Alliance for IoT and Edge Computing Innovation

High Priority IoT Standardisation Gaps and Relevant SDOs

Release 3.0

AIOTI WG Standardisation

26 January 2024

Executive Summary

This report introduces an approach for the definition and identification of key IoT gaps in several initiatives. Based on the prioritisation of these gaps, the deliverable starts to address the work done within the relevant Standards Developing Organisations (SDOs) that need to cooperate in order to solve these gaps.

The key purpose of this report is to reflect a structured discussion within the AIOTI WG Standardisation and to provide consolidated technical elements as well as guidance and recommendations on identified IoT gaps.

This release of the report can be considered as a complete new version, where some of the gap analysis concepts introduced in the AIOTI report "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0" have been reused.

Table of Content

Table of Figures

List of Tables

1. Goal and motivation

This report presents an approach for the definition and identification of key IoT standardisation gaps in several initiatives.

There are now several IoT Standards Landscape reports available, including the work done by AIOTI in "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0", by ETSI in STF 505 and by EUOS in "Landscape of Internet of Things (IoT) Standards". These reports have identified a number of available standards which have reached a final stage (Technical Standard (TS) or TR, etc.) in a Standards Developing Organisation (SDO) or industrial consortia, and can be used for the work and development of the IoT community.

In this context, the possibility to develop large-scale interoperable solutions within this IoT landscape may be hindered if some elements in this landscape are missing. Such elements, referred to as "gaps", need to be carefully identified, characterised and prioritised in order to make sure that their resolution can be addressed by the IoT community (and more widely if needed).

The key purpose of this document is to start a structured discussion within the AIOTI WG Standardisation and to provide consolidated technical elements as well as guidance and recommendations on the identified IoT gaps.

The used methodology and applied definitions in this report are based on the AIOTI "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0" and AIOTI "High Priority Edge Computing Standardisation Gaps and Relevant SDOs, Release 1.0" reports.

The AIOTI "IoT LSP Standard Framework Concepts R3" report and the EUOS "Landscape of Internet of Things (IoT) Standards" report have been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives.

Most of the IoT research and standardisation challenges included in following sections have been described using the IoT research and standardisation challenges description template provided in Annex I.

This release of the report can be considered as a complete new version[1], where some of the gap analysis concepts introduced in the AIOTI report "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0" have been reused.

[1] Note that this release of the report has been written by AIOTI members that are as well members of the EUOS TWG IoT and Edge and contributed in EUOS on writing a similar IoT standardisation Gap analysis report. Moreover, the AIOTI and EUOS IoT standardisation Gap analysis reports have been edited by the same person. Therefore, a significant part of the text used in the AIOTI and EUOS IoT standardisation Gap analysis reports will be identical.

2. Possible IoT computing challenges

This section introduces IoT research and standardisation challenges that have been identified either from the IoT activities of the AIOTI members, for the period January 2020 up to date, or from literature studies. The goal of this IoT challenges collection is to form the basis of identifying the IoT standards gaps.

The research and standardisation challenges included in this section, have been described using the research and standardisation challenges description template provided in Annex I.

In the context of this report a standardisation challenge is considered to be the challenge, where solutions are available and mature enough and therefore, could initiate a standardisation activity in the context of an SDO. A research challenge is considered to be a challenge that is able to initiate a research activity.

2.1 IoT challenges collected from Ongoing Projects

This section provides description of IoT EU funded ongoing projects.

2.1.1 Challenges reported in DataPorts: A Data Platform for the Cognitive Ports of the Future

Abstract:

DataPorts is a project funded by the European Commission as part of the H2020 Big Data Value PPP programme. DataPorts brings together knowledge, expertise and innovation potential of very experienced partners in the fields of Industrial Data Platforms, IoT and Data Acquisition, Data Analytics and AI applications, blockchain, smart contracts and data sharing and trading, data providers, data protection and security, and technology integration. The consortium consists of 13 partners from 4 EU member countries: Spain, Greece, France and Germany, and an associated state: Israel. More specifically, the consortium involves 2 SMEs and 3 large-industry partners.

The project involves the design and implementation of a data platform and its deployment in two relevant European seaports connecting to their existing digital infrastructures and addressing specific local constraints.

The DataPorts Platform main aim is to connect to the different IoT systems and to the digital infrastructures currently existing in digital seaports, enabling the interconnection of a wide variety of systems into a tightly integrated ecosystem. In addition, it offers reliable data sharing and trading based on data owners' rules and offering a clear value proposition. Finally, it also strives to leverage on the data collected to provide advanced Data Analytics services based on which the different actors in the port value chain could develop novel AI and cognitive applications.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/871493
Project official URL:	https://dataports-project.eu/

IoT and/or Edge Computing research challenges:

The main challenge related with the IoT is the provision of all the technical tools and components through the platform for the acquisition, aggregation, processing and analysis of the data coming from the different stakeholders, sources and existing platforms. It implies:

- Contributing to specific activities related to standards in the freight sector, and to standardisation organisations and alliances related to IoT, security, cloud and big data and blockchain.

- Defining data models, mechanisms and enablers to provide semantic interoperability with data platforms, IoT devices, and other data sources, and developing the interoperability tools needed to facilitate generation of interfaces for sensing.

- Offering an IoT SDK Framework where data providers can feed their data into the data platform. For example, this data can be obtained from sensors, IoT platforms, IT systems (open or private), PCS controlled by the ports or Market Agents.

- Providing support to develop advanced services for cognitive ports, linking the platform with existing initiatives and results from areas like IoT, Big Data analytics or Artificial Intelligence.

- Achieving validation in two relevant European seaports connecting to their existing digital infrastructures and addressing specific local constraints.

Finally, it is interesting to highlight a specific scenario focused on the use of IoT sensors integrated with the DataPorts Platform. In that scenario regular containers will be fitted with permanent IoT devices, turning them into "Smart Containers". These "Smart Containers" are embedded with a set of sensors, enabling the measurement of real-time information such as identifying location, door opening and closing, vibrations, temperature, humidity, and any measured physical parameters of the surrounding environment of the containers. These IoT devices help stakeholders to gain valuable knowledge on the exact whereabouts and status of their container, enabling them to improve their logistics. By receiving a notification that the container has been unloaded from the ship, the user is enabled to proceed to dispatch a truck to pick it up at the optimal time. In addition, having Smart Container data may also decrease cargo loss, legal costs, insurance fees and investigation processes and damage to goods. At the same time, door-to-door visibility may result in increased cargo security; better service level, on-time deliveries since the processes flow better.

2.1.2 Challenges reported in DEMETER: IoT-based data analysis to improve farming

Abstract:

DEMETER's goal is to lead the digital transformation of Europe's agri-food sector through the rapid adoption of advanced IoT technologies, data science and smart farming, ensuring its long-term viability and sustainability.

Our key objective is to empower farmers and farmer cooperatives to a) use their existing platforms and machinery to extract new knowledge to improve their decision making and b) ease the acquisition, evolution and updating of their platforms, machinery and sensors by focusing their investments where these are needed. In parallel, DEMETER aims to transform the technology ecosystem for agriculture by reinforcing and establishing agreed standards, an agreed common information model, an interoperability space combined with an online/physical networked ecosystem and a set of interoperability components which will make the use of IoT technology effective and easy. This is achieved by a combination of human and digital solutions including the DEMETER Stakeholders Open Collaboration Space (SOCS) which is an online platform dedicated to all stakeholders (farmers, advisors, and technology suppliers) where they can collaborate, share best practices and participate in the co-creation processes.

In DEMETER, twenty pilot projects are used to demonstrate and evaluate how innovations and extended capabilities benefit from the interoperability mechanisms employed. Equally, these pilots monitor the evolution of the maturity level in the stakeholders involved.

A plethora of heterogeneous data is collected across pilots, ranging from simple temperature measurements to audio and video streaming. Various communication technologies are used, including LoRaWAN and 4G. Some data is processed locally, on the edge, while the main processing is done in cloud.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/857202
Project official URL:	www.h2020-demeter.eu
Pilot projects URL:	DEMETER Pilot Projects
Project dissemination material URL:	https://h2020-demeter.eu/dissemination-material/

IoT and/or Edge Computing research challenges:

- Development of a common agricultural data model (AIM) reflecting various dominant standards and existing models
- Semantic interoperability and heterogeneous data integration over IoT infrastructures
- Data analytics and knowledge extraction over IoT originating data
- Decision making and recommendations for farmers and agri advisors based on IoT infrastructures
- Syntactic interoperability over enablers deployed over IoT
- Security, privacy, trust and confidentiality over IoT
- Controlled sharing of resources in the agrifood domain, including IoT resource sharing support
- Processing of collected data on the edge (audio-video) to streamline and optimize the process.
- Validation of edge networking/ML technologies and integration with the cloud services.

2.1.3 Challenges reported in IoTAC: Security By Design IoT Development and Certificate Framework with Front-end Access Control

Abstract:

The IoTAC project aims to deliver a novel, secure and privacy-friendly IoT architecture that will facilitate the development and operation of more resilient IoT service environments through (i) monitoring and evaluation of applications security throughout the broader software development lifecycle; (ii) the introduction of an advanced access control mechanism based on new interactions and workflow using chip card and PKI technology; (iii) the runtime monitoring of the system as well as provisioning of security countermeasures that are implemented both at hardware- and at software-level and (iv) associated platforms which will provide security certification of the produced applications and system, based on international security standards, best practices and the research results of the project.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/952684
Project official URL:	https://iotac.eu/

IoT and/or Edge Computing research challenges:

- Advanced Security by Design concepts and implementations
- Quality Assurance and Trustworthiness of IoT Systems and Applications

2.1.4 Challenges reported in IoT-NGIN: Next Generation IoT as part of Next Generation Internet

Abstract:

It is well known that the Internet of Things (IoT) has been identified as one of the next big concepts to support societal changes and economic growth. To address this opportunity, the EU-funded project IoT-NGIN introduces novel research and innovation concepts to establish itself as the 'engine' that will fuel the next generation IoT. It starts by uncovering a pattern based meta-architecture and optimises IoT/machine-to-machine and 5G/machine-cloud-machine communications by extending the edge cloud paradigm. Moreover, it enables user and self-aware autonomous IoT systems through privacy-preserving federated machine learning and ambient intelligence, with augmented reality support. Finally, IoT-NGIN research towards distributed IoT cybersecurity and privacy. IoT-NGIN will be validated using dozens of heterogeneous devices, including drones and robots.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/957246
Project official URL:	https://iot-ngin.eu
Social media URL:	https://twitter.com/IotNgin
	https://www.linkedin.com/company/iot-ngin/
	https://www.facebook.com/IotNgin
Project material URL:	https://gitlab.com/h2020-iot-ngin
	https://hub.docker.com/u/iotngin

IoT and/or Edge Computing research challenges:

Research challenges in IoT-NGIN project:

- IoT Meta Architecture
- Enhance IoT/5G Further Enhancement Device-to-Device (FeD2D)
- Data sovereignty and privacy "by design"
- Privacy preserving federated ML
- Protection against attacks on federated ML
- DLT-based meta-level Digital Twins

Innovation challenges in IoT-NGIN

- Optimising 5G resource allocation
- Ultra-reliable IoT based on Time Sensitive Networking
- Secure edge cloud IoT micro-services execution framework
- Ambient Intelligence monitoring and control
- Dynamic machine self-learning framework

2.1.5 Challenges reported in SHAPES: Smart and Healthy Ageing through People Engaging in Supportive Systems

Abstract:

Throughout Europe, many people are handicapped by reduced capabilities that are either permanent or temporary. The EU-funded SHAPES project aims to create the first European open Ecosystem enabling the large-scale deployment of a broad range of digital solutions for supporting and extending healthy and independent living for such older individuals. SHAPES builds an interoperable platform integrating smart digital solutions to collect and analyse older individuals' health, environmental and lifestyle information, identify their needs and provide personalized solutions that uphold the individuals' data protection and trust. Important aspects are semantic IoT interoperability mechanisms developed as part of the core SHAPES Technological Platform that enables interoperability among more than 37 already integrated Digital Solutions, with open interfaces for third party solutions that can be integrated via the Marketplace. The project employs innovative approach to IoT interoperability, which avoids transferring private and identifiable data via the core of the platform, instead aligning the parties directly involved in data exchange with respect to their Information Models and interfaces. Hence only types of data exchanged may be visible to potential intruders, but no actual data, since it physically is not transferred in SHAPES.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/857159
Project official URL:	https://shapes2020.eu/

IoT and/or Edge Computing research challenges:

As part of its IoT and edge technological developments, the SHAPES project has defined and currently implements the SHAPES Technological Platform (TP), providing the architectural elements, APIs and SDKs and deployment of digital e-Health solutions, aimed at supporting seamless interoperability among IoT devices, platforms and services with respect for privacy and security of identifiable personal data. The associated challenges are to:

- Develop SHAPES TP's Framework – including components, interfaces and data models – ensuring security, scalability, extensibility, reliability, modularity, configurability and seamless dynamic interoperability among IoT systems, devise and services.
- Deploy foundation capabilities, including Big Data collection, management and processing without need to exchange private data, including speech recognition and video analytics.
- Implement IoT interoperability services following applicable standards concerning IoT-based platforms and the cross border exchange of health-related information.
- Implement proprietary security mechanisms (Single-Sign-on authentication for enabling data host authorization), supporting human-friendly authentication mechanisms (e.g., multimodal biometrics) to ensure data protection and privacy.
- Integrate and test e-Health Digital Solutions in the SHAPES Technological Platform, assessing their readiness for deployment in pilots. This includes 20 projects with dedicated solutions brought into SHAPES through three (3) Open Calls.
- Address secure e-Health systems interoperability via 5G mobile communication networks.

2.1.6 Challenges reported in ASSIST-IoT: Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT

Abstract:

ASSIST-IoT will provide an innovative reference architecture, envisioned as a decentralized ecosystem, where intelligence is distributed among nodes by implementing AI/ML close to data generation and actuation, and hyperconnecting nodes, in the edge-cloud continuum, over a softwarised smart network. This smart network will be realized by means of virtualized functions with clear separation of control and data planes, facilitating efficient infrastructure programmability. Moreover, the action will follow a DevSecOps methodology to ensure the integration of security, privacy, and trust, by design, in all aspects of the envisioned ecosystems.

ASSIST-IoT will be supported by several pillars: (i) an innovative IoT architecture to adapt to the NGI paradigm with a three-dimensional approach including intelligence, security and privacy by design, supporting decentralized collaborative decision-making; (ii) moving from semantic interoperability to semantically-enabled cross-platform, cross-domain data transactions within decentralized governance, DLT-anchoring transaction security, privacy and trust; (iii) development and integration of innovative devices, supporting context-aware computing to enable effective decision making close to events; (iv) introduction of self-* mechanisms, supporting self-awareness and (semi-)autonomous behaviours across IoT deployments, and (v) Tactile Internet support for latency applications, like AR/VR/MR, and human-centric interaction with IoT components. Results of the action will provide foundation for a comprehensive practice-based methodology for future designers and implementers of smart IoT ecosystems.

Finally, to validate research results, and developed solutions, and to ensure their wide applicability, extended pilot deployments with strong end-user participation will take place in: (i) port automation; (ii) smart safety of workers, and (iii) cohesive vehicle monitoring and diagnostics, bringing about domain-agnostic aspect of the approach.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/957258
Project official URL:	https://assist-iot.eu/
Social media URL:	https://www.facebook.com/assistiot/
	https://www.instagram.com/assistiot/
	https://www.linkedin.com/in/assist-iot-project/?originalSubdomain=be

IoT and/or Edge Computing research challenges:

The growing volume of unstructured data, sent by IoT devices, exceeds that of structured data. Many existing applications do not benefit from opportunities and flexibility offered by the existence of multiple data sources/streams. As data grows in size and heterogeneity, issues of scalability and interoperability become a rising concern. Modern AI uses Big Data to support users, self-train, and continually improve its performance. Increasing need for near-real-time reaction, and automatic decision making, suggests/enforces application of AI close to events, utilizing edge computing, smart networking and smart devices. These challenges require novel approaches, leading to highly decentralized ecosystems, supported transversely by security, privacy and trust enablers, to facilitate data sharing and protect the growing attack surface. Last but not least, human-centricity and new ways of interacting with IoT ecosystems have to be a core part of an innovative proposal, like the decentralized and multi-plane architecture that ASSIST-IoT introduces.

The challenges in the project are particularly:

- Design, implementation and validation of an NGIoT Reference Architecture, decentralised architecture (and its reference implementations), validated in three real-life pilots backing the NGI approach,
- Definition and implementation of distributed smart networking components,
- Definition and implementation of decentralized security and privacy exploiting DLT,
- Definition and implementation of smart distributed AI enablers, AI components (including smart devices), to be deployed in the "proper locations" across the IoT ecosystem continuum,
- Definition and implementation of human-centric tools and interfaces,
- Support Tactile IoT/AR low latency networks are needed, since interaction between users, devices and systems has to be smooth enough to be considered real-time,
- Interoperability will be addressed in terms of scalability, security, privacy and heterogeneity of data sources.

2.1.7 Challenges reported in IM-TWIN: from Intrinsic Motivations to Transitional Wearable INtelligent companions for autism spectrum disorder

Abstract:

Research into autism spectrum disorder (ASD) is important since the condition affects about 1 in 10 new born children in developed countries. Previous EU-funded research resulted in the development of a prototype wearable companion robot called PlusMe for ASD treatment and daily support. The EU-funded IM-TWIN project now aims to furnish PlusMe with intelligent behaviour, give it extra embedded biosensors and cameras for detecting a child's affective state and integrate all components into an Internet of Things system itself called IM-TWIN. It will also validate the device and its components with target stakeholders and perform activities to advance the system components to a higher technology readiness level. The project's work will help to meet the needs of ASD therapy centres and families with children with ASD.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/952095
Project official URL:	https://im-twin.eu/

IoT and/or Edge Computing research challenges:

The IM-TWIN project aims to develop some of the outcomes of the FET GOAL-Robots project towards market exploitation. The basic-research FET GOAL-Robots project aimed to study how intrinsic motivations ("curiosity") drive exploration and learning in children, and how such processes can be used to develop innovative autonomous robots. This led to conceive the idea that intrinsic motivations can be used to build engaging interactive robots usable for the treatment of children with developmental disorders, in particular within the Autism Spectrum Disorder (ASD). ASD is a condition with dramatic importance for the well-being of society as it affects about 1 out of 10 new borns in developed countries. We thus developed a "wearable companion robot", usable for the treatment and daily support of ASD, called PlusMe, now at the stage of prototype.

The IM-TWIN project has two sets of objectives. The first is to develop a highly-modular system pivoting on the PlusMe, called the IM-TWIN, addressing the needs of the market segment involving ASD therapy centres and, potentially, families with ASD children: this involves endowing the PlusMe with intelligent behaviour, equipping it with additional embedded biosensors and cameras for detecting the child's affective/emotional state, and integrating all components as a whole IoT system. The second set of objectives aims to validate the device and its components with target stakeholders, and to carry out a number of activities directed to advance the system components to a higher Technological Readiness Level (TRL7 for the PlusMe): this involves identifying the target groups and analysing ASD-related markets, refining and implementing an effective IPR strategy, planning the steps for individual and collective exploitation of the project outcomes, and finally creating a startup for the exploitation of the IM-TWIN system and its components. IM-TWIN will also foster the development of a lively high-tech research and application ecosystem.

2.1.8 Challenges reported in GATEKEEPER: Smart Living Homes – Whole Interventions Demonstrator For People At Health And Social Risks

Abstract:

The rising population of elderly in the EU member states is giving rise to new challenges in relation to independent living. The EU-funded GATEKEEPER project aims to ensure healthier independent lives for the ageing populations. It will connect healthcare providers, businesses, entrepreneurs, elderly citizens and the communities they live in. The goal is to create an open, trust-based arena for matching ideas, technologies, user needs and processes. The project will also incorporate data protection while underpinning value creation using advanced marketing patterns. The solutions deployed will involve 40 000 elderly citizens, as well as authorities, institutions, companies, associations and academics, and 8 regional communities from 7 EU Member States.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/857223
Project official URL:	https://www.gatekeeper-project.eu/about-gatekeeper/

IoT and/or Edge Computing research challenges:

- To deliver the **GATEKEEPER DIGITAL PLATFORM implemented through fault tolerant, secure, flexible and scalable micro-services infrastructure, based on open source and data standards**, built on top of reference W3C-Web of Things architectural models and including services referred to the health domain through HL7-FHIR and to the home domain through SAREF.
- To deliver the GATEKEEPER HEALTHCARE SPACE, where **intuitive and self-configuring dashboards, intelligent services for early risk detection and care plans, and a federated data infrastructure are provided** to healthcare professionals.
- To deliver the GATEKEEPER **CONSUMER SPACE**, where certified solutions, services and devices are provided to citizens for the management and prevention of health and social risks.
- To deliver the GATEKEEPER **BUSINESS SPACE**, where certified companies are able to develop solutions, services and devices alone or in partnership, following a set of standards in order to reach and boost the Digital Single Market.
- To deliver the GATEKEEPER ECOSYSTEM TRANSACTION SPACE, where services for data storage and processing, big data analytics and advanced visualization of business-oriented KPIs are provided for the exchange of solutions among providers and suppliers, based on data sharing and Value-based healthcare paradigms.
- To execute a series of PILOTS to demonstrate the effect, benefit, value and scalability of the GATEKEEPER solutions around REFERENCE USE CASES COVERING PRIMARY, SECONDARY and TERTIARY PREVENTION, initially deployed in 8 regions of 7 European countries.

- To provide an ECOSYSTEM COCREATION framework, resulting from Responsible and Social Innovation principles, aiming at engage and generate TRUST from Citizens, Healthcare Professionals, Supply and Demand Side, extended through open calls to SMEs, Start-ups, and new regions in an open innovation fashion.

- To implement a **STANDARDIZATION STRATEGY that allow the GATEKEEPER solution to be aligned with SDOs around legal and privacy aspects, healthcare, ageing, homes, cities and energies, IoT, Big Data and other Key Enabling Technologies, as well as value-based procurement**.

- To transform and process GATEKEEPER results in a reference and sustainable IMPACT FRAMEWORK for decision making about procurement of innovative solutions, integrating elements from Value-based Healthcare, Real World Data, and Health-Technology Assessment, involving relevant actors inside and outside the consortium through Communication and dissemination activities, for worldwide outreach of project activities and achievements.

2.1.9 Challenges reported in CHARM: Challenging environments tolerant Smart systems for IoT and AI

Abstract:

CHARM project will develop condition monitoring, predictive maintenance, automation, real-time manufacturing control and optimisation and virtual prototyping system demonstrators and test them in industrial settings. The ECS (Electronics, Components and Systems) technologies must be designed to withstand combinations of severe thermal, mechanical and chemical stress present during the manufacturing processes used in the industry.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/876362
Project official URL:	https://charm-ecsel.eu/

IoT and/or Edge Computing research challenges:

Digitalization has been identified as one of the key enablers for renewal and competitiveness of European manufacturing industries. However, grasping the digitalization and IoT-related opportunities can be limited by the harsh environmental conditions of the manufacturing processes and end use environments. The ECSEL-IA 2019 project initiative CHARM aims to contribute to solving this problem by **developing ECS technologies that tolerate harsh industrial environments**. The project concept centres around real industrial challenges from different types of end use industries. The synergies and impacts arise from similarities in technology solutions serving different applications and industry sectors.

The CHARM Use Cases include six different industry sectors, majority of them presented by innovative cutting-edge large enterprises that belong to the world-wide market leaders of their own sectors – while most of them being new to the ECSEL ecosystem: mining (Sandvik Mining and Construction Oy, FI), paper mills (Valmet Technologies Oy, FI), machining (Tornos SA, CH), solar panel manufacturing lines (Applied Materials Italia SRL, IT), nuclear power plants maintenance and decommissioning (ÚJV Řež a.s. CZ), and professional digital printing (Océ-Technologies B.V NL). The planned demonstrators engage these big players with European ECS value chains and showcase capabilities that serve manufacturing industries' needs at large. The **new technologies to be developed include novel multi-gas sensors, robust high temperature and pressure sensors, flexible sensors for paper machine rolls, wireless power transfer systems, connectivity solutions for rotating parts, advanced vision systems, and enablers for autonomous driving**.

2.1.10 Challenges reported in ATLAS: Agricultural Interoperability and Analysis System

Abstract:

Advanced digital technology and data play a vital role in ensuring sustainable production in today's agricultural industry. The EU-funded ATLAS project aims to develop an **open platform and create a sustainable environment for innovative agriculture**. The project will address the lack of **data interoperability in agriculture** by combining the use of agricultural equipment with sensor systems and data analysis. The ATLAS platform aims to deliver a service offering hardware and software interoperability using data from sensors to demonstrate the benefits of digital agriculture in a wide range of sectors affecting modern agriculture.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/857125
Project official URL:	https://www.atlas-h2020.eu/

IoT and/or Edge Computing research challenges:

The overall objective of ATLAS is the development of an open digital Interoperability Network service for agricultural applications and to build up a sustainable ecosystem for innovative data-driven agriculture using the Network.

The Interoperability Network will allow the flexible combination of agricultural machinery, sensor systems and data analysis tools to overcome the problem of lacking interoperability and will enable farmers to increase their productivity in a sustainable way by making use of the most advanced digital technology and data.

It will also define a service architecture, providing hardware and software interoperability layers which enable the acquisition and sharing of data from a multitude of sensors and the analysis of this data using a multitude of dedicated analysis approaches.

The technology developed in ATLAS will be tested and evaluated within pilot studies on a multitude of real agricultural operations across Europe along several use cases, e.g:

- precision agriculture tasks,
- sensor-driven irrigation management,
- data-based soil management,
- behavioural analysis of livestock.

2.1.11 Challenges reported in TERMINET: nexT gEneRation sMart INterconnectEd ioT

Abstract:

Tens of billions of devices are connected to the Internet of Things (IoT), and the number of connections is growing every second. Information is being constantly sent and received from one smart device to another. Based on cutting-edge technologies such as software-defined networking (SDN), multiple-access edge computing, and virtualisation for next-generation IoT, the EU-funded TERMINET project will develop a novel next-generation reference architecture. Its main aim is to simplify the connection of a vast number of different devices through a flexible SDN-enabled middleware layer. To improve supply chain processes, the project will design an IoT-driven decentralised and distributed blockchain framework within manufacturing. TERMINET's approach will be tested in real-life situations such as energy, smart buildings, smart farming, healthcare and manufacturing.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/957406
Project official URL:	https://terminet-h2020.eu/

IoT and/or Edge Computing research challenges:

- natural sciences/computer and information sciences/internet/internet of things
- social sciences/economics and business/business and management/business models
- engineering and technology/materials engineering
- engineering and technology/electrical engineering/electronic
- engineering/information engineering/electronic engineering/robotics/autonomous robots/drones
- natural sciences/biological sciences/ecology/ecosystems

2.1.12 Challenges reported in Hexa-X: A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds

Abstract:

2030 and beyond the world will face tremendous opportunities and challenges of sustainable growth. The Hexa-X vision is to Connect human, physical and digital worlds with a fabric of 6G key enablers. The key objectives of the Hexa-X project are: (1) Foundation for an end-to-end system architecture towards 6G; (2) Radio performance towards 6G; (3) Connecting intelligence towards 6G; (4) Network evolution and expansion towards 6G; (5) Impact creation towards 6G.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/101015956
Project official URL:	https://hexa-x.eu/

IoT and/or Edge Computing research challenges:

Figure 1 illustrates the key value areas as stated in the Hexa-X vision and associated KPIs and capabilities. Each key value area reflects multifaceted aspects for which KVIs need to be developed. The key values are sustainability, inclusiveness and trustworthiness, where sustainability is explicitly considered from two perspectives in Hexa-X. 6G in itself needs to be sustainable, which could, for example, be mapped to the network energy efficiency as a KPI. In addition, 6G is an enabler for sustainability and sustainable growth in other markets and value chains, potentially covering aspects of inclusiveness and trustworthiness. Trustworthiness as another core value for Hexa-X, in the context of security considerations for 6G. In addition, the value of new capabilities enabled with 6G needs to be captured; this includes integrated sensing, embedded devices, local compute integration and integrated intelligence, as illustrated in the lower right. Flexibility is seen as a core capability. As core capability, flexibility covers, for example, the applicability of 6G to a new value chain, including ease of deployment and operation in that environment and, consequently, the goal of enabling new business opportunities. Flexibility as new capability of 6G impacts, for example, AI-based network management and operation.

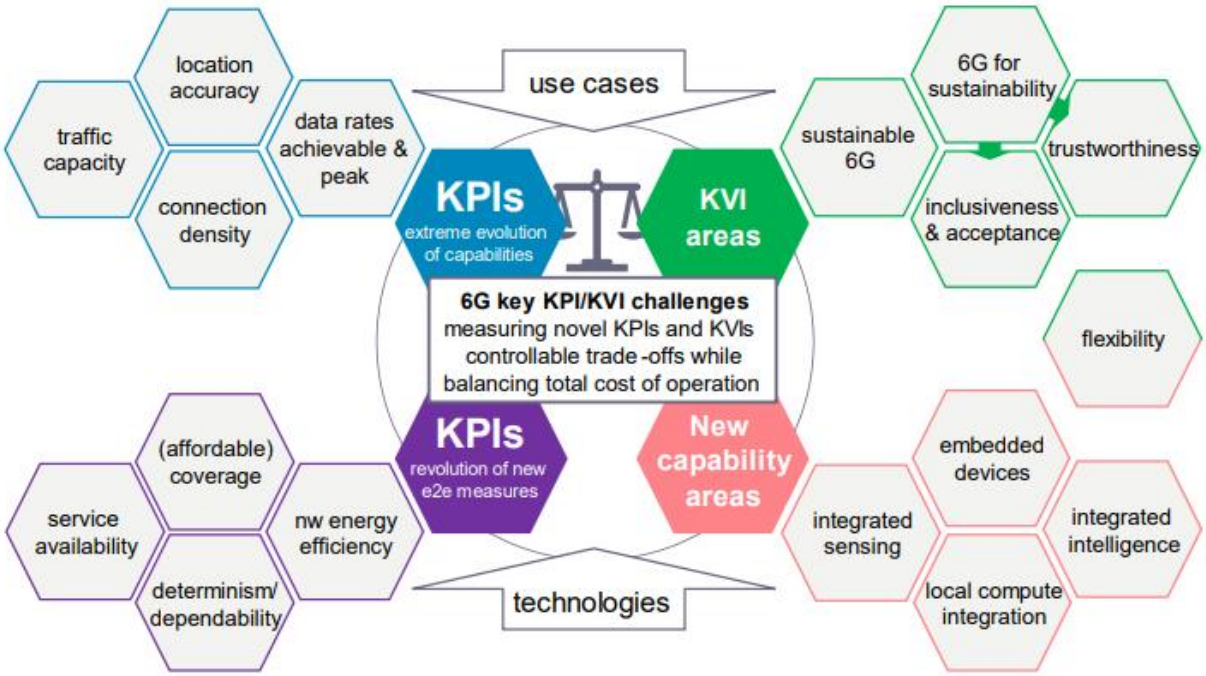

Figure 1: Clustering of Hexa-X Key Performance Indicators s and Key Value Indicators, copied from Hexa-X D1.1

In addition to the novel concept of KVIs, KPIs and performance goals need to go beyond what 5G can do to address new use cases discussed in the previous chapter. This includes increasing peak data rates and data rates achievable at the cell edge, density of connections, traffic capacity, and location accuracy to a substantial extent. For some performance goals, for example, dependability and determinism, service availability, affordable coverage, and network energy efficiency, the focus will shift more towards new end-to-end KPIs in specific use cases, and extreme performance in terms of data rates might be confined to specific scenarios rather than being a general, system-wide goal. Depending on the use case, novel KPIs for this end-to-end perspective will be defined. In addition, the relation between the fulfilment of KPIs and the associated total cost of operation becomes increasingly complex, given the number of stakeholders involved and the potential of networked intelligence and service-oriented ownership and business models on a local and global scale.

2.1.13 Challenges reported in InterConnect: Interoperable Solutions Connecting Smart Homes, Buildings and Grids

Abstract:

The EU energy market is conditioned by digitalisation. New rules and technological developments allow the proliferation of energy service providers in the EU member states with users having full knowledge and control over their appliances. However, interoperability represents a serious problem as a change of provider could mean the replacement of installations. The EU-funded InterConnect project proposes effective energy management using a resilient and practical ecosystem that is user-centric and market-driven. The project involves a range of specialised stakeholders, including advanced technology actors, manufacturers, providers and energy users. Via seven pilots, they will showcase an effective digital market for ensuring energy-efficiency at reduced costs that is beneficial to end-users.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/857237
Project official URL:	https://interconnectproject.eu/about/

IoT and/or Edge Computing research challenges:

- Large-scale pilots leading to market driven deployments
- Establish interoperability framework validating SAREF and semantic interoperability
- Marketplace of integrated digital platforms bringing the gap between IoT and Energy
- User centric energy and non-energy devices

2.1.14 Challenges reported in IntelliIoT: Intelligent, distributed, human-centered and trustworthy IoT environments

Abstract:

Traditional IoT setups are cloud-centric and typically focused around a centralized IoT platform to which data is uploaded for further processing. Those have multiple limitations, such as unreliable cloud connectivity, limited bandwidth, long reaction time, lack of self-awareness, and privacy concerns. Next generation IoT applications are incorporating technologies such as artificial intelligence, distributed ledgers and augmented reality, in order to realize semi-autonomous behaviour of vehicles, guidance for human users, or machine-to-machine interaction. Such applications must move to the edge or closer to the operational assets to amplify the level of their performance, create a more stable operation, and enable faster response. This transformation needs to build on localized IoT environments comprised of heterogeneous devices (e.g., edge computers as well as resource-constrained devices) that can collaboratively execute highly automated IoT applications – which include functions for sensing, actuating, reasoning, and control. IntelliIoT developed an architectural framework to enable IoT environments for semi-autonomous applications endowed with intelligence, built-in security, and trust and evolving with the human-in-the-loop. In IntelliIoT, three exemplary use cases of next generation IoT applications in the area of agriculture, heathcare and manufacturing have been demonstrated in a lab environment.

URL/Reference:

Project URL generated by the European Commission:	https://cordis.europa.eu/project/id/957218
Project official URL:	https://intelliot.eu/
Social media URL:	https://www.twitter.com/intelliot_eu
	https://www.linkedin.com/company/intellioteu/

IoT and/or Edge Computing research challenges:

IntelliIoT derive research challenges from three key classes of Next Generation (NG) IoT use cases described as scenarios from distinct vertical domains:

- Agriculture, where a fleet of vehicles (e.g., tractors) is semi-autonomously operated in conjunction with supporting devices (e.g., drones);
- Healthcare, where humans (patients) are semi-autonomously guided by artificial advisors based on IoT device input; and
- Manufacturing, where semi-autonomous machine-to-machine collaboration is important (e.g., interaction between industrial robot arms and machinery). In all three use case areas, a human expert plays a key role in controlling, monitoring and teaching AI-enabled autonomous systems.

To achieve project's vision, following key enablers and resulting research challenges are highlighted below:

- Autonomy and distributed intelligence: For the IntellIoT vision, distributed Machine Learning (ML) needs to consider application-specific target accuracies and worst-case training latencies under tolerable number of failures (reliability and robustness guarantees), wireless resources availability, on-device energy, storage, or computing restrictions. In addition, studying the control stability (plant, string, swarm- stabilities) of both single and multi-agent systems will be mandatory. Investigating the co-design of ML, communication-computation and control will be the basis of IntellIoT for developing the novel distributed AI solutions. For enabling the human-in-the-loop, the fusion between transfer learning, optimization and Federated Learning/Re-enforced Learning is a major research challenge.
- Next generation IoT computation and communication infrastructure: IoT applications are moving from the cloud to the edge, so that computing happens in closer proximity to the data producers and consumers. While IoT/edge devices can provide the computation side of the infrastructure, the communication side needs to be driven by advanced networking technologies, such as 5G New Radio (NR) and its extensions towards private networks and Industrial IoT. Building on the computation and communication infrastructure, IoT artifacts need to be able to discover and interact with one another. A first major step towards this goal has been the Web of Things (WoT), where interactions between devices are based on the Web architecture. Crucially, however, interoperability on the semantic level is a central requirement in the future evolution of the Web. Based on efforts of the W3C WoT, new means to use hypermedia for designing evolvable Web APIs and general-purpose clients are being explored. IntellIoT builds up on these developments towards integrating them with research on multi-agent systems (MAS) towards enabling a hypermedia-based MAS (HyperMAS) that are vertically and horizontally scalable with respect to the number of agents, devices, and interactions among these components. It will support self-aware agents within IoT environments and semi-autonomous IoT systems.
- Humans and trust in intelligent IoT: The wide adoption of IoT technologies in a plethora of domains, necessitates considering security, privacy, and trust requirements early in the design phase. Even securely initialised devices can be compromised, allowing attackers to affect connected devices, the network, or collaborative applications. Trust-based mechanisms can be used to defend against such attacks by monitoring the behaviour of each participant. An IoT deployment must also have the intelligence to protect itself proactively, e.g., through Moving Target Defence (MTD) techniques, where AI-driven agents periodically alter the network topology and/or configuration to counter attacks. Thereby, security assurance evaluations for IoT systems are still in their infancy. Supporting these security and trust mechanisms, IntellIoT will utilize blockchain, smart contracts, and distributed ledger (DLT) technologies to encode transaction logic and policies, which include the requirements and obligations of the party requesting access to an IoT resource as well as its provider.

All three use cases (agriculture, healthcare, and manufacturing) are based on semi-autonomous behaviour of the IoT system. Multiple heterogeneous devices are interacting, and autonomous control of their collaboration is provided through AI, which can be (re-) trained through human intervention. This pattern can be assumed for many next generation IoT applications.

Research challenges related to the described pattern are spread over three key areas:

- Providing the distributed artificial intelligence for autonomous behaviour,
- Providing efficient and reliable communication and computation resources, and
- Incorporating the human (by providing trust in the system) and learning from his input.

2.2. Other types of challenges

This section describes challenges found in other sources than EU funded projects.

2.2.1 Green machine learning for the IoT

Description of IoT research/standardisation requirement:

The energy consumption of modern machine learning approaches has become a concerning matter in the artificial intelligence community. Current machine learning models may include multiple layers consisting of thousands, millions or even billions of parameters. The training, maintaining, and running of such models may require the utilization of a large amount of computational resources. This amount can be prohibitively large for IoT devices –especially the ones which are battery-operated. In addition, the execution of modern machine learning approaches can generate a large carbon footprint can make their use unsustainable.

This challenge refers to designing green machine learning approaches which consider the impact of training and inference stages. Green machine learning must consider that the target environment may consist of cloud/edge resources and IoT devices, and that while all resources should be exploited, each resource may need to be treated differently.

Type of requirement:

- Non-functional requirement

Source:

- AIOTI Strategic Research and Innovation Agenda report
- Publication "Green Deep Reinforcement Learning for Radio Resource Management: Architecture, Algorithm Compression, and Challenges"

Application/Industry domain:

- Computationally intensive machine learning can be used in various fields including Health, Manufacturing and Urban Society.

2.2.2 Software Containers at the Edge

Description of IoT research/standardisation requirement:

Cloud computing applications move towards the edge of the network to avoid network bottlenecks and high communication latency when communicating with IoT devices. To accommodate this shift from the cloud to the edge, the technologies that run natively in cloud resources need to be adapted for the computing resources that are usually found in IoT environments, e.g., edge computing devices. An essential technology for running applications in the cloud is the use of software containers. Nevertheless, software containers may still not be supported due to resource/network requirements that are typically not be met by devices found in the IoT.

This challenge refers to defining the rules and designing the mechanisms for enabling the support of software containers at the edge of the network. Software containers can significantly improve application portability between different types of edge devices commonly found in IoT environments. However, this is, at the moment, difficult because resource-constrained devices may not have the computational power to run containers, especially since the requirements of a container may vary. It is therefore important to tackle this problem with appropriate rules and mechanisms, potentially separating "thick" container runtime (e.g., in the cloud resources) from "thin" container runtime (e.g., in the IoT resources).

Type of requirement:

- Functional requirement: Portability of applications among different resource-constrained devices at the edge of the network.

Source:

- AIOTI Strategic Research and Innovation Agenda report
- Publication "Toward Lighter Containers for the Edge" in HotEdge 2020

Application/Industry domain:

- Smart Cities: Deploying software containers at the edge of the network can bring benefits to various domains related to different vertical domains. An example is the Smart Cities, but it can be applied in all vertical domains.

2.2.3 Semantic interoperability of IoT data spaces

Description of IoT research/standardisation requirement

The rapid proliferation of IoT devices has generated an overwhelming amount of data, leading to the emergence of data spaces as a promising solution for managing and harnessing this vast information. However, the effective utilization of IoT data across diverse domains and applications may be hindered by the lack of semantic interoperability. This challenge aims at highlighting the need to achieve semantic interoperability in IoT data within different data spaces. This can be achieved by leveraging standardized data models and ontologies to achieve seamless data integration which can promote innovative applications and advanced decision-making.

This challenge refers to achieving semantic interoperability within data spaces that target different domains of the IoT. Notably, semantic interoperability within a single domain may be achieved using existing approaches such as the Asset Administration Shell (AAS) which targets the Industrial IoT, or the Semantic Sensor Network (SSN) ontology which focuses on sensor networks. <<Include as well SAREF>> While these models could be used within a data space, achieving semantic interoperability within multiple data spaces is still a challenge. Addressing this challenge could enable the common understanding of data, facilitating accurate interpretation and meaningful analysis of IoT data from different domains.

Type of requirement:

- Functional requirement: Achieve semantic interoperability within multiple data spaces that target different IoT domains

Source:

- AIOTI Report: Guidance for the Integration of IoT and Edge Computing in Data Spaces

Application/Industry domain:

- Semantic interoperability within data spaces can be applied to various domains of the IoT such as: horizontal domain, and all vertical domains.

2.2.4 Digital Twins – overall

Description of IoT research/standardisation requirement:

Digital twins are digital models of real-world products, systems or processes, and may be used for a variety of purposes, including monitoring, integration into software systems, planning and simulation. Digital twins provide an abstraction that decouples application software from the underlying details of the heterogeneous technologies and standards used to communicate with physical systems. This reduces the cost and complexity for developing applications and adapting them to changing requirements.

Type of requirement:

There is a need for many different kinds of standards in respect to digital twins. The following is a high-level account of functional requirements:

- **Identifiers** – how are digital twins identified to applications – how are identifiers managed, e.g., centralised and decentralised frameworks
- **Trust** – what kinds of attestations are needed to engender trust by remote applications? How can such attestations be revoked?
- **Security** – who can access which digital twins for what purposes – how to bootstrap security – how to report security breaches – how to describe and manage mitigations – the role of AI for detection and mitigation, etc.
- **Privacy** – requirements for compliance with regulations and corporate policies
- **APIs** – how to describe the software APIs exposed by digital twins
- **Knowledge** – how to describe digital twins in respect to their affordances, semantics, vocabularies, security requirements, terms and conditions of use, etc. This may also cover knowledge relating to energy consumption, repair, recycling and safe disposal of physical systems. Frameworks for distributed knowledge, e.g., Linked Data, and for mapping data and services across heterogeneous vocabularies that inevitably arise in large scale systems, likewise, support for changes over time, e.g., versioning and tracking version dependencies by application software
- **Data** – data formats, data models, analytics, streaming and real-time requirements
- **Discovery** – including centralised and decentralised frameworks for discovery
- **Provisioning** – how to provision digital twins, covering all stages of their life cycles, including orchestration, and market-based frameworks for matching suppliers and consumers, e.g., auctions.
- **Monitoring** – how to track usage and other kinds of analytics, support for proactive maintenance and performance tuning

Non-functional requirements include the use of particular technologies, e.g., graph models for knowledge and data, HTTPS for rest-based APIs, and public-key cryptography for security. A promising area of study is policy languages where open standards are key to adoption across the European Union. Federated learning can be used for training algorithms without the need to risk privacy/confidentiality. Blockchains provide a technical framework for distributed ledgers for smart contracts, identifier management, attestations and so forth.

Source

The above insight into standards comes from experience gained in many IoT related EU projects, along with work on the Web of Things and Linked Data at W3C:

- Boost 4.0 – smart manufacturing – https://boost40.eu/
- Gatekeeper – smart healthcare at home – https://www.gatekeeper-project.eu
- SmartEdge – swarm-based smart IoT – https://www.smart-edge.eu
- Nephele – orchestration of distributed IoT – https://nephele-project.eu
- TERMINET – IoT edge-cloud orchestration – https://terminet-h2020.eu
- F-Interop – IoT testing frameworks – https://cordis.europa.eu/project/id/687884
- Create-IoT – IoT coordination and support action – https://european-iot-pilots.eu/project/create-iot/
- W3C Web of Things – https://www.w3.org/WoT/

Application/Industry domain:

Digital twins are useful across many application sectors, e.g., horizontal domain and as well vertical domains, such as smart cities, manufacturing, logistics, healthcare, agriculture and so forth. The points listed above come from discussions in standards groups and experience in many research projects.

2.2.5 Heterogeneous vocabularies and ontologies in Digital Twins

Description of IoT research/standardisation requirement:

The ability to express knowledge is key to many applications of digital twins (see above). In any sufficiently large enough context, it is inevitable the different communities will use different vocabularies reflecting differences in requirements and differences in the sequences of modelling and naming decisions involved in developing applications. This also applies to enterprises where different business units within an enterprise will have different mindsets relating to their different functional goals.

The term "knowledge graph" generally refers to graph-based representations of data, data models and other metadata. Knowledge graphs are increasingly popular due to their flexibility compared with traditional relational databases. A single knowledge graph will become unwieldly as it grows to encompass the needs of an enterprise or ecosystem. It is therefore helpful to be able to decompose large knowledge graphs into a set of a smaller ones that use vocabularies suited to their users. This may still involve the role of a corporate entity for setting standards across an enterprise.

A further challenge is that software is expensive to develop and maintain. Changes required in one area of business may not be required in another. This leads to a mix of old and new software and processes, necessitating the need for managing change and tracking dependencies, e.g., on different versions of data vocabularies, data models and APIs.

Yet another challenge is that in the real world, knowledge is often imperfect and may be uncertain, imprecise, incomplete and inconsistent. This includes fuzzy scales, where a value corresponds to a fuzzy range. Fuzzy logic has a long history of application for device control. Argumentation theory has been worked on since the days of Ancient Greece and replaces logical proof with plausible arguments for and against a premise in question, akin to everyday practice in courtrooms, as well as to analyses for safety and for ethical approvals.

Type of requirement:

This brings opportunities for standards that simplify dealing with complex heterogeneous vocabularies and ontologies:

- Metrics for vocabularies and ontologies at different levels of maturity
- Mapping data across different vocabularies and ontologies according to the context
- Explicit versioning where direct backwards compatibility becomes impractical
- Tracking dependencies by software applications and processes
- Support for distributed knowledge graphs, including access control and trust
- Support for uncertain, imprecise, incomplete and inconsistent knowledge
- Support for applying argumentation theory when logical proof is unfeasible

These ideas have emerged from experience in standards discussions and research projects.

Source:

The above insights into standards comes from experience gained in many IoT related EU projects, along with work on the Web of Things and Linked Data at W3C:

- Boost 4.0 – smart manufacturing – https://boost40.eu/
- Gatekeeper – smart healthcare at home – https://www.gatekeeper-project.eu
- SmartEdge – swarm-based smart IoT – https://www.smart-edge.eu
- Nephele – orchestration of distributed IoT – https://nephele-project.eu
- TERMINET – IoT edge-cloud orchestration – https://terminet-h2020.eu
- F-Interop – IoT testing frameworks – https://cordis.europa.eu/project/id/687884
- Create-IoT – IoT coordination and support action – https://european-iot-pilots.eu/project/create-iot/
- W3C Web of Things – https://www.w3.org/WoT/

Application/Industry domain:

- Digital twins and heterogeneous vocabularies and ontologies are useful across many application sectors, e.g., horizontal domain and as well vertical domains, such as smart cities, manufacturing, logistics, healthcare, agriculture and so forth. The points listed above come from discussions in standards groups and experience in many research projects.

2.2.6 Quality of metadata in Digital Twins

Description of IoT research/standardisation requirement:

In respect to digital twins, metadata may vary considerably in its quality.

Type of requirement:

- Missing metadata – where the metadata hasn't been collected
- Out of date metadata – where the metadata available is too old to rely on
- Incorrect metadata – where a mistake has been made in its transcription
- Inaccurate metadata – where the metadata was poorly measured
- Heterogeneous vocabularies for metadata – e.g., for different ways to express locations such as postal addresses

This can effect the applications, including the ability to apply machine learning, necessitating data cleaning in mitigation. Bad metadata can make it harder to counter bias in datasets.

What kinds of standards would help? Establishing better standards for metadata could encourage improvements in the quality and reliability of metadata. We may also want to consider standards for annotating metadata in respect to quality.

Source:

These ideas come from experience across IoT projects and general awareness of the high cost of data cleaning for data science applications.

The above insight into standards comes from experience gained in many IoT related EU projects, along with work on the Web of Things and Linked Data at W3C:

- Boost 4.0 – smart manufacturing – https://boost40.eu/
- Gatekeeper – smart healthcare at home – https://www.gatekeeper-project.eu
- SmartEdge – swarm-based smart IoT – https://www.smart-edge.eu
- Nephele – orchestration of distributed IoT – https://nephele-project.eu
- TERMINET – IoT edge-cloud orchestration – https://terminet-h2020.eu
- F-Interop – IoT testing frameworks – https://cordis.europa.eu/project/id/687884
- Create-IoT – IoT coordination and support action – https://european-iot-pilots.eu/project/create-iot/
- W3C Web of Things – https://www.w3.org/WoT/

Application/Industry domain:

- Digital twins and quality of data are useful across many application sectors, e.g., horizontal domain and as well vertical domains, such as smart cities, manufacturing, logistics, healthcare, agriculture and so forth.

2.2.7 IoT Swarms

Description of IoT research/standardisation requirement:

IoT swarm edge systems consist of a collection of IoT devices whose coordination features decentralised and distributed control akin to flocks of birds, shoals of fish and colonies of ants, termites and bees. Swarm intelligence describes emergent behaviour arising from the interaction of the swarm participants with each other and their environment.

One kind of IoT swarms involves low powered devices that form a self-organising communication network that is resilient to faults and signal losses. Another kind of IoT swarm is where devices communicate via asynchronous message exchange between digital twins at an abstraction level above that of the underlying data formats and network protocols. This is a form of multi-agent system.

Swarm participants may have different capabilities and take on different roles as needed. This diversity increases resilience in respect to dynamically changing contexts, analogous to a group of people with diverse skills and opinions, that working together can solve challenges faster and more effectively. This relates to the idea of a hive mind as the collective intelligence of the group. Knowledge gained by a group member becomes available to the group as a whole, speeding adaptation.

Swarms of identical agents may be vulnerable to attacks that spread rapidly across the swarm. This calls for research on ensuring that attacks can be quickly detected and defended against, limiting such spreads. This could seek inspiration from biology, e.g., the immune system of multi-cellular organisms.

Type of requirement:

There are many opportunities for research and standardisation, e.g.:

- Energy – enabling swarms to be resilient to devices running low on energy reserves
- Interference – enabling swarms to be resilient to electromagnetic interference
- Security – secure messaging, secure updates, resilience to physical- and cyber-attacks
- Perception – distributed approaches to sensor data processing and semantic fusion
- Latency – distributed approaches to real-time control over many actuators
- Low-Code – high level abstractions for faster development of control programs
- Neurosymbolic – combining symbolic and non-symbolic approaches
- Traffic management – streamlining the movement of mobile swarm agents

According to AIOTI SRIA:

- The energy spent on edge IoT devices during swarm task execution is a key aspect to be considered. Total energy consumption includes static energy consumption and dynamic energy consumption during different tasks and the connectivity to other IoT devices and edge processing.
- The development of collaborative edge IoT swarm systems raise the issue of vulnerability to attacks by hackers from other fleets or via the interface with the cloud. The inherent distributed architecture for edge IoT swarm systems makes them more robust and secure and implies that the information is shared, stored, exchanged, and analysed locally and inside the swarm fleet, making it harder for hackers to access sensible data.
- The collaborative intelligent interaction among the IoT swarms requires further research on federated learning to execute or train ML models in edge IoT devices as part of a swarm fleet.

The Research priorities timeline is shown in ***Table 1*** and is copied from AIOTI SRIA.

Table 1 Swarm systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Swarm programming languages, tools, and OS	Define applicability and requirements of different swarm system, coming out with a taxonomy that help in Identifying different category of swarm.	Efficient implementation of languages, OS and tool for swarm managing and simulation.	Coherent and homogeneous Integration of SW and tool that allow to treat swarm fleets as a legacy IoT device in the full IoT-edge-cloud continuum
Domain applicability of swarms	Use case definition and Impact on verticals analysis.	Integration of swarms in multiple verticals sectors and demonstrate added value.	Swarms substitute in a seamless way for final users some of the currently existing IoT devices.
Swarms AI-fication	Applicability of traditional AI methods to swarm systems.	Implementation of advanced AI techniques in swarm system.	Full integration of cutting-edge AI technologies in swarm management.
Communication within and outside of the swarm	New low-power and very low latency protocols for in-swarm communication.	Smooth integration of delay sensitive networks surrounding the swarm with the in-swarm communication protocols.	Fluent, low latency and self-organizing communication of in-swarm and out-of-swarm protocols.

Source:

More details on this challenge can be found in AIOTI Strategic Research and Innovation Agenda report.

The above insights into standards comes from experience gained in many IoT related EU projects, along with work on the Web of Things and Linked Data at W3C:

- Boost 4.0 – smart manufacturing – https://boost40.eu/
- Gatekeeper – smart healthcare at home – https://www.gatekeeper-project.eu
- SmartEdge – swarm-based smart IoT – https://www.smart-edge.eu
- Nephele – orchestration of distributed IoT – https://nephele-project.eu
- TERMINET – IoT edge-cloud orchestration – https://terminet-h2020.eu
- F-Interop – IoT testing frameworks – https://cordis.europa.eu/project/id/687884
- Create-IoT – IoT coordination and support action – https://european-iot-pilots.eu/project/create-iot/
- W3C Web of Things – https://www.w3.org/WoT/

Application/Industry domain:

- IoT swarms can be applied in all vertical domains, however, they might be more useful in agriculture, mobility, manufacturing, logistics and smart cities.

2.2.8 Digital for Green

Description of IoT research/standardisation requirement

- Specify (or modify existing) interfaces that help monitor and control of the energy usage in communication protocol layer stacks applied in IoT and edge computing solutions
- Specify (or modify existing) IoT and edge computing related standards, interfaces, data models and ontologies to reduce the energy and carbon footprint (by e.g., monitoring and controlling energy and carbon footprint) in EU Green Deal areas:
  - Climate action
  - Clean energy
  - Sustainable industry
  - Building and renovating
  - Sustainable mobility
  - Biodiversity
  - From farm to fork
  - Eliminating pollution
- Specify (or modify existing) security and privacy by design standards required to secure the IoT and edge computing solutions applied to monitor and control energy and carbon footprint usage in EU Green Deal areas and which are as well able to protect any personal data lifecycle used by these solutions

- Specify an **agreed and aligned methodology** to measure the total avoided carbon emissions in industry scenarios, when applying ICT (e.g., IoT and Edge computing);

Type of requirement:

- The ICT sector must **ensure** the environmentally sound design and deployment of digital technologies by minimising the ICT (IoT and Edge computing) carbon footprint (e.g., PCF):
  - **Measurement of the benefits** provided by ICT in carbon reduction is a struggle
  - Use of **standardised connectivity related metrics/parameters** related to carbon footprint, in order to be used by stakeholders to compare and evaluate the benefit of different connectivity solutions in reducing the carbon footprint of industrial sectors
  - Include scope3 impacts in the CO2e (CO2 equivalent) footprint (e.g., PCF) calculation
- **The definition of an agreed and aligned methodology** to measure the total avoided carbon emissions in industry scenarios, when applying ICT (e.g., IoT and Edge computing), is a key requirement for the success of deploying ICT (e.g., IoT and Edge computing) solutions to reduce carbon emissions in industry scenarios

Source

- Based on the AIOTI report: "IoT and Edge Computing Carbon Footprint Measurement Methodology", Release 1.1

Application/Industry domain:

- Digital for Green requirements challenges can be applied in horizontal and as well on all vertical domains.

2.3. IoT challenges collected from AIOTI SRIA

These IoT challenges are collected from AIOTI SRIA. Note that the provided text, figures and tables are copied from AIOTI SRIA.

2.3.1 IoT and Edge Computing Granularity

Description of IoT research/standardisation requirement:

The concept of data processing, analysis and storage using the centralised cloud computing paradigm, comprising of a set of technologies, infrastructure, services, and applications, is no longer aligned with the always increasing demand of cellular, e.g., massive Machine Type Communication (mMTC), services and wireless intelligent connectivity usage scenarios[2]. Such scenarios aim at ensuring that the always growing number of IoT devices connected to the network can operate according to their specification, do not operate under conditions limiting the capabilities, and fulfil the expected Quality of Service (QoS). A new approach is therefore looked for, so to avoid creating silos and issues regarding both connectivity and real-time data processing and storage.

Edge computing provides the mechanisms for distributing data processing and redefines the IoT landscape by moving data processing and analytics at the edge by using AI/ML techniques and ensuring an advanced level of embedded security.

Edge computing moves service provisioning closer to producers and users of such services. It provides low-latency, mobility support, data analytics close to the data source, and reduced energy consumption.

For intelligent IoT applications, the edge computing concept is mirrored in the development of different edge computing levels (micro, deep, meta), that incorporate the computing and intelligence continuum from the sensors/actuators, processing units, controllers, gateways, on-premises servers to the interface with multi-access, fog, and cloud computing.

In IoT, there are many expectations for AI-based applications. AI processing happens mainly in the cloud.

Type of requirement:

With the improvement of AI enabling technologies, AI processing is moving into IoT devices. Intelligent edge devices will integrate software to train the AI model for different applications and executable software that runs the AI algorithms on the IoT devices.

Achieving a middleware architecture that integrates all the levels of the edge granularity and manage to effectively handle heterogeneous IoT resources, including networking and computing, is a new challenge for IoT/edge computing, leading to a unified networking and computing architecture.

The Research priorities timeline is shown in **Table 2** and is copied from AIOTI SRIA.

[2] B. Raaf et al., "Key technology advancements driving mobile communications from generation to generation", in Intel Technology Journal 18 (1), 2014.

Table 2 IoT and edge computing research priorities

Topic	Short Term 2023-2024	Medium Term 2025-2027	Long term 2028-2030
AI	Develop effective AI-based solutions that can exploit the benefit of DL and Federated Learning In different ways for the different needs of the Edge Granularity	How to deliver an IoT/edge-cloud continuum that takes care of all the specificities of all the Involved layers in a smooth way.	Distinction of the several Edge Granularity totally transparent to both systems and humans (final users).
Accelerators	Adapt, by using dedicated accelerators like ASICs or reconfigurable ones like FPGAs (depending on the constraints and requirements in focus), the different needs of the different edge granularity.	Exploit the smaller technology node so to embed in edge devices advanced accelerators functionalities.	No distinction possible anymore between FPGA and dedicated HW.
New HW architectures	Promising new pre-commercial architectures (like neuromorphic computing ones) will be assessed against existing traditional architectures based on CPU/GPUs or vector processors.	Edge devices containing novel HW architectures that can run AI algorithms so to achieve better results than the currently existing HW architecture based on CPU and GPU.	Synergy between legacy and novel architectures and usage of one or the other according to the real-time needs of the use case in focus, taking into consideration also real-time self-adaptation to the different workloads.
Security	Design a secure-by-construction distributed architecture that can impact all the different granularities of the Edge.	Deploy such architecture across different verticals and industrial domains.	Take on board quantum and post-quantum novel approach to ensure the highest possible security level at all layers and kind of devices in a transparent way for final users.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- IoT and Edge Computing Granularity can be applied in horizontal and as well on all vertical domains.

2.3.2 IoT Edge and X-Continuum Paradigm

Description of IoT research/standardisation requirement:

Distributed IoT digital platforms and infrastructures for collecting, processing, computing, communicating, and running analytics are evolving towards an interconnected ecosystem allowing complex applications to be executed from IoT edge to high-performance computing capabilities.

The IoT digital continuum includes computing resources placed at optimal processing points in the IoT system from the cloud data centre to edge IoT systems and endpoint devices that integrate E2E capabilities such as sensing, processing, connectivity, computing, storage, intelligence, security, safety, and privacy as illustrated in **Figure 2**.

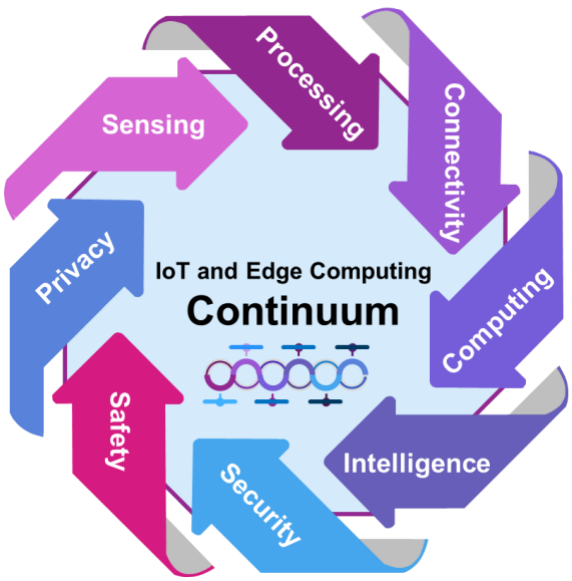

Figure 2 X-continuum paradigm, copied from AIOTI SRIA

One main challenge in this domain is how to accurately reproduce relevant behaviours of IoT applications workflow and representative settings of the IoT physical infrastructure, including AI-based learning/training and inferencing underlying the complex distributed continuum from micro-, deep-, meta-edge to cloud.

Type of requirement:

The implementation of IoT continuum-X requires research that integrates ideally open-source intelligence tools, HW and SW platforms, and systems, thus addressing the non-functional aspects of IoT systems with multiple elements as part of the continuum-X.

The Research priorities timeline is shown in

Table 3 and is copied from AIOTI SRIA.

Table 3 IoT edge and X-Continuum research priorities, copied from AIOTI SRIA

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Continuum refinement	High-level IoT-edge-Cloud continuum solutions for basic services, protocols, and resource allocation.	More refined continuum support of functionalities and lower layers management.	Fully supported and smooth management of all the edge granularities, types, services resources, and functions, in a fully heterogeneous ecosystem.
Common shared data space	Definition of domain-specific edge IoT applications aligned to common European data spaces.	Definition and implementation of common European data spaces.	Fully compatible interwork of data spaces with all geographical areas.
Instantiation	Piecewise and vertical-specific instantiation of all kinds of resources.	Coherent and homogeneous instantiation of all kinds of resources.	No distinction between the kinds of resources, all are treated as If they were homogeneous and available everywhere.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- IoT Edge and X-Continuum Paradigm can be applied in horizontal and as well on all vertical domains.

2.3.3 Intelligent Connectivity

Description of IoT research/standardisation requirement:

Networks and connectivity are becoming more heterogeneous and IoT devices use more and more a variety of equipment with different wireless access technologies. With the constant increase of the numbers of users (new contracts) and especially of things (sensors, metering systems, mobile/static robots, vehicles, drones, etc.) joining each day the communication network, the need for a smarter and more effective way of handling the related growing data created by those devices is becoming more and more an issue that needs the attention of the IoT community.

To handle such complexity and to manage in a smart way how the communication system can properly manage such an increasing amount of data (scalability problem), there's the need to define and elaborate on the intelligent connectivity concept, to optimise the usage of the networks but also to decrease the overall energy consumption of the overall IoT system.

Intelligent connectivity can be seen as the smooth synergy of different technologies and domains, so to offer final users of a communication system the best possible QoS, according to the given resource, available technology, and energy constraints.

Type of requirement:

The requirements of real-time response may be, amongst others, safety and mission-critical (like in telemedicine, for example) and, consequently, IoT communications solutions are numerous and diverse.

The next-generation IoT must address the convergence between different cells and radiation and develop new management models to control roaming while exploiting the coexistence of many different cells and radio access technology (RAT). New management protocols to handle user assignments regarding cells and technology will have to be deployed in the mobile core network to access network resources more efficiently.

Satellite communications is becoming a commercial reality and is to be considered as a new RAT, especially in remote (white spot/blind spot/not spot) areas. With the emergence of safety applications, minimising latency and various protocol translations bring tangible benefits to E2E latency.

The Research priorities timeline is shown in

Table 4 and is copied from AIOTI SRIA.

Table 4 Intelligent connectivity research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Mesh connectivity	Extend the mesh connectivity to different protocols e.g., LoRA 2.4GHz and dual-band transceivers, low-power and higher data rates.	Wi-Fi development and enhance support for TSN for industrial environments. AI-based cognitive solutions for mesh network management and mesh topology scalability.	Mult-protocol, multi frequency modules for autonomous edge IoT devices and vehicles. Seamless wireless/cellular connectivity for autonomous distributed systems. Ultra-low power, higher data rate mesh heterogenous mesh network architectures.
Interoperability	Seamless roaming between available wireless (including cellular) connectivity. Interoperability solutions for edge IoT connectivity in heterogenous applications and across industrial sectors.	E2E network automation and orchestration across multiple network domains and protocol layers. Interoperability solution for self-configuration, self-healing	Interoperability solution for high precision location and positioning services across heterogenous wireless networks.
Satellite	Advance the development on nanosatellites for IoT applications and the integration with terrestrial edge IoT infrastructure.	Research on management protocols deployed in the mobile core network to increase the efficiency of accessing network resources and reduce the energy consumption.	Satellite-cellular-wireless continuum for edge IoT applications.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Intelligent Connectivity can be applied in horizontal and as well on all vertical domains.

2.3.4 Energy-Efficient Intelligent IoT and Edge Computing Systems

Description of IoT research/standardisation requirement:

The number of IoT applications is constantly increasing, due to the fact that more and more IoT devices are being deployed in different industrial sectors.

Such IoT applications are consuming increasing amounts of energy, and new technologies and methods need to be developed to increase the energy-efficiency of the IoT devices, AI algorithms, architectures and IoT systems to reduce the overall power consumption.

Next-generation IoT edge applications and networks need greater flexibility to implement edge utilisation mechanisms to maximise energy-efficiency, latency, processing, data transfer, and dependability.

From the IoT system architecture perspective, the technological trend is to move the data processing and analysis from cloud to edge. This shift requires that the edge IoT devices in the edge micro-, deep- and meta-edge domains (e.g., sensors/actuators, microcontrollers, end-devices, gateways, edge servers) become more energy-efficient and support AI techniques at low power consumption to ensure high autonomy/longer battery life, system availability and reliability.

Edge IoT and AI green designs (e.g. advanced and adequate semiconductor technologies, efficient design, energy-efficient SW/HW platforms) are needed for providing environmentally reliable components at all IoT architectural layers and functions, energy-efficient and low CO_2 footprint at IoT infrastructure and technical solutions (edge, hybrid edge-cloud, AI-based learning/training, etc.), and finally also allowing the deployment of green manufacturing (e.g. manufacture IoT electronic components, HW/SW platforms, and IoT systems with minimal or no impact on the environment).

Type of requirement:

The complexity of intelligent IoT applications at the edge requires designing, analysing and optimising the energy-efficiency at the IoT system level by considering the aggregation, over the technology stack, of the functions required to fulfil a given IoT task. This includes estimating the energy used for learning/training of different algorithms implemented in various IoT architectural layers, both during inference and learning by employing real data sets from different databases, the energy consumption of the edge IoT devices (micro-, deep-, meta-edge), the energy consumption of the communication networks and the other processing and storage units by the IoT application, for performing different tasks and services.

The Research priorities timeline is shown in

Table 5 and is copied from AIOTI SRIA.

Table 5 Energy-efficient intelligent IoT and edge computing systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Energy harvesting	Research on hybrid solutions combining ultra-low power connectivity with energy harvested from ambient radio frequencies (RF), thermal, kinetic, and photovoltaic (e.g., solar, and indoor/outdoor lighting) energy sources.	Multi energy harvesting, wireless power for edge IoT devices. Energy harvesting solutions at mesh network edge IoT devices.	Energy harvesting for edge IoT devices integrating positioning and sensing. Cognitive energy management orchestration in edge IoT systems for data processing energy optimisation.
Energy-efficient hardware	Research on the next-generation of energy harvesting ultra-low-power devices with on-demand wake-up feature integrated into edge IoT applications	Edge IoT devices base on printed electronics (e.g., conductive inks, metal etching, laser-direct structuring (LDS) for printable circuits and batteries) to be embedded in objects and products. Energy harvesting for edge IoT devices integrating machine-vision camera systems using AI and ML.	Research on energy-harvesting interfaces for kinetic energy harvesting from heterogenous generators (piezoelectric, triboelectric etc.).
Energy-efficient data processing	System-level optimisation techniques combining lower power consumption and energy harvesting technologies. E2E energy methods and models for data compression and exchange in edge-cloud IoT platforms.	Benchmarking methods for energy-efficient and low CO_2 footprint of edge IoT infrastructure and technical solutions.	Energy-efficient data aggregation mechanisms in intelligent edge IoT systems considering the associated processing capabilities across the computing continuum.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Energy-Efficient Intelligent IoT and Edge Computing Systems can be applied in horizontal and as well on all vertical domains.

2.3.5 Heterogeneous Cognitive Edge IoT Mesh

Description of IoT research/standardisation requirement:

IoT edge can be formed by a mesh network of intelligent IoT devices using edge IoT platforms, including AI model training and ML inference that process, analyse, store information locally close to the data sources, and communicate and exchange information with other edge devices, computing units and across the computing continuum, made of cloud platforms and data centres.

Cognitive compute continuum applied in decentralised environments, including edge mesh infrastructures, can operate efficiently and reliably without a central entity for full knowledge and management about available resources and current workloads.

Type of requirement:

Novel IoT and edge computing designs bring innovative adaptive and behavioural-awareness capabilities to the IoT, so to set the foundations for developing the next-generation cognitive and self-adaptive IoT systems.

The huge number of heterogeneous edge IoT devices need to be integrated into mesh networks, in which the infrastructure nodes connect directly, dynamically, and non-hierarchically to other nodes and cooperate with one another to efficiently route data to and from edge IoT devices.

The Research priorities timeline is shown in Table 6 and is copied from AIOTI SRIA.

Table 6 Heterogeneous cognitive edge IoT mesh research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Architecture	Architectural models and meta-embedded operating systems with integrated stack for wireless mesh networking.	AI-based cognitive mesh architectures that integrate components and modules addressing context awareness, autonomous control, ambient intelligence, semantic reasoning, and federated learning.	Dynamic cognitive mesh architectures with AI and context-based configuration capabilities integrating features for swarm intelligence and distributed processing capabilities.
Cognitive Capabilities	Evolutive artificial cognitive mechanisms for edge IoT systems and the integration with mesh networks topologies.	Development of new algorithms and SW/HW self-X capabilities.	Integration of cognitive self-evolution capabilities in the entire mesh network and across the edge granularity including scalable AI capabilities across the continuum.
Computing Models	Computation algorithms for distributed computing applied to different heterogeneous, resource-constraint edge IoT devices across the edge continuum.	Heterogeneous cognitive edge IoT mesh frameworks integrating features such as distributed data collection, data analytics, networking, data management, edge IoT device management, resource management, service management, orchestration, and federated learning.	Meta-mesh computing models for global optimisation (energy, processing, time, etc.) of distributed systems.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Heterogeneous Cognitive Edge IoT Mesh can be applied in horizontal and as well on all vertical domains.

2.3.6 IoT Digital Twins, Modelling and Simulation Environments

Description of IoT research/standardisation requirement:

An IoT DT is a virtual representation of an IoT device that models the device's characteristics, properties, environmental conditions, behaviours, and functions over the operational lifetime, based on real-time data and information synchronised automatically and bi-directionally at a specified frequency and accuracy. An IoT DT uses simulation, ML, and reasoning to simulate various scenarios in different IoT applications and help optimise and improve the overall IoT system functionalities and services.

The real-time feature represents a vital characteristic to define IoT DTs, considering that the real-time instances vary according to IoT applications. In many IoT applications, time values are not defined identically, and such issue should be carefully considered when designing IoT DT instances. The synchronisation between the physical IoT device and its virtual representation in the simulation environment and the synchronisation of the events and scenarios in the simulation platform is critical for the performance of the whole IoT system.

Type of requirement:

The research areas for IoT DTs must consider the scope and augmentations of the IoT DT and the operational environment combined with the functions needed to realise the IoT DTs' communication capabilities, and the update frequency required for providing the optimal precision of the IoT DT, based on data measured and acquired during the operation and use of physical IoT devices.

Further research needs to investigate the different levels of IoT and edge computing intelligence through cognitive functions, implemented in the physical/digital and virtual devices.

Understanding, defining, and designing the simulation capabilities of the future IoT platforms, which will be able to provide different fidelity levels of simulation tuned by input parameters, time dependency, behaviour, and prediction aspects, intelligence, and IoT device complexity, are very challenging tasks, which require further investigation.

The Research priorities timeline is shown in

Table 7 and is copied from AIOTI SRIA.

Table 7 IoT Digital Twins, Modelling and Simulation Environments research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
IoT DT Models	Aggregation of heterogeneous IoT DT models.	Energy-efficient models. E2E features and optimisation.	Horizontal and vertical integration of IoT DT models. IoT DT that is capable of modelling and simulating the future state and behaviour of the IoT device.
IoT DT Modelling and Simulation Platforms	IoT DT platforms at the edge. Virtual sensing and actuation functions and simulations.	Predictive modelling platforms. Modelling and simulation of energy efficiency.	Integrated IoT platforms with virtual simulation environments including XR.
IoT DT Security	IoT DT security features integrated.	IoT DTs counterfeiting identification and mitigation.	Automatic recognition of fake DTs and their isolation or elimination.
IoT DT Connectivity	Simulation and modelling of the communication channels.	Define influence of the environments on the communication parameters of the IoT DTs.	Virtual platforms for the connectivity of IoT devices.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- IoT Digital Twins, Modelling and Simulation Environments can be applied in horizontal and as well on all vertical domains.

2.3.7 Internet of Things Senses

Description of IoT research/standardisation requirement:

Internet of Things Senses (IoTS) is an aspect of the IoT paradigm, by which unique sensing technologies are applied to replicate over the Internet the senses of sight, hearing, taste, smell, and touch, facilitated by AI, VR/AR, intelligent connectivity, and automation.

IoTS developments are essential for IoT, considering the growing interest towards technologies related to the Metaverse, which require cognitive decision-making capabilities of the edge devices, thanks to the use of AI algorithms implemented into such devices (e.g., robotic things).

Digital sensory experiences introduced by IoTS provide new types of Human-Machine Interface (HMI) devices, replacing keyboards, mice, and joysticks by providing interactions with the senses, so to allow a radical re-shape of some industrial domains as well as new use cases and business models.

In addition to the five standard human senses, one could consider in the IoTS domain an additional one, which is the sense of space (see **Figure 3**), based on merging and fusing the information from multiple sensor types and correlating them with the cognition process to better comprehend there surrounding environment where edge IoT devices are operating.

The sense of space is essential in the mobile autonomous edge devices operating in fleets across various environments. These edge IoT devices can use other sensors to deliver complex behaviours, for instance to detect movement for balance control, tilt the body of an object, and sense the direction and acceleration to attain and maintain equilibrium.

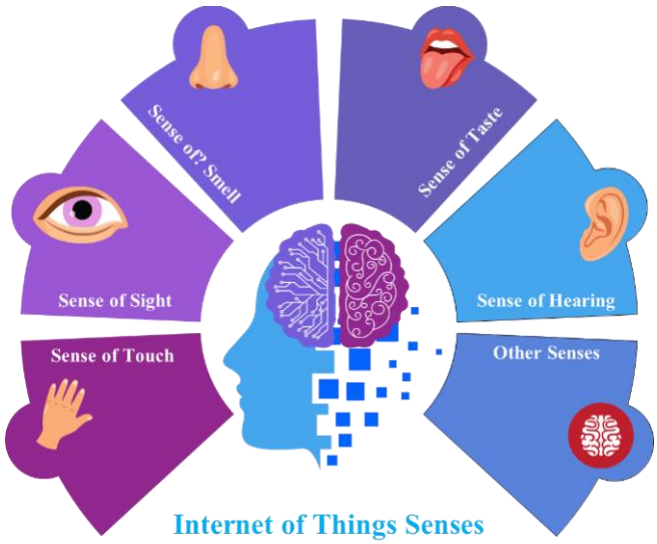

Figure 3 Internet of things senses

Type of requirement:

The development of IoTS, including Tactile IoT, requires reliable, robust and intelligent connectivity solutions and new edge-ready software and hardware for quickly and seamlessly managing, storing, analysing, and accessing the huge amount of data produces by sensors.

Further research and development in hyperconnectivity are needed to take the metaverse, VR and AR to the next level for uniform video streaming and remote control/surgery, or tactile internet.

Further research on sense-based intelligent connectivity includes the feel, taste, and smell of digital objects replicas of physical edge IoT devices and the development of platforms that can model and simulate the merging of digital and physical worlds into one another.

Implementing the intelligent connectivity solutions demanded by IoTS applications require new research to address the efficient radio resource allocation in wireless/cellular networks due to multiple haptic, human-to-human (H2H), machine-to-machine (M2M), and machine-to-human (M2H) communications that have various and sometimes conflicting service requirements.

The Research priorities timeline is shown in

Table 8 and is copied from AIOTI SRIA.

Table 8 Internet of things senses research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Sensors and Actuators	Development of haptic edge sensors and actuators with wireless mesh connectivity capabilities. Enhance the sensors capabilities in terms of precision, range, sensitivity, response time, spatial resolution, reliability, cost, and temperature dependence.	Research on lightweight energy-efficient, fast response time, low-cost, actuators providing capabilities of both the cutaneous and kinaesthetic feedback.	Development of new haptic actuators, cutaneous, muscle type for force tension, kinaesthetic, skin type for vibration, pressure, pain, temperature, etc.
Sensing Systems	Research on surface sensing using multiple arrays of sensors and techniques to identify the forces across the surface. New reading techniques for distributed sensing and actuation optimised for low-energy and acceptable latency.	AI-based sensor fusion techniques for multi-modal sensory. Real-time multiplexing schemes across protocol layers for integrating the various modalities in dynamically varying wireless environments.	Research on edge AI platforms for integration of multi-modal sensing systems for edge IoT applications.
Resource Managing and Orchestration	Further work on standardised groups of energy-efficient haptic codecs to be integrated into the kinesthetics and tactile information, to perform effectively in time-varying wireless environments. Development of new suitable performance metrics for analysing and comparing the performance (e.g., information fusion, connectivity features, data processing techniques, data reduction and control, compression, etc.) of various haptic systems over IoTs.	Research on the optimisation of collaborative multi edge IoT device communication and the effect of overlay routing, and IP-level routing on E2E latency. Research on ultra-high reliability in haptic communications considering trade-offs among reliability, latency, packet header to the payload ratio, etc.	Research on managing and orchestrating the wireless/cellular networks parameters to provide priority for resources based on QoS, safety-, mission-critical features for IoTS systems.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Internet of Things Senses can be applied in horizontal and as well on all vertical domains.

2.3.8 Decentralised and Distributed edge IoT Systems

Description of IoT research/standardisation requirement:

New network architecture paradigms for the forthcoming intelligent connectivity era are driven by a decomposition of the architecture[3] into platforms, functions, orchestration, and specialization aspects.

Future network platforms will be associated with an open, scalable, elastic, and agnostic heterogeneous cloud, which is data flow centric, will include hardware acceleration options together with a heterogeneity of computing architecture (x86, RISC-V, ARM, etc).

Type of requirement:

Research is needed in novel IoT distributed architectures to address the convergence of low latency, Tactile Internet, edge processing, AI and distributed security based on ledger or other technologies, and an effective deployment of multi-access edge computing (MEC).

Developing specific architectural requirements for distributed intelligence and context awareness at the edge is a future research topic, especially when considering the integration with mesh network architectures, so to form knowledge-centric networks for IoT, capable of serving many different applications coming from numerous vertical sectors.

Research on orchestration of IoT heterogeneous networks, adaptation of software defined radio and networking technologies for IoT, considering built-in E2E distributed security as well as hardware-based security solutions[4], trustworthiness, and privacy issues in edge computing environment must be extended, addressing the federation and cross-platform Integration for edge IoT applications.

The Research priorities timeline is shown in Table 9 and is copied from AIOTI SRIA.

Table 9 Decentralised and distributed edge IoT systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Decision making	Partially distributed decision-making mechanisms and techniques. Federated sub-system sharing a common decision mechanism	Fully distributed decision-making methods. Federated systems of systems sharing the same decision mechanisms	Fully distributed and federated systems, using heterogeneous decision mechanisms targeted to specific QoS or vertical sectors.

[3] Y. Xu, B. Qian, K. Yu, T. Ma, L. Zhao and H. Zhou, "Federated Learning Over Fully-Decoupled RAN Architecture for Two-tier Computing Acceleration," in IEEE Journal on Selected Areas in Communications, doi: 10.1109/JSAC.2023.3236003.

[4] J. Gopika Rajan. and R. S. Ganesh, "Hardware Based Data Security Techniques in IOT: A Review," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 408-413, doi: 10.1109/ICOSEC54921.2022.9952021.

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Security aspects	Established Privacy preserving techniques. Block-chain based security methods applied to selected vertical sectors.	Scalable block-chain based security mechanisms addressing some vertical sectors. Trustworthy and auto-adapting communication among several vertical sectors.	Secure-by-design system of systems, endowed with swarm intelligence and hardware-based security measures, fully Decentralised security procedures, self-adapting to real-time demands of heterogenous actors.
Learning mechanisms	Distributed learning. Federated learning.	Distributed and federated learning.	Continuous learning, self-adapting to the dynamic changing environment of a heterogeneous network supporting several vertical sectors.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Decentralised and Distributed edge IoT Systems can be applied in horizontal and as well on all vertical domains.

2.3.9 Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems

Description of IoT research/standardisation requirement:

To perform according to the devised expectations[5], the new distributed IoT architectures for computing optimisation across the edge continuum need to improve responsiveness by reducing decision-making latency, to increase data security and privacy, to decrease power consumption, using less network bandwidth, thus maximizing efficiencies, reliability, and autonomy.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

The IoT edge contains computing capabilities scaled across the micro-, deep- and meta-edge to process workloads, including the latest technology like AI model training and ML inference and signal processing, using signal conditioning[6] followed by neural networks[7] computing. The neural network computing and memory requirements are significantly reduced by using signal conditioning on the raw data.

In this context, federated learning as a distributed ML technique, which creates a global model by learning from multiple decentralised edge clients, is a significant technological development that can be implemented in distributed IoT architectures across the edge continuum.

Type of requirement:

Research on standard protocols and interfaces should address the integration of AI-based algorithms and lightweight protocols for communicating with different devices in a heterogeneous environment.

More research is needed to develop distributed learning/training algorithms and to maximise the average time between errors and optimise the availability by minimising the failure probability and average recovery time in the OTA learning/training process.

The IoT federated learning/training must consider the hybrid computing method that combines HW/SW and AI techniques across the edge continuum. Hybrid computing implies the integration of specialised advanced AI processors at different computing levels for both high-level and low-level operations.

Further research is needed to develop optimised algorithms for federated learning/training to complement and effectively leverage the computing capabilities with the AI-based processors and other types of processor architectures.

The Research priorities timeline is shown in

[6] R. Tirupathi and S. K. Kar, "Design and analysis of signal conditioning circuit for capacitive sensor interfacing," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 1717-1721, doi: 10.1109/ICPCSI.2017.8392007.

[7] Z. Li, F. Liu, W. Yang, S. Peng and J. Zhou, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 12, pp. 6999-7019, Dec. 2022, doi: 10.1109/TNNLS.2021.3084827.

Table 10 and is copied from AIOTI SRIA.

Table 10 Federated learning and AI for edge IoT systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Federate learning approaches	Techniques and methods to integrate federated learning into IoT/edge computing systems. Management of edge IoT systems, by addressing mesh network security and management by leveraging ML. Research on central training data sets and edge IoT local data sets.	Edge IoT intelligence architectures and AI frameworks for federated learning. Development of tools and tool chains for dedicated edge IoT federated learning. Methods for providing reference training datasets for performing standard federated learning application tuning.	Benchmarking techniques and methods for edge IoT federated learning. Scalability and portability of AI-based models for federated learning across the edge granularity.
Federated learning architecture and frameworks	Advanced architectural approaches for the federated learning server integrated into mesh networking environments.	Extend the capabilities of open-source federated learning frameworks. Communication and computation efficiency of the federated learning architectures, synchronisation optimisation among edge IoT devices.	Federated learning architectures addressing task scheduling, dynamic resource allocation to achieve low-latency services.
Hardware platforms for federated learning	HW requirements for implementing federated learning in edge IoT computing environments.	HW heterogenous solutions to minimise memory transfer, increase energy efficient and improve computational speed. Computation offloading and content caching using dynamic cache allocation techniques, context-aware offloading algorithms adapted to resource-constrained (e.g., limited storage and capacity) edge IoT devices.	HW/SW/AI algorithms heterogeneity management. Understanding of the effect of system heterogeneity on the AI model aggregation efficiency, accuracy and the divergence or convergence of optimisation processes.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems can be applied in horizontal and as well on all vertical domains.

2.3.10 Operating Systems and Orchestration Concepts for edge IoT Systems

Description of IoT research/standardisation requirement:

The extension of the IoT edge and edge-cloud federation is redefining the use of OSs and orchestration concepts across the IoT-edge-cloud continuum in real-time applications.

The increased use of embedded systems combined with processing units at the edge requires new ways of virtualising the computing capabilities and the OSs across the diversity of the HW components at the IoT edge. This also requires more frequent updates and upgrades of FW, SW, algorithms, and security patches for edge IoT devices. Challenges arise with more functions and services implemented in FW/SW/algorithms and the increasing complexity of electronic component interoperability, including managing agile and vulnerable edge IoT devices.

Type of requirement:

Ubiquitous meta-OS for IoT edge and orchestrating methods are needed to simplify the development, orchestration, and security of distributed IoT edge architectures and solutions. The development of new solutions using at the edge containers, virtual machines, and unikernels[8] provides a flexible foundation for expanding distributed edge computing deployments with a choice of heterogeneous HW, applications, and federated edge-clouds infrastructures. This brings further challenges to ensure distributed firewall, open orchestration APIs, support for virtual machines, containers, and unikernels application deployment models.

The Research priorities timeline is shown in Table 11 and is copied from AIOTI SRIA.

Table 11 Operating systems and orchestration concepts for edge IoT systems research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Decentralization techniques	Mature federated learning techniques that provide clear advantages in selected verticals and use cases	Advanced federated learning techniques suitable for all verticals	New paradigm of distributed management
Context awareness	Understanding the key surrounding parameters and functionalities that can guarantee an advance context awareness	Context awareness improved with semantic capabilities, i.e., abstracting from the sheer heterogeneous data and going up in the abstraction layer	New context awareness paradigm
Operating Systems	New meta-OS that can proof advantages against existing traditional OSs	Enhanced distributed meta-OSs that adapt resource computation and storage allocation to the run-time environment on a ms scale	Fully autonomous and reconfigurable management of the system resources in the IoT-edge-cloud continuum with fully distributed decision capabilities

[8] http://unikernel.org/

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Operating Systems and Orchestration Concepts for edge IoT Systems can be applied in horizontal and as well on all vertical domains.

2.3.11 Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems

Description of IoT research/standardisation requirement:

Current programming environments and tools for IoT[9] provide a centralised approach (either on-premises or cloud-based) where the main component transforms and processes most of the computation on data supplied by the edge and far edge devices.

This approach unfortunately implies several drawbacks, for instance unused edge computational power, a single point of failure, and violation of data boundaries (private, technological, etc.).

In this context, new research is needed in leveraging the resources available in lower-tier devices to improve overall dependability, performance, scalability, observability, and reproducibility of IoT systems using new programming and tools for distributed IoT.

Type of requirement:

The edge IoT distributed systems bring inherent challenges such as concurrency, partial failure, node dynamism, or asynchrony in their design and implementation.

The increasing complexity of the concurrent activities and reactive behaviours in edge IoT distributed systems are unmanageable by the existing programming models, tools, and abstraction mechanisms.

The Research priorities timeline is shown in

[9] A recent survey of the most used tools can be found at: https://www.iotforall.com/top-iot-tools-and-platforms-for-iot-development-and-developers.

Table 12 and is copied from AIOTI SRIA.

Table 12 Dynamic programming tools and environments for edge IoT systems research priorities

TOPIC	SHORT TERM	MEDIUM TERM	LONG TERM
	2023-2024	2025-2027	2028-2030
Programming tools	Programming tools for distributed algorithms for solving dynamic programming problems and work on models for asynchronous distributed computation addressing energy efficiency.	Tool chain techniques for edge IoT systems including formalisms and programming models. Enhance the language support for implementation, specification, and systematic testing of asynchronous edge IoT systems.	State machine-based programming language that supports the dynamic features required for building edge IoT asynchronous systems.
Integrated development environments	Integrated development environments and tools using module-based compositional refinement elements for development reasoning of dynamic edge IoT distributed systems.	Evolution of the development environment for edge IoT distributed systems to include the design of efficient, AI-based components, support for DLTs, swarm and mesh networking using mechanisms for addressing the heterogeneity of these systems.	Integrated development environments to address the dynamic changes in architectural patterns, abstractions, and component models for network-partition-tolerant, scalable, elastic, and self-X edge IoT distributed systems enabling testing and debugging.
Distributed system environments	Monitoring solutions for distributed edge IoT systems, including scanning how the data is collected, processed, distributed, and presented following what events are available and measuring the required parameters for the distributed processes.	Lightweight, agentless approaches and solutions for built-in monitoring technologies and protocols integrated into edge IoT distributed systems. Explore new hybrid and data streams approaches for monitoring distributed edge IoT systems.	Development programming models and protocols for reconfigurable edge IoT distributed systems.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems can be applied in horizontal and as well on all vertical domains.

2.3.12 Heterogeneous Edge IoT Systems Integration

Description of IoT research/standardisation requirement:

The next-generation IoT and edge systems are evolving towards heterogenous and hybrid systems, integrated using various technologies. IoT and edge computing heterogeneous system integration is essential for providing IoT solutions that offer scalability, security, and resilience for IoT application needs.

Heterogeneous edge IoT system integration refers to the integration of various HW/SW/AI components and convergence of different technologies into a higher-level IoT system that provides enhanced functionality and improved operating characteristics.

Type of requirement:

In edge IoT heterogeneous systems, memory bandwidth and data transfer between each compute unit can be unbalanced, and the different computing units have their own programming models, making integrating these systems difficult.

Edge IoT system integration requires interdisciplinary skills, work experience, proper planning, and vital ecosystems to cover the entire process, from design and development to deployment and maintenance.

IoT heterogeneous system integration implies the selection of IoT platforms that allows the storage, processing, sharing and visualization of the captured data by the distributed IoT devices, flexibility in managing content and permissions, and processing the data across the edge-cloud continuum, while allowing an easy use of the APIs, which can be focused on different kind of system integrations.

The Research priorities timeline is shown in Table 13 and is copied from AIOTI SRIA.

Table 13 Heterogeneous edge IoT systems integration research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Heterogenous HW solutions	Power-efficient performance for heterogenous HW including neural processing units (NPUs), to enable highly flexible, efficient processing for specific workloads and increased code portability across processors and platforms.	Reliable SW across the edge, fog, and cloud processing for heterogenous edge IoT HW systems.	Hybrid HW heterogeneous system architecture for edge IoT integrating heterogeneous processing elements into a coherent processing environment.
Heterogenous integration	Integration concepts to combine the heterogeneity of devices, data formats, communication, and interoperability issues due to heterogeneity.	Define frameworks for continuous design and validation flows for edge IoT heterogeneous systems.	HW/SW co-design on the next-generation intelligent, adaptive, and autonomous edge IoT systems.
Models	Modelling techniques for heterogeneous edge IoT systems considering models for physical phenomena, architecture, computation, communication scheduling, self-awareness, and adaptation.	Methods and techniques to model the edge IoT systems and their topology, heterogeneity, system loads, and simulation tools to identify how these parameters influence the system performance.	Simulation integration (co-simulation) of edge IoT heterogeneous systems by addressing scaling, composition, extensive range of required time resolution, HW-in-the-loop simulators and increasing automation in simulation integration.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Heterogeneous Edge IoT Systems Integration can be applied in horizontal and as well on all vertical domains.

2.3.13 Edge IoT sectorial and Cross-Sectorial Open Platforms

Description of IoT research/standardisation requirement:

The IoT platforms are categorised considering the area of operation and the functionalities (e.g., device, connectivity, edge, cloud), the sector (e.g., industrial, consumer, business), or the openness (e.g., open-source, commercial, proprietary) they address.

The IoT platforms developed around specific IoT devices or components provide the features for implementing functions to secure that the connected devices are installed, configured, and maintained using regular FW/SW updates and upgrades.

The IoT platforms focusing on connectivity provide capabilities and features for connecting various IoT devices to support, manage and orchestrate the connectivity functions, and implement communication services.

Type of requirement:

Specific research challenges for next-generation edge IoT platforms are to address the issues of heterogeneity, scalability and federated learning (FL) by implementing distributed architectures that guarantee the security and privacy of the data exchanged by an extensive number of intelligent edge IoT devices while subduing interoperability issues.

The research advances in the area of cognitive cloud platforms require new solutions for the federation of edge IoT platforms and the orchestration of edge-cloud domains for optimising the use of the resources, improving service quality, reducing the energy, the inefficient flow of data, and the costs.

Further research is needed to address the technological and semantic interoperability issues among heterogeneous IoT devices and platforms in the context of implementing distributed architectures and the integration of new technologies such as swarm computing.

The Research priorities timeline is shown in

Table 14 and is copied from AIOTI SRIA.

Table 14 Edge IoT sectorial and Cross-Sectorial Open Platforms research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Simulation capabilities	Edge IoT platforms can simulate and run a IoT devices in a specific vertical domain	Edge IoT platforms across multiple IoT verticals domains and supporting partial twinning.	Edge AI platforms working and seamless simulating all industrial domains and make use of advanced twinning.
Interoperability among platforms	Each edge IoT platform has its own API to expose its services to the outside world	Edge IoT platforms that can exchange data among themselves, making use of the recently defined data spaces at European level.	Edge IoT distributed platforms with embedded AI capabilities applied to industrial sectors and use Research on advanced edge AI platforms to exchange abstract data sets and make use of all defined data spaces at the European level.
Convergence of technologies	Edge IoT platforms that combine distributed architectures converging mesh, DLT and AI technologies.	Advanced edge IoT AI-based platforms with integrated cognitive functions for federated learning and other emerging distributed learning technologies.	Advanced edge IoT platforms including digital twining technologies to address the metaverse continuum for novel immersive applications.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- Edge IoT sectorial and Cross-Sectorial Open Platforms can be applied in horizontal and as well on all vertical domains.

2.3.14 IoT Verification, Validation and Testing (VV&T) Methods

Description of IoT research/standardisation requirement:

The broad range of existing security certification schemes for products, systems, domains, solutions, services, and organizations derives on a heterogeneous environment of solutions, making it difficult to understand what is needed to achieve a certain level of security in each context or technology. This heterogeneity also makes comparing certified devices more difficult, especially when different certification approaches, countries, and contexts are used. Currently, there is no unified solution that copes with these problems, facilitating the process of comparing and assessing the security levels.

Type of requirement:

The distributed environment and the changing behaviour of edge IoT devices drive the IoT applications to be very dynamic and, therefore, exposed to unexpected behaviour. Identifying unexpected behaviour and assuring that the demanded behaviour is followed can create a challenge in dynamic systems. Intended behaviours in edge IoT distributed systems can be defined as properties. Model-checking techniques are used to see whether these properties hold onto the formal specification of the system. In this context, property specification, verification and virtual validation can help detect errors in edge IoT dynamic and distributed systems.

Further research must consider upcoming technologies such as HW/SW neuromorphic and swarm computation. Of further interest is the automation and integration of the design/verification/debug cycle with operational data: automated repair, diagnosis, and updates for systems in the field based on observed failures.

The Research priorities timeline is shown in Table 15 and is copied from AIOTI SRIA.

Table 15 IoT Verification, Validation and Testing Methods research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Edge IoT AI-based systems VV&T	Virtual validation of edge IoT based system including AI-based components.	VV&T of self-X behaviours (e.g., self- configuration, self-healing, and self-adaption, etc.) of edge IoT systems.	Development of VV&T methods and techniques for real time and time constrained AI-based edge IoT distributed systems.
Distributed systems VV&T	Validation methods for edge IoT distributed systems focusing on both proof-based verification and systematic testing.	Mesh networking systems integrated as part of edge IoT infrastructure.	Edge IoT distributed systems embedding digital twin solutions.
Heterogenous systems VV&T	HW/SW neuromorphic and swarm computation applied to edge IoT distributed systems.	Heterogenous IoT distributed systems comprising of DLT platforms, edge AI frameworks and various ML implementations.	Federation of multi-blockchain-based data processing, edge IoT computing and swarm intelligence. Heterogenous edge IoT interoperability testing.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- IoT Verification, Validation and Testing (VV&T) Methods can be applied in horizontal and as well on all vertical domains.

2.3.15 IoT Trustworthiness and Edge Computing Systems Dependability

Description of IoT research/standardisation requirement:

Trustworthiness of the edge IoT systems can be defined as the degree of confidence one has that the edge IoT system performs as expected. Designing IoT edge trustworthiness into edge IoT systems requires the identification of characteristics and mechanisms of trust that can be embedded into the edge IoT system.

Type of requirement:

With IoT devices taking over critical tasks in system control and/or health areas, dependability is one major trend: data provided must be reliable and trustworthy.

Dependable edge IoT systems will incorporate devices and services of multiple different vendors which will only increase the challenge. For example, such systems need to cope with data privacy, cybersecurity, reliability, and safety at the same time.

Without proper standards and planning, guaranteeing all these attributes over a set of diverse devices from different vendors (being deployed in different networks and data centres) is next to impossible.

The IoT and edge computing systems have challenges in addressing the automated cybersecurity evaluation towards a more agile and cost-effective certification, dealing with the IoT dynamism.

Finally, there is also the need for objectives and evidence-based evaluation methodologies that would allow for a homogeneous evaluation, including comparability aspects. This limits the security management mechanisms addressing the whole lifecycle of the IoT device, dealing with the security changes that might invalidate the certificate.

The Research priorities timeline is shown in Table 16 and is copied from AIOTI SRIA.

Table 16 IoT Trustworthiness and Edge Computing Systems Dependability research priorities

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Trustworthiness	Edge IoT trustworthiness of ML models and explainability of AI (XAI) models used in Federated Learning.	Trustworthiness models for edge IoT self-adapting systems based on digital twin and AI-based technologies.	Frameworks providing guidelines, good practices and standards oriented to end-to-end trust in edge IoT systems.
Dependability	Define methods and tools to support the dependability system properties definition, composition and validation and relate the properties to different standards addressing different technologies.	Dependability properties at different layers of the edge IoT architecture by considering scalable concepts for HW, SW, connectivity, AI algorithms (inference, learning) and the design of flexible heterogeneous architectures that optimise the use of computing resources and the use of resource-constrained devices.	Virtualisation and simulation tools for managing the evaluation of edge IoT system dependability.

Topic	Short Term	Medium Term	Long term
	2023-2024	2025-2027	2028-2030
Benchmarking	Define different benchmarking methods and techniques of trust for an edge IoT system and provide compliance to an agreed-upon standard via certification schemes.	Benchmarking heterogenous edge IoT systems based on DLT, digital twins, mesh networking and AI technologies.	Benchmarking reference data sets for training edge IoT systems for federated learning.

Source:

- More details on this challenge can be found via: AIOTI Strategic Research and Innovation Agenda report.

Application/Industry domain:

- IoT Trustworthiness and Edge Computing Systems Dependability can be applied in horizontal and as well on all vertical domains.

3. Standardisation Gaps

The previous section introduced the IoT research and standardisation challenges that have been identified either from the IoT activities of the AIOTI community or from literature studies. Challenges and groups of challenges were presented in various degrees of detail and for specific applications and domains.

This section provides the method of identifying and mapping the AIOTI identified IoT challenges in standardisation gaps.

3.1 Definition and classification of standardisation gaps

The definition of a Standardisation Gap is based on the AIOTI in "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0" report and the ETSI and STF 505 document ETSI TR 103.375:

- **standardisation gaps**: missing or duplicate elements in the IoT standardization landscape
- **examples of standardization gaps are**: missing standards or regulations, missing APIs, technical interoperability profiles that would clarify the use cases, duplications that would require harmonization.

3.2 Standardisation Gaps: Identification

This section provides a collection of the identified IoT standardisation gaps. The identification of standards gaps is an important activity for the IoT and has been a subject of brainstorming with the AIOTI WG standardisation community.

The result of this brainstorming was to identify which IoT challenges that were described in Section 2 of this report are not mature and stable enough in order to initiate a standardisation action/activity. It was concluded that the only IoT challenges that required more research before being standardised are the IoT challenges:

- "2.2.1 Green machine learning for the IoT"
- "2.2.7 IoT Swarms"
- "2.3.2 IoT Edge and X-Continuum Paradigm"
- "2.3.5 Heterogeneous Cognitive Edge IoT Mesh"

The rest of the IoT challenges can be considered to be standardisation gaps.

3.3 Standardisation Gaps: Prioritisation

This section provides a prioritisation of IoT standardisation gaps in terms of their impact in the IoT landscape. The method of prioritising the standardisation gaps is by investigating the standardisation activities in SDOs, such as W3C, ETSI, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE and identifying missing or duplicate elements in the IoT standardization landscape.

In particular, the approach of prioritising the standardisation gaps is based on the intensity that a standardisation challenge is covered/worked out by an SDO.

4. Gap analysis and resolution work in SDOs

4.1 Gap Resolution

The identification and prioritisation of gaps, and in particular standardisation gaps, has been done with the objective to ensure that they can be dealt with and resolved (and closed) by one or more organizations in the IoT community, depending on the breadth and complexity of the gap.

The resolution of the (standardisation) gaps is the work of the relevant organizations of the IoT community, in particular the Standards Developing Organisations (SDOs) and Standards Setting Organisations (SSOs), see ETSI "Understanding ICT Standardization PRINCIPLES AND PRACTICE" report.

4.2 AIOTI identified IoT challenges covered/worked out by SDOs

History shows that many organisations have devoted resources to surveying the IoT standardisation landscape, as discussed in the introduction, however, each such effort has been a "snapshot", filtered by the particular focus of the organisation at that time, so that much of the work needs to be repeated by the next organisation or for the next update. Each such effort has required a "pull" or "polling" of the material produced by many SDOs, rather than being automatically updated in some way by the producers of the specifications.

The AIOTI "IoT LSP Standard Framework Concepts R3" report and the EUOS "Landscape of Internet of Things (IoT) Standards" report have been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives. Using the information applied in these AIOTI and EUOS IoT landscape reports[10] an analysis has been done on key SDOs, such as: W3C, ETSI, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE, to identify whether the AIOTI identified IoT challenges, described in Section 2, are covered or worked out by this SDOs. The complete analysis is included in tables, such as

[10] *Disclaimer: In order to identify whether the collected IoT challenges have been considered (or being considered) by SDOs, a data base (excel sheet) with IoT specifications published (or that are being worked out) by SDOs has been used in this section.*

This database (excel sheet) has been developed by StandICT.eu EU Observatory of ICT Standards (EUOS) Technical Working Group TWG IoT&EDGE. The StandICT.eu project is funded by the European Union under grant agreements no. 951972 and 101091933.

Table 17, used as an example in this section to show the AIOTI identified IoT challenges covered/worked out by ETSI.

The rest of the tables that show how the AIOTI identified IoT challenges covered/worked out by key SDOs, such as: W3C, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE, are provided in the Addendum to this Report.

Table 17: AIOTI identified IoT challenges covered/worked out by ETSI

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI GS NGP 005: Next Generation Protocol Requirements	https://www.etsi.org/deliver/etsi_gs/NGP/001_099/005/01.01.01_60/gs_NGP005v010101p.pdf	The scope of the Standard is to specify the minimum set of key requirements for the Next Generation Protocols (NGP), Industry Specific Group (ISG). The present document addresses requirements in the following areas: - Business Case and Techno-Economics - Migration - General Technical Requirements - Addressing - Security - Mobility - Multi-Access Support (including FMC) - Context Awareness - Performance (including Content Enablement) - Network Virtualisation - IoT Support - Energy Efficiency - e-Commerce - MEC - Mission Critical Services - Drones and Autonomous Vehicles and Connected Vehicles - Ultra Reliable Low Latency Communications	2.1.6 (Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT) 2.1.11 (nexT gEneRation sMart INterconnectEd ioT)
ETSI	ETSI TS 103 596-1 V1.1.1: Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 1: Conformance Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359601/01.01.01_60/ts_10359601v010101p.pdf	The present document provides a test specification, i.e. an overall test suite structure and catalogue of test purposes for the Constrained Application Protocol (CoAP). It will be a reference base for both client-side test campaigns and server side test campaigns addressing the conformance issues. It also provides a basis for interoperability testing and performance testing.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TS 103 596-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359602/01.01.01_60/ts_10359602v010101p.pdf	The present document provides an introduction and guide for developers and users investigating in security testing of the COAP communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. The structure of the present document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for COAP. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the COAP protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TS 103 596-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for CoAP; Part 3: Performance Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359603/01.01.01_60/ts_10359603v010101p.pdf	The present document provides an introduction and possible test specification, i.e. an overall test suite structure and catalogue of performance test purposes for the Constrained Application Protocol (CoAP) protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the performance issues.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TS 103 597-1 V1.1.2 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 1: Conformance Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359701/01.01.02_60/ts_10359701v010102p.pdf	The MQ Telemetry Transport (MQTT) protocol is one of the most popular representatives as many surveys have shown. In the present document the MQTT conformance testing is presented. It provides a basis for interoperability testing and performance testing.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TS 103 597-2 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359702/01.01.01_60/ts_10359702v010101p.pdf	The present document provides an introduction and guide for developers and users investigating in security testing of the MQTT communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. It belongs to a multipart technical specification addressing the most relevant testing aspects of MQTT: • conformance; • security; and • performance testing. While the conformance testing part presents a complete set of test purposes, the content for security and performance parts is different and focus on evaluating relevant testing techniques and the provision of samples that are specific for MQTT. For this reason, the structure of the document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for MQTT. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the MQTT protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TS 103 597-3 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for MQTT; Part 3: Performance Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359703/01.01.01_60/ts_10359703v010101p.pdf	Technology advancements are bringing ever-increasing computing power and network speed in the communication domain. The number of communicating devices is expected to increase by 2 orders of magnitude in the following decade and with that several challenges emerge. A main challenge pertains to efficiency regarding resource consumption and overall performance. As existing communication protocols evolve and new ones are created to fit the current technological capabilities and societal needs and the standards that serve the basis for interoperability and compliance. This is most relevant in the foreseen context of the Internet of Things (IoT) which envisions a very high density of connected devices in the near future. The Message Queuing Telemetry Transport (MQTT) protocol is one such example of evolution. While many IoT components communicate over standardized protocols, communication protocols for IoT like MQTT or CoAP evolved over time without a holistic approach for quality assurance. Although there are many published evaluations of various MQTT implementations, a lack of common language, methods and presentation of results is slowing down the adoption rate and overall evolution of the protocol. In the present document the performance testing is presented. It provides a basis for benchmark testing and performance evaluation for the MQTT protocol.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TS 103 410-1 SmartM2M; Extension to SAREF; Part 1: Energy Domain	http://www.etsi.org/deliver/etsi_ts/103400_103499/10341001/01.01.02_60/ts_10341001v010102p.pdf	This work extends the Smart Appliances reference ontology as defined in TS 103 264. The objective is to include input from the energy domain actors. This specification is defined as an extension of TS 103 264. Note: The TS 103 410 set of standards covers the multiple domains.	2.1.6 (Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT) 2.1.11 (nexT gEneRation sMart INterconnectEd ioT) 2.1.13 (Interoperable Solutions Connecting Smart Homes, Buildings and Grids)
ETSI	ETSI GR CIM 011 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)	https://www.etsi.org/deliver/etsi_gr/CIM/001_099/011/01.01.01_60/gr_CIM011v010101p.pdf	The present document is a choice of Test Purposes Description Language (TPDL), with the intention to capture all of the information required by the Test Template and should be parseable using software.	2.1.13 (Interoperable Solutions Connecting Smart Homes, Buildings and Grids)
ETSI	ETSI GS CIM 016 Context Information Management (CIM); NGSI-LD Testing Framework: Test Template	https://www.etsi.org/deliver/etsi_gs/CIM/001_099/016/01.01.01_60/gs_CIM016v010101p.pdf	The Testing Framework (document format) specifies a testing framework defining a methodology for the development of the test strategies, test systems and resulting test specifications. The present document identifies the implementation under test (scope of the testing), the format for the test specification, the test architecture, the points of control and observation, the naming conventions (e.g. for test case ID and test case grouping ID), etc..	2.1.14 (Intelligent, distributed, human-centred and trustworthy IoT environments)
ETSI	ETSI SAREF ontology SAREF: the Smart Applications REFerence ontology	https://saref.etsi.org/core/	The Smart Applications REFerence ontology (SAREF) is intended to enable interoperability between solutions from different providers and among various activity sectors in the Internet of Things (IoT), thus contributing to the development of the global digital market.	2.2.3 (Semantic interoperability of IoT data spaces); 2.3.12 (Heterogeneous Edge IoT Systems Integration)
ETSI	ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions	http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf	The scope of this document is a) to provide an overview of the IoT standards landscape: requirements, architecture, protocols, tests and related open source projects; b) to provide the roadmaps of the IoT standards, when they are available and to analyse the interactions of standards and open source in the context of IoT.	2.1.6 (Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT); 2.1.11 (nexT gEneRation sMart INterconnectEd ioT)
ETSI	ETSI TR 103 783 SmartM2M; SAREF: SDT interoperabilit	https://www.etsi.org/deliver/etsi_tr/103700_103799/103783	The objective of this technical report is to assure full alignment of SAREF and the oneM2M base ontology and provide guidelines about how devices adopting the oneM2M SDT (Smart Device Template) informational model	2.1.13 (Interoperable Solutions Connecting Smart

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
	y and oneM2M base ontology alignment	/01.01.01_60/tr_103783v010101p.pdf	can interoperate seamlessly with oneM2M devices and systems adopting SAREF and vice versa.	Homes, Buildings and Grids)
ETSI	ETSI TR 118 503 V1.0.0 Architecture Part 2: Study for the merging of architectures proposed for consideration	https://2020.standict.eu/sites/default/files/tr_118503v010000p.pdf	The present document provides an evaluation of existing M2M-related Architecture work undertaken by the founding partners of oneM2M, including: the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) of Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) of the USA; the China Communications Standards Association (CCSA); the European Telecommunications Standards Institute (ETSI); and the Telecommunications Technology Association (TTA) of Korea. Common Functional Entities and Reference Points are identified, as well as critical differences. New functionality will not be considered as part of this study. The present document is intended to ensure a common understanding of existing M2M Architectural approaches, in order to facilitate future normative work resulting in oneM2M Technical Specifications. The present document has been prepared under the auspices of the oneM2M Technical Plenary, by the oneM2M Architecture Working Group.	2.1.6 (Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT) 2.1.11 (nexT gEneRation sMart INterconnectEd ioT)
ETSI	ETSI EG 202 798 ITS; Testing; Framework for conformance and interoperability testing	http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/01.01.01_60/eg_202798v010101p.pdf	This document specifies the global framework for conformance and interoperability testing in ITS.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI EN 302 665 ITS; Communications Architecture	http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf	Definition of ITS Communications Architecture for Europe including the following views: • Scenario description; • Functional View and Information View; • OSI reference model view including Application View, Security View, Network&Transport View, Interface View, Management view; • Engineering view to support Implementation Guidelines for Interoperability; • Enterprise/Organizational/Operational view.	2.1.6 (Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT); 2.1.11 (nexT gEneRation sMart INterconnectEd ioT);
ETSI	ETSI TS 102 894-2 ITS; Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	http://www.etsi.org/deliver/etsi_ts/102800_102899/10289402/01.03.01_60/ts_10289402v010301p.pdf	Definition and specifications on the common data container at the applications and facilities layer.	2.2.2 (Software Containers at the Edge);
ETSI	ETSI TR 103 534-1 Teaching Material: Part 1 (Security)	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf	The document is based on the Security Report ETSI TR 103 533. It presents teaching material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability);

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TR 103 534-2 Teaching Material: Part 2 (Privacy)	https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf	The document is based on the Privacy Report ETSI TR 103 591. It focuses on producing teaching material on privacy and to direct the reader to other materials that are available in order to gain a basic understanding on what is involved in the privacy concept that is especially relevant, also, for the IoT environment.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability);
ETSI	ETSI TR 103 535 Guidelines for semantic interoperability in the industry	https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf	The document addresses the topic of semantic interoperability in the context of its potential usage by the industry in the development of IoT systems. The main objective of the document is to concretely foster the use of semantic interoperability in IoT by identify why it is important in industry IoT projects, to analyse the advantages and drawback of the available solutions.	2.2.3 (Semantic interoperability of IoT data spaces)
ETSI	ETSI TR 103 290 Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment	http://www.etsi.org/deliver/etsi_tr/103200_103299/103290/01.01.01_60/tr_103290v010101p.pdf	Smart City study would undertake compilation and review of activities taking place in the area of SMART City in Europe, Asia, and US. It will analyse the relevance of Smart City applications, and possible underlying network architecture. The report will describe use case descriptions for Smart City applications in context of but not limited to IoT communications.	2.2.2 (Software Containers at the Edge)
ETSI	ETSI TS 103 424 Publicly Available Specification (PAS); Smart Machine-to-Machine communications (SmartM2M)	https://www.etsi.org/deliver/etsi_ts/103400_103499/103424/01.01.01_60/ts_103424v010101p.pdf	The Home Gateway Initiative (HGI) worked on Specifications for home connectivity and Services enablement, in particular to encompass a delivery framework for Smart Home services. The defined architecture includes support for a standard, general purpose software execution environment in the HG (for third party applications), API definitions, device abstraction and interfacing with Cloud based platforms. This specification defines a smart home system architecture and derives requirements for the Home Gateway.	2.1.8 (Smart Living Homes – Whole Interventions Demonstrator For People At Health And Social Risks); 2.1.13 (Interoperable Solutions Connecting Smart Homes, Buildings and Grids)
ETSI	ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf	The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. Moreover, the present document addresses security considerations specific to constrained devices. The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table B.1 provides a schema for the reader to give information about the implementation of the provisions. Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document. The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)
ETSI	ETSI TR 103 533 Security; Standards Landscape and best practices	https://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr	The document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
		_103533v010101p.pdf	The document complements the overview of the Standards Landscape and best practice for privacy to be found in ETSI TR 103 591.	
ETSI	ETSI TR 103 591 Privacy study report; Standards Landscape and best practices	https://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf	The purpose of the document is to demonstrate that in view of the increasingly growing number of connected objects anticipated in the near future, effective protection of privacy and data protection would require that the relevant decisions are made upfront, at the design stage of the IoT systems.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)
ETSI	ETSI TS 103 646 V1.1.1 Methods for Testing and Specification (MTS); Test Specification for foundational Security IoT-Profile	https://www.etsi.org/deliver/etsi_ts/103600_103699/103646/01.01.01_60/ts_103646v010101p.pdf	The present document provides a test specification based on selected security requirements as known from IEC 6244-4-2. The chosen requirements have been collected by defining a dedicated IoT profile. The resulting IoT profile represents a generic minimum security level for IoT devices. Advanced requirements for higher security demands have been excluded. The present document serves as reference for a test campaign addressing the foundational security requirements of the IoT-Profile. The standardized notation TDL-TO has been applied for the definition of test purposes as it supports a unified presentation and semantics.	2.1.3 (Security By Design IoT Development and Certificate Framework with Front-end Access Control); 2.1.14 (Intelligent, distributed, human-centred and trustworthy IoT environments)
ETSI	ETSI TS 103 701 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf	The present document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 / ETSI EN 303 645, addressing the mandatory and recommended provisions as well as conditions and complements ETSI TS 103 645 / ETSI EN 303 645 by defining test cases and assessment criteria for each provision.	2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TS 102 731 ITS; Security; Security Services and Architecture	http://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf	The document will specify mechanisms and protocols for secure and privacy-preserving communication in vehicular environments, including vehicle-to-vehicle and vehicle-to infrastructure communication. It will provide credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. It will incorporate mechanisms such as addressing schemes building on pseudonymization concepts, the protocols for address update, and for exchanging, updating, and invalidating credentials to counterfeit attacks on security and reliability of communication. Further methods to prevent malicious tracking of identity and location will be provided.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)
ETSI	ETSI TR 103 536 Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms	https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf	The document outlines the nature, the role of IoT platforms and proposes elements for the identification of the most relevant ones. It also addresses detailed examples such as Industrial IoT to outline the challenges posed to generic IoT platforms. It addresses the issues related to the interoperability and interworking of IoT platforms, in particular standardized IoT platforms, and how the way they are handled can foster their adoption by the IoT community.	2.1.1 (A Data Platform for the Cognitive Ports of the Future)
ETSI	ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperabilit	http://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr	Providing guidelines for Security, Privacy and Interoperability in IoT System Definition based on the analysis of representative use cases.	2.3.15 (IoT Trustworthiness and Edge

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
	y in IoT System Definition; A Concrete Approach	_003680v010101p.pdf		Computing Systems Dependability)
ETSI	ETSI GS MEC 033 V3.1.1 Multi-access Edge Computing (MEC); IoT API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/033/03.01.01_60/gs_MEC033v030101p.pdf	The present document defines the IoT API to assist the deployment and usage of devices that require additional support in a MEC environment, e.g. due to security constraints, limited power, compute and communication capabilities, such as IoT and MTC devices. The API enables the device provisioning and configuration of the associated components and applications requiring connection to these devices. The present document describes the information flows and the required information. It also specifies the RESTful binding with the data model.	2.1.1 (A Data Platform for the Cognitive Ports of the Future)
ETSI	ETSI TR 103 675 AI for IoT: A Proof of Concept	http://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf	The present document is addressing the development of a Proof of Concept based on three Use Cases analysed and selected in the associated ETSI TR 103 674. ETSI TR 103 674 addresses the issues related to the introduction of AI into IoT systems and, as first priority, into the oneM2M architecture. ETSI TR 103 674 has identified and described several Use Cases of which three are used for the development of the Proof of Concept described in the present document.	2.1.14 (Intelligent, distributed, human-centred and trustworthy IoT environments)
ETSI/ one M2M	ETSI TR 103 716 V1.1.1 oneM2M Discovery and Query solution(s) simulation and performance evaluation	http://www.etsi.org/deliver/etsi_tr/103700_103799/103716/01.01.01_60/tr_103716v010101p.pdf	This work will develop a simulation with the goal to provide a proof of concept and a performance evaluation to support the selection and development of the discovery and query solution to be contributed to oneM2M. An extract of the simulation results will be used to support the discussion and the proposal with oneM2M.	2.3.6 (IoT Digital Twins, Modelling and Simulation Environments)
ETSI	ETSI TR 103 621 V1.2.1 Guide to Cyber Security for Consumer Internet of Things	http://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf	The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.	2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)
ETSI/ one M2M	ETSI TR 118 567 V4.0.0 oneM2M: Study on Management Object migration to SDT	http://www.etsi.org/deliver/etsi_tr/118500_118599/118567/04.00.00_60/tr_118567v040000p.pdf	The present document studies the completion of SDT (Smart Device Template) using <flexContainer> resource specializations and the possible migration of the existing device management model using Management Object (<mgmtObj>). The present document is initiated in the context of the Management Object Migration.	2.2.2 (Software Containers at the Edge)
ETSI	ETSI TS 103 942 Methods for Testing & Specification (MTS): Security Testing; IoT Security Functional Modules	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66187	Assemble security related functional modules within an IoT architecture, that support Security by Design and trustworthiness in order to retrieve relevant security testing methods and specific detailed test purposes using TDL-TO for generic IoT architectures applicable in multiple industrial domains.	2.1.3 (Security By Design IoT Development and Certificate Framework with Front-end Access Control); 2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods)
ETSI	ETSI TR 103 946 Methods for	https://portal.etsi.org/weba	Compile case study experiences related to the security validation and assurance for the integration and conformity	2.1.3 (Security By Design

SDO	Specification			Relevant AIOTI identified IoT challenges
	Title	URL	Abstract	Labels & Sections
	Testing & Specification (MTS): Security validation of IoT architecture application and conformity Case Study Experiences	pp/WorkProgram/Report_WorkItem.asp?WKI_ID=66188	of IoT applications with an existing IoT architecture in order to have a common understanding in MTS and related committees and to support trustworthiness. Industrial experiences may cover but are not restricted to the following domains: smart home, smart grid, unmanned air systems, automated driving.	IoT Development and Certificate Framework with Front-end Access Control); 2.3.14 (IoT Verification, Validation and Testing (VV&T) Methods); 2.3.15 (IoT Trustworthiness and Edge Computing Systems Dependability)

5. Standards Gaps Analysis and Recommendations

Section 4.2 of this report together with the Addendum to this Report provides an analysis on whether the 37 AIOTI identified IoT challenges, specified in Section 2 of this report are covered/worked out in the 670 SDO specifications that were listed in the EUOS "Landscape of Internet of Things (IoT) Standards" report[11].

As introduced in Section 3.3, the approach of prioritising the standardisation gaps is based on the intensity that a standardisation challenge is covered/worked out by an SDO.

[11] *Disclaimer: In order to identify whether the collected IoT challenges have been considered (or being considered) by SDOs, a data base (excel sheet) with IoT specifications published (or that are being worked out) by SDOs has been used in this section.*

This database (excel sheet) has been developed by StandICT.eu EU Observatory of ICT Standards (EUOS) Technical Working Group TWG IoT&EDGE. The StandICT.eu project is funded by the European Union under grant agreements no. 951972 and 101091933.

Table 18 gives an overview of the number of specifications and SDOs that are covering / working out each of the AIOTI identified IoT challenges.

The IoT challenge labels from S2.1.1 to S2.3.15, depicted in

Table 18, are representing the descriptions of the challenges described in Section 2, from subsection 2.1.1 to subsection 2.3.15 respectively.

Based on a brainstorming with the AIOTI WG Standardisation community, it has been concluded that depending on the level of the intensity that an IoT standardisation challenge is covered/worked out by an SDO, 3 categories can be distinguished:

high intensively covered standardisation gap in SDOs, marked in

- Table 18 with colour green and is represented in the situation: (*high #SDOs (≥ 4) & high #specs (≥ 8));*

medium intensively covered standardisation gap in SDOs, marked in

- Table 18 with colour yellow, and is represented in the situation: (*high #SDOs (≥ 4) & low #specs (< 8)) OR (low #SDOs (< 4) & high #specs (≥ 8));*

low intensively covered standardisation gap in SDOs, marked in

- Table 18 with colour red, and is represented in the situation: (*low #SDOs (< 4) & low #specs (< 8)*).

Table 18: AIOTI identified IoT challenges covered/worked out by SDOs

#chall	Description	IEC	ETSI	3GPP	ISO/IEC	EN/CENELEC	IEEE	ITU	W3C	IETF	OneM2M	#SDO	#Specs
2.1.1	Challenges reported in DataPorts: A Data Platform for the Cognitive Ports of the Future	41	2		31	37	1		5	24		7	141
2.1.2	Challenges reported in DEMETER: IoT-based data analysis to improve farming				31			1	4		1	4	37
2.1.3	Challenges reported in IoTAC: Security By Design IoT Development and Certificate Framework with Front-end Access Control	10	5		8	3			1	27		6	54
2.1.4	Challenges reported in IoT-NGIN: Next Generation IoT as part of Next Generation Internet				3		1	3	1	25	6	6	39
2.1.5	Challenges reported in SHAPES: Smart and Healthy Ageing through People Engaging in Supportive Systems							1			2	2	3
2.1.6	Challenges reported in ASSIST-IoT: Architecture for Scalable, Self-*, human-centric, Intelligent, Secure, and Tactile next generation IoT	9	5		3	1	1	2	4	21	1	9	47
2.1.7	Challenges reported in IM-TWIN: from Intrinsic Motivations to Transitional Wearable INtelligent companions for autism spectrum disorder				3			1				2	4
2.1.8	Challenges reported in GATEKEEPER: Smart Living Homes – Whole Interventions Demonstrator For People At Health And Social Risks		1					10			2	3	13
2.1.9	Challenges reported in CHARM: Challenging environments tolerant Smart systems for IoT and AI					22	1	1			1	4	25
2.1.10	Challenges reported in ATLAS: Agricultural Interoperability and Analysis System							1			1	2	2
2.1.11	Challenges reported in TERMINET: nexT gEneRation sMart INterconnectEd ioT		5		3	6					1	4	15
2.1.12	Challenges reported in Hexa-X: A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human,			3			4		2	4	5	5	18
2.1.13	Challenges reported in InterConnect: Interoperable Solutions Connecting Smart Homes, Buildings and Grids		3		1		3		4		9	5	20
2.1.14	Challenges reported in IntellioT: Intelligent, distributed, human-centered and trustworthy IoT environments		1		2	1		4			1	5	9
2.2.1	Green machine learning for the IoT											0	0
2.2.2	Software Containers at the Edge		3									1	3
2.2.3	Semantic interoperability of IoT data spaces	41	2		8	20	1	1	2	15	8	9	98
2.2.4	Digital Twins – overall		1		2							2	3
2.2.5	Heterogeneous vocabularies and ontologies in Digital Twins				4							1	4
2.2.6	Quality of metadata in Digital Twins				2							1	2
2.2.7	IoT Swarms											0	0
2.2.8	Digital for Green	1			2	5		8		26		5	42
2.3.1	IoT and Edge Computing Granularity		1								2	2	3
2.3.2	IoT Edge and X-Continuum Paradigm											0	0
2.3.3	Intelligent Connectivity	11								87		2	98
2.3.4	Energy-Efficient Intelligent IoT and Edge Computing Systems							1			1	2	2
2.3.5	Heterogeneous Cognitive Edge IoT Mesh											0	0
2.3.6	IoT Digital Twins, Modelling and Simulation Environments		1		1							2	2
2.3.7	Internet of Things Senses											0	0
2.3.8	Decentralised and Distributed edge IoT Systems	20		3		7				99		4	129
2.3.9	Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems										2	1	2
2.3.10	Operating Systems and Orchestration Concepts for edge IoT Systems											0	0
2.3.11	Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems							1	2			2	3
2.3.12	Heterogeneous Edge IoT Systems Integration		1								7	2	3
2.3.13	Edge IoT sectorial and Cross-Sectorial Open Platforms										3	1	3
2.3.14	IoT Verification, Validation and Testing (VV&T) Methods	17	11			2		16		25	2	6	73
2.3.15	IoT Trustworthiness and Edge Computing Systems Dependability	13	11		3					26	8	5	61

Figure 4 and Figure 5 provide a more detailed overview of the intensity that an IoT standardisation challenge is covered/worked out by an SDO and by specifications, respectively. The IoT challenge labels from S2.1.1 to S2.3.15, depicted in Figure 4 and Figure 5, are representing the descriptions of the challenges described in Section 2, from subsection 2.1.1 to subsection 2.3.15 respectively.

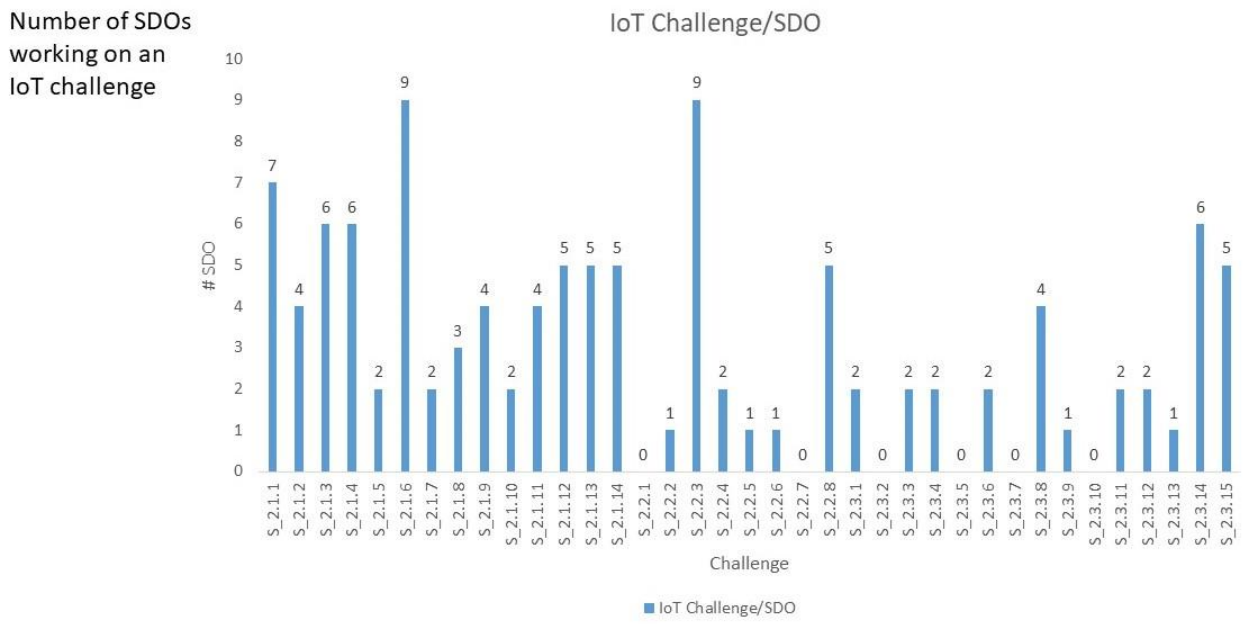

Figure 4: Number of SDOs covering / working out an AIOTI IoT identified challenge

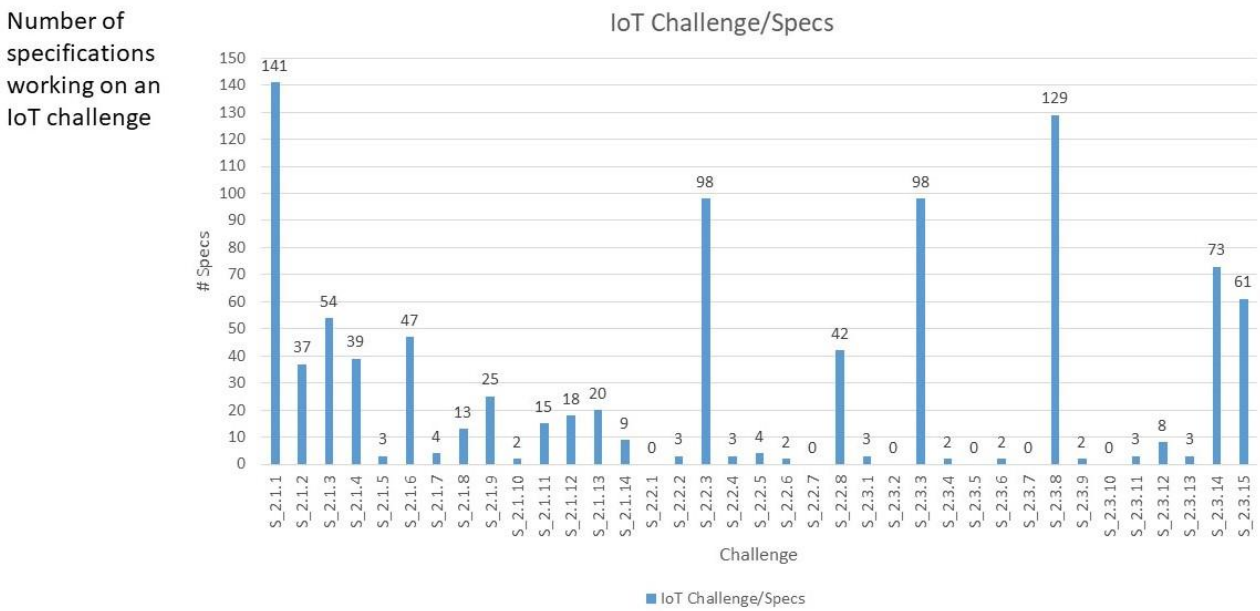

Figure 5: Number of specifications covering / working out an AIOTI IoT identified challenge

From this analysis it can be concluded that:

- the following IoT challenges, need more research before being standardised:
  - "2.2.1 Green machine learning for the IoT"
  - "2.2.7 IoT Swarms"
  - "2.3.2 IoT Edge and X-Continuum Paradigm"
  - "2.3.5 Heterogeneous Cognitive Edge IoT Mesh"
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - "2.1.5 Challenges reported in SHAPES: Smart and Healthy Ageing through People Engaging in Supportive Systems"
  - "2.1.7 Challenges reported in IM-TWIN: from Intrinsic Motivations to Transitional Wearable INtelligent companions for autism spectrum disorder"
  - "2.1.10 Challenges reported in ATLAS: Agricultural Interoperability and Analysis System"
  - "2.2.2 Software Containers at the Edge"
  - "2.2.4 Digital Twins – overall"
  - "2.2.5 Heterogeneous vocabularies and ontologies in Digital Twins"
  - "2.2.6 Quality of metadata in Digital Twins"
  - "2.3.1 IoT and Edge Computing Granularity"
  - "2.3.4 Energy-Efficient Intelligent IoT and Edge Computing Systems"
  - "2.3.6 IoT Digital Twins, Modelling and Simulation Environments"
  - "2.3.7 Internet of Things Senses"
  - "2.3.9 Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems"

- "2.3.10 Operating Systems and Orchestration Concepts for edge IoT Systems"
- "2.3.11 Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems"
- "2.3.12 Heterogeneous Edge IoT Systems Integration"
- "2.3.13 Edge IoT sectorial and Cross-Sectorial Open Platforms"

- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
  - "2.1.8 Challenges reported in GATEKEEPER: Smart Living Homes – Whole Interventions Demonstrator For People At Health And Social Risks"
  - "2.3.3 Intelligent Connectivity"

6. Conclusion

This report presented an approach for the definition and identification of key IoT standardisation gaps in several initiatives.

The used methodology and applied definitions in this report, are based on the AIOTI "High Priority Edge Computing Standardisation Gaps and Relevant SDOs, Release 1.0" report.

The AIOTI "IoT LSP Standard Framework Concepts R3" report and the EUOS "Landscape of Internet of Things (IoT) Standards" report have been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives.

The key purpose of this report is to reflect a structured discussion within the AIOTI WG Standardisation and to provide consolidated technical elements as well as guidance and recommendations on identified IoT gaps.

In particular, Section 2 describes the research and standardisation key IoT challenges, Section 3 describes the identification and prioritisation of the AIOTI identified IoT challenges in standardisation gaps, Section 4 describes the gap analysis work in SDOs and Section 5 describes the standardisation gaps analysis and recommendations and includes the mapping of 670 SDOs specifications to the 37 IoT challenges identified by AIOTI and presented in Section 2. Based on this analysis it can be concluded that:

- the following IoT challenges, need more research before being standardised:
  - "2.2.1 Green machine learning for the IoT"
  - "2.2.7 IoT Swarms"
  - "2.3.2 IoT Edge and X-Continuum Paradigm"
  - "2.3.5 Heterogeneous Cognitive Edge IoT Mesh"
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - "2.1.5 Challenges reported in SHAPES: Smart and Healthy Ageing through People Engaging in Supportive Systems"
  - "2.1.7 Challenges reported in IM-TWIN: from Intrinsic Motivations to Transitional Wearable INtelligent companions for autism spectrum disorder"
  - "2.1.10 Challenges reported in ATLAS: Agricultural Interoperability and Analysis System"
  - "2.2.2 Software Containers at the Edge"
  - "2.2.4 Digital Twins – overall"
  - "2.2.5 Heterogeneous vocabularies and ontologies in Digital Twins"
  - "2.2.6 Quality of metadata in Digital Twins"
  - "2.3.1 IoT and Edge Computing Granularity"
  - "2.3.4 Energy-Efficient Intelligent IoT and Edge Computing Systems"
  - "2.3.6 IoT Digital Twins, Modelling and Simulation Environments"
  - "2.3.7 Internet of Things Senses"
  - "2.3.9 Federated Learning, Artificial Intelligence technologies and learning for edge IoT Systems"

- "2.3.10 Operating Systems and Orchestration Concepts for edge IoT Systems"
- "2.3.11 Dynamic Programming Tools and Environments for Decentralised and Distributed IoT Systems"
- "2.3.12 Heterogeneous Edge IoT Systems Integration"
- "2.3.13 Edge IoT sectorial and Cross-Sectorial Open Platforms"

- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
  - "2.1.8 Challenges reported in GATEKEEPER: Smart Living Homes – Whole Interventions Demonstrator For People At Health And Social Risks"
  - "2.3.3 Intelligent Connectivity"

Annex I Template used for IoT research/standardisation requirement

Please fill in the yellow field

X. Title of IoT research/standardisation requirement

<<Title>>

X.1 Description of IoT research/standardisation requirement

- Provide motivation of having this edge computing research/standardisation requirement

  << Please fill in here >>
- Provide the description of the requirement

  << Please fill in here >>
- Type of Requirement, see explanation and examples of functional and non-functional requirements, below)

  << Please fill in here >>
  - These requirements can be split in:
    - Functional requirements

      (to possibly consider them – but not limited to – with respect to the identified functions/capabilities)
    - Non-functional requirements

  Functional Requirement (Examples)

  - Real-time communication with the stakeholders in case of emergency (Latency, jitter, etc.)
  - Reliable communication between the stakeholders
  - Scalable communication between systems to interconnects different critical infrastructures
  - Standard-based communication between critical infrastructure to align emergency information exchange with new and legacy systems

  Non-Functional Requirement (Examples)

  - Performance
  - Flexibility
  - Scalability
  - Interoperability
  - Reliability
  - Safety
  - Security and privacy
  - Trust
  - Secure communication between the emergency bodies due to the information nature
  - Interoperability between communication protocols (linked also with the possibility to use standard communication protocols between the systems)

X.2 Source

- Provide reference to project, SDO, alliance, published documents, etc.
- If requirement coming from an SDO/Alliance/OSS, please provide details, such as:
    - Group, e.g., WG/TC/SG
    - Work Item
    - Name of Specification
    - Other relevant information

<< << Please fill in here - Reference, URL, etc.>>

X.3 Application/Industry domain:

- Application/Industry domain (see explanation below):

  << Please fill in here ->>
    - Horizontal, Health, Mobility, Energy, Buildings, Agriculture, Manufacturing, Urban Society, etc.

Annex II Editors and Contributors to this Deliverable

The document was written by several participants of the AIOTI WG Standardisation.

Editors:

- Georgios Karagiannis, Huawei
- Axel Rennoch, Fraunhofer

Reviewer:

- Damir Filipovic, AIOTI Secretary General

Authors and key contributors:

Name	Company/Organisation
Nikolaos Giannakakos	Unisystems
Damir Filipovic	AIOTI Secretary General
Sascha Hackel	Fraunhofer FOKUS
Asbjørn Hovstø	Hafenstrom AS, Norway
Georgios Karagiannis	Huawei
Vasileios Karagiannis	Austrian Institute of Technology (AIT)
Artur Krukowski	RFSAT
Antonio Kung	Trialog
Zbigniew Kopertowski	Orange
Ana Lavinia Petrache	BEIA Consult
Dave Raggett	W3C
Axel Rennoch	Fraunhofer FOKUS
Jorgo Risto	BEIA Consult
Mari-Anais Sachian	BEIA Consult
Philippe Sayegh	Verses
Erwin Schoitsch	Austrian Institute of Technology (AIT), Austria
Orfeas Voutyras	Institute of Communication and Computer Systems (ICCS)/ National Technical University of Athens (NTUA)

Acknowledgements

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT and Edge Computing ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT and Edge Computing Innovation in society. AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT and Edge Computing ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies.