross-domain data usability of IoT devices" https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf	Technical Report	Q3 2021
AIOT	OPL partners	Contribution to AIOTI Computing Continuum Requirements on IoT/Edge Computing & Optical Communication – use cases and requirements	Technical Report	Q2 2022
AIOT	OPL partners	Contribution to AIOTI Edge Computing Gap analysis – architecture and functionalities, under preparation	Technical Report	Q3 2022
BDVA	OPL, UPV, SRIPAS	Position paper about data spaces and interoperability, under preparation	Position Paper	Q3 2022
AIOTI	OPL, UPV, SRIPAS	Position paper about data space, under preparation	Position Paper	Q3 2022

AIOTI	OPL, UPV	Co-editor of new AIOTI report „EU funded projects landscape focusing on IoT and Edge computing"	White Paper	Q4 2022
AIOTI	OPL, partners	High Level Architecture (HLA) next release 6.0	Technical report	Q4 2022
ITU-T	OPL partners	ITU-T SG-20 contribution to IoT architecture and network orchestration	Recommenda-tion	Q4 2022
ESCO	S21SEC	Contribution to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem	White Paper	Q4 2022

7. Relevant results for the project

The summary of different activities in the area of standardisation area in ASSIST-IoT project is presented for each of SDO's and initiatives. The main focus is on 3 SDO's and 3 initiatives.

*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 contributions to Technical Reports (use cases for human interfaces in IoT services).
- Potential contribution for SmartM2M STF 602 SAREF: Industry adoption facilitation and oneM2M ontology alignment.

*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 the standardisation work and planned contributions to SG13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures.
- Following up the SG20: IoT, smart cities & communities.
- Participation in ITU-T meetings: SG13 and SG20.

*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, Federated Machine Learning, C/AISC/FML.
- Following up the selected Working Groups: Tactile Internet, COM/MobiNet-SC/TI, Security Assessment Framework for the IoT Application Deployments, COM/MobiNet-SC/IOTAF.
- Thorough analysis of contribution possibilities, deepening the work carried out before D9.2.
- Identification of current relevant projects.
- IEEE SA Training + Development programs – the course has been passed.
- Publishing in IEEEXplore Digital Library

*Short summary of the work done with **AIOTI** (by ASSIST-IoT):*

- Active participation in the AIOTI Standardisation WG.
- Thorough analysis of contribution possibilities, deepening the work carried out before D9.2.

- Contributions to white papers, position papers and technical reports in different technical subjects: HLA, data spaces, edge computing and gaps analysis.
- Align technical architecture of ASSIST-IoT with the specifications of HLA release 5.0 (see deliverable D3.6).
- Confirm membership (UPV).

*Short summary of the work done with the **BDVA** (by ASSIST-IoT):*

- Active participation in the working groups.
- Identification of gaps.
- Started contribution to the white and position papers (eg. data spaces).
- Presentation of ASSIST-IoT advances in EBDVF 2021.

*Short summary of the work done with the **ESCO/ENISA** (by ASSIST-IoT):*

- Active participation in the working groups.
- Identification of gaps in cybersecurity domain.
- Contribution to cybersecurity white papers and best practices.

At the first period of the project, ASSIT-IOT started a lot of activates around different standardisation technical subjects using different paths to contribute in different SDO's and initiatives but focus on main technical subjects (most important I the project) and focus on main SDOs and initiative that are most active currently in our technical domains. In table below KPIs defined in the project proposal and target and achieved values are presented.

Table 3. Standardisation KPIs in the first half of the ASSIST-IoT project.

KPI	Target	Achieved
Supported standards in ASSIST-IoT	15	32
Communications to improve existing standards	2	2
Recommendations in relevant SDOs including Technical Reports, White Papers and Position Papers	4	5
SDOs and pre-normative initiatives engaged	6	9
Identified standards related to ASSSIT-IOT	50	70

8. Conclusions and next steps

From the standardisation activities and achievements description in above chapters we can observe the promising start of involvement in different standardisation subjects with focus on most related to the project developments, active participation in selected SDO's and initiatives, close follow up of their work as well as broad analysis of the standardisation needs and gaps. For the second period of the project more contributions is expected with broad cooperation among project partners. Also, a special Task Group in the project for standardisation purposes will be formatted to have more effective and fluent contributions preparation. Below the summary of further planned work per SDO's/initiatives is presented. Beside continuous follow up the standardisation work the new work items and contributions are planned.

Participation in ETSI:

- Further active participation in ETSI work.
- Follow up for new Specialist Task Forces and new work items.
- Participation in Working Groups for forthcoming standard actions.
- Cooperation using AIOTI for contribution to ETSI TR and evaluation of the ETSI reports and standards.

Participation in ITU-T:

- Active participation and follow up using OPL membership in ITU-T SG13 and SG20.
- Contributions to ITU-T, SG20 potential contributions under preparation.
- ITU-T SG meetings participation.
- New work items identification and analysis of new proposed subjects.

Participation in IEEE SA:

- Contributing to IEEE SA Open (GitLab)
- Contact IEEE SA Operational Program Management Team
- Explore membership of IEEE Societies to fostering Project submission.
- Participation as Working Groups for forthcoming standard actions.
- Participation as balloting stakeholder in 2 standardisation processes.
- Participation as public reviewer in 1 standardisation action of each relevant identified active project.

Participation in AIOTI:

- Participation in the AIOTI Board that will take place in IoT Week 2022 (Dublin, Ireland).
- Enrol in WG Standardisation WP3 to participate in the SDOs exploration and alignment.
- Enrol in WG Standardisation WP2 to actively contribute to the next release of HLA (v6.0).
- Contribution to white papers in data spaces subject.
- White paper co-editor of new AIOTI report „EU funded projects landscape focusing on IoT and Edge computing".
- Participation (as external contributors) to next events/actions of WG Urban Society.
- Enrol and actively contribute in VWG Mobility and Logistics to deliver a new scope-wide document (latest is from 2015).
- Observe and contribute to the next documents and actions of VWG Buildings, emphasising on the role of IoT in combination with BIM and as an indoor geo-localisation commodity.

Participation in BDVA/DAIRO:

- Enrol in TF7.SG7 and TF7.SG11 to align technical work of pilots 1, 3A and 3B and potentially contribute with relevant inputs via UPV (member of BDVA).
- Follow closely the reports of TF6.SG6 Standardisation.
- Participate in TF6-SG1 Data technology and architectures.
- Collaborate in the edition of the forthcoming SRIDA – Strategic Research, Innovation and Deployment Agenda of DAIRO.
- Contribution to position paper about data spaces and interoperability.

Participation in ESCO/ENISA:

- Active participation and follow up by S21SEC.
- New work items: WG identifies the capacities and capabilities to sustain EU digital autonomy by developing and fostering trusted technologies.
- Next contribution to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem.
- Contribution to new white papers about best practices in cybersecurity.

9. 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

[7] "An EU Strategy on Standardisation - Setting global standards in support of a resilient, green and digital EU single market", February 2022, https://ec.europa.eu/docsroom/documents/48598

[8] ETSI STF601 Cross-domain usability of IoT devices for humans and machines, TC (Technical Committee) SmartM2M, Technical Report „Use cases for cross-domain data usability of IoT devices", https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf

[9] AIOTI, High Level Architecture (HLA), Release 5.0, December 2020, https://aioti.eu/wp-content/uploads/2020/12/AIOTI_HLA_R5_201221_Published.pdf

[10] AIOTI, IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges, Release 1.0 September 2021, https://aioti.eu/wp-content/uploads/2021/10/AIOTI-Beyond-5G-R1-Report-Published.pdf

[11] AIOTI, IoT Relation and Impact on 5G Release 3.0, April. 2020, https://aioti.eu/wp-content/uploads/2020/05/AIOTI-IoT-relation-and-impact-on-5G-R3-Published.pdf

[12] AIOTI, High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0 January 2020, https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

[13] AIOTI, Edge Computing Standard Framework Concepts, Release 1.0, , September 2021, https://aioti.eu/wp-content/uploads/2021/09/AIOTI-SDOs_alliance_landscape_edge_computing_standard_framework_R1-Published.pdf

[14] AIOTI, Computing Continuum Scenarios, Requirements and Optical Communication enablers

[15] BDVA, Speeding Up Industrial AI And Trustworthiness, Position Paper, May 2021, https://bdva.eu/sites/default/files/Industrial%20AI%20and%20Trustworthiness%20-%20Position%20Paper%20-%20ConsultationVersion-May21.pdf

[16] BDVA/DAIRO, Response to the European Commission's proposal for AI Regulation, Position Paper, August 2021, https://www.bdva.eu/sites/default/files/BDVA_DAIRO%20response-feedback%20AI%20Regulation_Final_0.pdf