Alliance for Internet of Things Innovation

High Priority Edge Computing Standardisation Gaps and Relevant SDOs

AIOTI WG Standardisation

1 April 2022

Executive Summary

This report introduces an approach for the definition and identification of key edge computing and/or combination of IoT/IIoT, edge computing and cloud computing gaps in several initiatives. Based on the prioritisation of these gaps, the deliverable starts to address the work done within the relevant SDOs that need to cooperate in order to solve these gaps.

In the context of AIOTI, the synergy and integration of IoT/IIoT and edge computing, is considered to be a part of the paradigm shift from centralised solutions to decentralised and distributed computing architectures, in which information processing is located close to the edge, where "things" (e.g. sensors/actuators, devices, machines and humans) produce and utilise that information, knowledge and related experience.

The purpose of this document is to reflect a structured discussion within the AIOTI WG Standardisation community and to provide consolidated technical elements as well as guidance and recommendations.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table of Contents

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table of Figures

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

List of Tables

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

1 Goal and motivation

This report introduces an approach for the definition and identification of key edge computing and/or combination of IoT/IIoT, edge computing and cloud computing standardisation gaps in several initiatives.

There are several definitions on edge computing. In particular, several standards developing organization (SDO) and industry associations have provided definitions of edge and fog computing, see as well [IETF-T2TRG]:

- ISO defines the term edge computing as a "form of distributed computing in which significant processing and data storage takes place on nodes which are at the edge of the network" [Edge-ISO].
- ETSI focuses and defines multi-access edge computing as a "system which provides an IT service environment and cloud-computing capabilities at the edge of an access network which contains one or more type of access technology, and in close proximity to its users" [Edge-ETSI_MEC].
- The Industrial Internet Consortium defines fog computing (which is similar to edge computing) as "a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum" [Edge-OpenFog].

In the context of AIOTI [AIOTI-IoT-Edge-Computing] the synergy and integration of IoT/IIoT and edge computing, is considered to be a part of the paradigm shift from centralised solutions to decentralised and distributed computing architectures, in which information processing is located close to the edge, where “things” (e.g. sensors/actuators, devices, machines and humans) produce and utilise that information, knowledge and related experience.

There are now several Edge Computing Standards Landscape available, see [AIOTI-edge-landscape] that have identified a number of standards that are available, i.e. which have reached a stable stage (Technical standard (TS) or TR, etc.) in a Standards Developing Organisation or industrial consortia, and can be used for the work and developments of the edge computing community.

However, the possibility to develop large-scale interoperable solutions within this edge computing 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 edge computing community (and more widely if needed).

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

The used methodology and applied definitions in this report, are taken from [AIOTI-IoT-Gaps].

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

Annex IV includes the mapping of SDOs specifications to the AIOTI identified edge computing challenges.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2 Possible edge computing challenges

This section introduces edge computing research and standardisation challenges that have been identified either from the edge computing activities of the AIOTI members or from literature studies. The goal of this edge computing challenges collection is to form the basis of identifying the edge computing 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 III.

2.1 Data interoperability, Security and Privacy, decentralised IoT/IIoT computing architectures and real-time processing research challenges

2.1.1 Description of research challenges

- Data interoperability, including semantic interoperability, remains a key challenge in the IoT and edge arena. Research should explore a pragmatic approach, where semi-automatic interoperability is achieved through limited human interaction. With the increasing platform-to-platform communication, it will also require solutions for IoT-driven processes interoperability.
- Future proof security and trust. Research should focus on 'intelligent' approaches to security and privacy, i.e. on the ability to 'learn' new attack patterns and derive counter solution autonomously. Solutions linked to ensuring trust and traceability of IoT data should scale, coping with requirements posed by real-time data scenarios in several IoT market segments.
- Privacy by design: to understand and forecast the impact of IoT and edge computing solutions on society, a multidisciplinary approach is needed embracing legal, sociological, ethical and privacy by design research in relation to the adoption of IoT and connected technologies, such as Artificial Intelligence.
- Data trustworthy from the point of interoperability and security, in terms of maintaining the provenance and nature of the information across platforms. This will be the base for future intelligent and self-adaptive systems.
- A new operating system at the edge for decentralised IoT/IIoT computing architectures and real-time processing
- Edge computing has triggered a paradigm shift in cloud computing
    - Orchestrating resources to form a "computing continuum"

2.1.2 Source

The above described research challenges are listed in the AIOTI position paper "Strategic Foresight Through Digital Leadership - IoT and Edge Computing Convergence" prepared by the AIOTI WG Research and Partnerships [AIOTI-IoT-Edge-Computing].

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.1.3 Application/Industry domain

Those research challenges applied as well to all possible vertical industry domains and as well to horizontal industrial domains.

2.2 Deep Edge resources, Edge, Mobile Edge Computing and Processing research challenges

2.2.1 Description of research challenges

Deep edge resources:

Deep edge, with its IoT as well as end-user or vertical industry devices, is becoming part of the common resource pool, provided as a non-decomposable set of resources by some edge entity, such as an end-user, industrial site owner, or a building owner. Future research includes:

- Address edge-specific constraints through suitable scheduling mechanisms that take those constraints into account, while relying on edge-specific control agents enabling the enforcement of the policies underlying the scheduling solutions
- Focus into novel programming models and (e.g., policy) languages that not only support all of these services, applications and deployments but also cater to the expected dynamics of the market itself.
- Provide new IoT device management techniques that are adapted to the evolving distributed architectures for IoT systems based on an open device management ecosystem

Edge, Mobile Edge Computing and Processing:

5G and beyond-mobile networks will enable unprecedented density of connected devices, many of which will create tremendous amounts of data. As an example, an autonomous car is expected to create data at an estimated rate of 5 terabytes per hour. Transferring these raw data to a central cloud for processing is not feasible for (at least) three reasons:

- **Bandwidth:** If the device is connected via LPWAN (e.g. NB-IoT with an uplink peak data rate of 159 kbit/s[1]) the bandwidth is limited and not suitable to transfer large amount of data (e.g. multimedia data).
- **Network Congestion:** With a culminated capacity of the last mile exceeding the capacity of the core network by two orders of magnitude, the core is becoming a bottleneck for huge amounts of data to be transferred to the cloud data centers while at the edge there is sufficient capacity available.[2]
- **Latency:** There are applications where latencies beyond the range of hundreds of milliseconds are not acceptable. Multiplayer online gaming is an example which is a driving force in edge

[1] See https://en.wikipedia.org/wiki/Narrowband_IoT

[2] See e.g. https://blogs.akamai.com/kr/2018_Edge_Korea_TomLeighton.pdf or https://www.akamai.com/de/de/about/events/edge-highlights.jsp#edgeworld-2019-tom-leighton-through-the-clouds-a-view-from-the-edge (at ~ 13:00 minutes)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

development (gamers are paying for latency!). In safety relevant use cases it often is not just a question of “user experience” but a matter of life or death.

Storing (or buffering) raw data locally is often not an alternative either, since devices do not have sufficient storage capacity or storage is just too expensive. Taking the example of an autonomous car above and with a current storage price of roughly 20 € per Terabyte, to store the raw data of that car would cost 100 € per hour – even without redundancy.

Those restrictions can be overcome by taking Content Delivery Network (CDN) technologies a step further and process data in or near the device by which it is being created (e.g. in a mobile phone or in a surveillance camera). The processing can result in immediate action of an actuator in response to sensor inputs or in condensing data before storing them or sending them to a central cloud. Artificial intelligence comes into play to identify relevant data patterns, but also as a means of network resource optimization and network security. Beyond 5G networks are expected to come with AI already embedded in the network functions[3].

[3] See e.g. https://ieeexplore.ieee.org/document/9430853

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

When data are being condensed for transfer or storage this must be done in a manner that potentially valuable information is being retained. Regulatory requirements may also be relevant for data retention (e.g. in autonomous driving). Such handling of data will be important design decisions when developing edge applications.

Developers are facing competing frameworks to make their apps edge-aware – some of which are provided by large cloud providers (e.g. AWS Greengrass, Azure IoT Edge). To avoid another lock-in, users might consider open source alternatives like ETSI MEC[4], LF Edge[5], Open Edge Computing[6] or OpenStack[7] (just to name a few).

Developers will also have to deal with different levels of edge computing complexity. One dimension of complexity is the edge-awareness of the application. In the case of edge-unaware applications, developers do not have to deal with the edge specifics and the network is responsible to handle client requests transparently in a manner that those are handled by the server instance with optimum network proximity (just like in today's CDNs). On the other hand, edge-aware applications will have to make use of the available edge-resources by exploiting the specific APIs that are exposed by the edge implementation.

A second dimension of complexity is mobility. When the device is mobile, this is uncritical as long as the edge application is running on the device itself ('device edge'). But if for example the processing is done at the base station ('far edge'), the application context needs to be moved from one base station to another as the user is moving through the mobile network. If roaming between different MNOs comes into play, things even get more complex.

As a side effect, to not send data to a central cloud can be seen as a gain in privacy. However, this presupposes that data security is guaranteed in the edge. This, in turn, is not a trivial task, because the attack surface increases enormously and the remote management of the high number of edge devices is a challenge and requires new methods and standards.

Availability can be another benefit of edge computing. Given the edge applications are programmed accordingly they can provide business continuity in situations of loss of network connectivity or downtimes (planned or unplanned) of the cloud data center.

While edge computing will certainly support the goals of the digital transition, we should not forget about the other side of the medal: sustainability and the green transition. On the positive side of the energy equation, edge computing reduces energy-hungry data transfers.

[4] https://forge.etsi.org/rep/mec
[5] https://www.lfedge.org/
[6] https://www.openedgecomputing.org/
[7] https://www.openstack.org/use-cases/edge-computing

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

On the downside, the intelligence and processing power required at the edge comes at a (energy) cost. Research should be undertaken on how the net carbon footprint of edge computing could be minimized. When the device is energy constrained (e.g. battery driven) other options like energy harvesting could be taken into consideration.

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 the use of multi-access edge computing:

- built-in end-to-end distributed security, trustworthiness and privacy issues in edge computing for IoT are important, as well as federation and cross-platform service supply for IoT

2.2.2 Source

The above described research challenges are listed in [Networld2020-SRIA] and the AIOTI " IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges" [AIOTI-BY5G].

2.2.3 Application/Industry domain

Those research challenges applied as well to all possible vertical industry domains and as well to horizontal industrial domains.

2.3 User Trust, Pricing models and Low cost fault tolerant systems, Service Discovery, Service Delivery and Mobility, Collaborations between Heterogeneous Edge Computing Systems research challenges

2.3.1 Description of research challenges

- **Users Trust:** on Edge computing and on computing continuum systems: the success of edge computing and computing continuum is related and linked to trust that is regarded as one of the most important factors for the acceptance and adoption of these Edge computing and computing continuum systems by consumers and users
- **Dynamic and Agile Pricing Models**: the rapid increase of the edge computing applications and services opens the need for dynamic pricing and market places
- **Service Discovery, Service Delivery and Mobility:** distributed and federated edge computing systems require service discovery and delivery support, in particular, for scenarios where multiple mobile devices are used that require services simultaneously and uninterruptedly

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

- **Collaborations between Heterogeneous Edge Computing Systems**: due to the fact that the ecosystem of Edge computing systems consists of a collection of different processing/computing points, i.e., cloud data centre, edge computing systems and end devices, and different underlying communication infrastructures, makes the collaboration between such systems a challenging task
- **Low-Cost Fault-tolerant deployment models**: Deployment models that are Fault-tolerant are important because they ensure the continuous operation of any system in the event of failure with little or no human involvement.

2.3.2 Source

The above described research challenges are listed in [ZaAh19].

2.3.3 Application/Industry domain

Those research challenges applied as well to all possible vertical industry domains and as well to horizontal industrial domains.

2.4 Digital for Green research challenges

2.4.1 Description of research challenges

1. Define and evaluate approaches on increasing energy efficiency in communication infrastructures applied in IoT and edge computing solutions;
2. Develop and evaluate IoT and edge computing solutions that support monitoring and controlling energy and carbon footprint usage in EU Green Deal areas:
   - Climate action
   - Clean energy
   - Sustainable industry
   - Building and renovating
   - Sustainable mobility
   - Biodiversity
   - From farm to fork
   - Eliminating pollution;
3. Develop and evaluate security and privacy by design approaches 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;
4. Develop (or reuse) and evaluate interfaces, data models and ontologies required by IoT and edge computing solutions that support monitoring and controlling energy and carbon footprint usage in EU Green Deal areas;
5. More research and innovation activities on standards or guidelines are required to define the Carbon footprint of ICT installations – in use but also incl. material production, assembling, recycling (LCA - Life Cycle Assessment);
6. R&I activities on “green AI”, developing strategies and implementation concepts;
7. R&I activities for reference designs and benchmark platforms;

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

8. R&I activities on sustainable power supplies, employing alternative energy sources for small devices (energy harvesting) and energy storage devices (batteries, capacitors) with low carbon footprint;

9. R&I activities on energy-efficient wireless protocols targeting massive IoT applications (M-IoT, NB-IoT, 5G/6G).

2.4.2 Source

The above described research challenges are listed in the AIOTI Digital for Green vision report prepared by the AIOTI Digital for Green Interest Group [AIOTI_DfG_2021].

2.4.3 Application/Industry domain

Those research challenges applied as well to all possible vertical industry domains and as well to horizontal industrial domains.

2.5 Digital for Green standardisation challenges

2.5.1 Description of standardisation challenges

1. 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
2. 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
3. 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

2.5.2 Source

The above described standardisation challenges are listed in the AIOTI Digital for Green vision report prepared by the AIOTI Digital for Green Interest Group [AIOTI_DfG_2021].

2.5.3 Application/Industry domain

Those standardisation challenges applied as well to horizontal industrial domains and as well to all possible vertical industry domains.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.6 IoT and edge computing can support the Environmental, Social and Governance (ESG) monitoring research challenges

2.6.1 Description of research challenges

The Environmental, Social, and Corporate Governance (ESG) can be defined as an evaluation of a company's collective conscientiousness for social and environmental factors.

The ESG regulations in EU, such as the Corporate Sustainability Reporting Directive and the Sustainable Finance Disclosure Regulation (SFDR) are impacting the way companies deploy and do business, in tracking the trends, the costs and the forward outlook, where Environmental, Social, and Corporate Governance topics play a significant role.

ESG is usually seen as a score that is compiled from the data that is collected from surrounding specific metrics related to intangible assets within the enterprise and could be considered a form of corporate social credit score.

In this context, a challenge is to explore how the rapid growth in capabilities of other new technologies such as AI, Machine Learning, HPC, AR/VR, drones, robotics and IoT are accelerating the pursuance, monitoring and performance of ESG.

The challenge is to use digital technology, such as IoT and edge computing to assist the collection of surrounding specific metrics and data, required by ESG, which when compared with traditional financial accounting data is non-standard and incomplete.

These requirements imposed by this challenge can be divided in:

- Functional requirements
    - What infrastructure shall be in place to ensure the underlying technology, metrics and data are available and accessible?
        - ESG Data Taxonomy: Define a robust, comparable and reliable ESG data taxonomy. As per European Banking Federation: “Therefore, ensuring availability of high quality and comparable ESG data should be regarded as an EU strategic infrastructure project to meet the EU sustainability objectives both under the Action Plan on Sustainable Finance and the EU Green Deal”
    - What are the underlying connectivity requirements?: The overwhelming majority of IoT connections are likely to require some form of connectivity (cellular, WiFi, optical, cable, etc.) in the last mile, whether directly from terminal devices themselves or from aggregation hubs.
        - ESG related regulations to consider that IoT sensors, e.g., Smart meters, can be used as remote reading capabilities collectors from assets
        - Define Technology -driven ESG ratings as they are becoming increasingly influential, since they offer financial service institutions the ability to compare the ESG performance of companies, which is currently complex due to the low degree of standardised methods for ESG metric and data collection & monitoring.
- Non-functional requirements

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

- Data-Security and privacy: These requirements are significant due to the fact that the ESG data and metrics that are collected and monitored can be considered to be sensitive and personal data related, where typically compliance to GDPR is required.
- Avoid lock in and fragmentation and support of Interoperability: A large number of players in the IoT ecosystem (e.g., over 400 IoT platform providers) are driving the development and deployment of their own IoT platforms and solutions on supporting ESG. This can lead to lock in and fragmentation. Deploying Interoperable IoT and edge computing platforms and solutions for this purpose, can avoid the fragmentation challenge. This requires the use of standardized interfaces, protocols, data models and ontologies to support the collection and monitoring of ESG related metrics and data. Interoperability can as well enable cross-industry solutions to unlock mutual benefits and enable new monetization models.

2.6.2 Source

- World Economic Forum report IoT Guidelines For Sustainability
- Sustainable Finance Working Group (SFWG) - **TECH-DRIVEN ESG PRACTICES** https://g20sfwg.org/wp-content/uploads/2021/08/2021-FC4s-GDFA-Tech-driven-ESG-Practices..pdf
- The European Banking Federation, together with five other financial industry associations, is calling for the European Commission to establish a common ESG data register in the European Union https://www.ebf.eu/ebf-media-centre/a-centralized-register-for-esg-data-in-eujoint-letter/

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.6.3 Application/Industry domain

ESG metrics and rating will be useful for:

- European Commission
- Country Governments
- Private Industrial Sector (horizontal and all vertical industry domains)
- The financial sector

2.7 Explainable AI using human argumentation research challenges

2.7.1 Description of research challenges

There are many opportunities for applying AI algorithms that are derived from applying machine learning (e.g., Deep Learning with multi-layer artificial neural networks). However, trust in such algorithms depends on being able to provide meaningful explanations for the output of the algorithms. Here, the key is to make the explanations understandable and satisfying to people. In other words, this technique use the forms of argumentation that people are familiar with, something that has been the subject of study since Ancient Greece.

It is unfortunate that algorithms derived from machine learning inevitably have problems with a multitude of edge cases due to limitations in the training data. Humans approach such edge cases by reasoning with respect to additional knowledge. AI algorithms are in effect compiled knowledge (System 1), and can be contrasted with deliberative reasoning (System 2), see Daniel Kahneman's "Thinking, Fast and Slow".

To provide human-meaningful explanations, we need human-like reasoning. Accordingly, we need to see more research into a wide variety of different forms of reasoning, including logical deduction and ontological entailment, induction, abduction, spatial and temporal reasoning, causal reasoning, plausible reasoning with imperfect knowledge, qualitative reasoning, fuzzy reasoning, analogical reasoning and so forth. This spans approaches based on formal semantics, approaches based on probability theory, as well as informal approaches that mimic human reasoning.

This is not only relevant to Deep Learning, as symbolic knowledge (e.g., as expressed in ontologies) also needs to be able to provide deeper explanations when queried by users. This could relate to examples that underlie the ontology (e.g., exemplars of taxonomic categories), as well as to other kinds of knowledge. When the existing ontology proves to be inadequate, it will need to be dynamically updated to take into account a more nuanced model of the world.

Common sense is needed to support natural language interaction and everyday reasoning. According to Jim Taylor, it can be defined as sound judgment derived from experience rather than study. In other words, it relies on general knowledge rather than specialised knowledge.

Humans are not a gold standard, as many people exhibit poor judgement, e.g., purchasing things they cannot afford, smoking, eating junk food, holding irrational beliefs contrary to evidence as well as blatant prejudices against people from different backgrounds. Machine common sense needs to be assessed from a practical perspective, including adherence to ethical principles and standards of normative behaviour.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

How can we codify such principles and standards? Is it possible to include ethical principles and standards of normative behaviour as part of common sense and to attend to them as part of metacognition, akin to an inner voice for cognitive agents?

2.7.2 Source

According to DARPA:

> *"The absence of common sense prevents intelligent systems from understanding their world, behaving reasonably in unforeseen situations, communicating naturally with people, and learning from new experiences. Its absence is considered the most significant barrier between the narrowly focused AI applications of today and the more general, human-like AI systems hoped for in the future."*

Europe needs to invest in research along similar lines to DARPA's Machine Common Sense Program, which is investigating two broad complementary approaches: mimicking how children acquire everyday knowledge, and the potential for mining knowledge from across the Web.

See: https://www.darpa.mil/program/machine-common-sense

2.7.3 Application/Industry domain

Those research challenges are applicable horizontally and as well to most of the vertical industry domains (e.g., manufacturing, energy, health, agrifoord, smart cities, buildings, mobility).

2.8 Digital Twin research challenges

2.8.1 Description of research challenges

This section lists perceived challenges associated to Digital Twin implementation in large scale/productive environments. It also identified enabling technologies suitable to ease solution and addressing of such challenges.

Following topics are challenges to implementation due to implied data volumes and required computing-intensive function. For such reason, edge computing represent possible infrastructural and architectural solution to such issues.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

The following challenges:

A. **Data management**: Intended as interoperability, scalability of heterogeneous data repositories, that must be reliable, maintainable and available in all conditions. Big amount of data needs to be managed potentially for long time. Multiple Data storage solutions (including relational and not-relational databases are nowadays available)
B. **Data privacy and security**: Data needs to be characterized by integrity, confidentiality, availability and non-repudiation.
C. **Data quality**: Not consistent data, redundant data, wrong syntax data need to be filtered out. More, correlation and semantic annotation are provided to enrich knowledge and to allow epistemological analysis of collected information for potential utilization for knowledge management (e.g. through ML or AI approaches).

Can be addressed by the following enabling technologies:

A. **Digital platforms**: Edge distributed infrastructures and architectures can provide appropriate service levels for the envisaged application. Specifically edge processing platforms can tune data quantities to be transferred.
B. **Cryptography** and blockchain technologies: In rode rot ensure data privacy and security, multiple solution are already available through cryptography applications (e.g. PKI Public Key Infrastructure), novel distributed ledger technologies can be evaluated for limited information quantities sharing, in parallel with traditional encryption solutions.
C. **Big data technologies**: These enabling technologies encompass Analytics and Data Mining tools.

At the present the above mentioned enabling technologies are available and stable, no specific obstacle is preventing their implementation and deployment. Major issues are related with business owners to share information on distributed platforms and availability of skilled resources able to design and implement infrastructures, architectures and applications. On the other hand, edge computing technologies can overcome issues originated by bandwidth issues and potential latency. Below, additional challenges and requirements are listed:

1. **Real-time communication of data and latency**: Data compression, communication technologies like 5G and internet of things technologies
2. **Physical realism and future projections**: Sensor technologies, high fidelity physics-based simulators, data-driven models
3. **Transparency and interpretability**: Hybrid analysis and modelling, explainable artificial intelligence
4. **Large scale computation**: Computational infrastructure, edge, fog and cloud computing
5. **Interaction with physical asset**: Human machine interface, natural language processing, vi-sualization augmented reality and virtual reality

2.8.2 Source

The above described research challenges are derived from an IEEE Access scientific paper [RaSa20].

2.8.3 Application/Industry domain

Those research challenges are applicable horizontally and as well to most of the vertical industry domains (e.g., manufacturing, energy, health, agrifoord, smart cities, buildings, mobility).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.9 From Digital Twins to Data Spaces for Knowledge Graphs standardisation challenge

2.9.1 Description of standardisation challenges

Digital Twins have proven themselves as a valuable means for abstracting away from physical devices, offering affordances for live access to devices, simulations of device behaviour for planning, and digital memories for instances and classes of devices throughout their lifecycle. Knowledge Graphs provide a powerful generalisation for digital twins in respect to declarative descriptions of devices and the context in which they are situated, as well as associated services and how to invoke them. A knowledge graph can contain data, models, meta-models and other metadata including provenance, and information relating to privacy and confidentiality along with policies and agreements between service providers and consumers. Data Spaces are a framework for ecosystems of digital value chains involving data owners, data intermediaries and data consumers. Data spaces for public/private federated knowledge graphs provide a natural extension from digital twins to digital value chains that span the edge to cloud continuum, and which preserve data sovereignty through technical and contractual means. Access to restricted information and services is subject to authorisation based upon the user's identity and role. Standards are needed to avoid fragmentation that impedes interoperability.

Description of the requirement:

Standards are needed in a number of areas:

- Graph metamodel for vertices, edges and properties as the basis for porting graphs across different databases, e.g., RDF quad stores and Property Graphs
- Ontologies for affordances, data schemas, domain semantics, privacy, security, causal models, material models for recycling, and information for repairs in support of the circular economy
- Framework for data integration across different ontologies given that it is unrealistic to expect everyone to use the same ontologies given differences in requirements and perspectives
- Coordination of distributed processing across data owners and intermediaries with data pipelines and workflows, e.g., for privacy preserving federated learning, event detection, search and data joins, where multiple data owners and intermediaries are involved
- Framework for facilitating trust involving digitally signed attestations by third parties and immutable logs for audit trails and compliance testing, with ontologies for access control and data sharing policies, as well as smart contracts for agreements.

Types of Requirements:

The above are a mix of functional and non-functional requirements. However, the details will depend on further study. This is an opportunity for Horizon Europe, for SDO's and for industry alliances.

2.9.2 Source

A number of different SDOs are already working on related standards, here are just a few:

- W3C: Web of Things, RDF-star, decentralized identifiers, signed graphs, etc.
- ETSI: ISG CIM: NGSI-LD
- IEEE: P2874 Spatial Web WG

We could also cite some relevant European projects, e.g., Horizon 2020 TERMINET, as just one example.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.9.3 Application/Industry domain

Open standards for data spaces for public/private federated (and distributed) knowledge graphs across the edge-cloud continuum would be applicable across many domains. Some standards would, however, be targeted at specific domains, e.g., for specialised ontologies.

2.10 Quality assurance for IoT & Edge computing infrastructures and applications standardisation challenge

2.10.1 Description of standardisation challenges

The introduction and/or use of any edge computing communication protocol and configuration requires high quality and confidence in the implementations. This includes the application of various types of test, e.g., conformance, interoperability and robustness/security test scenarios. From the viewpoint of a standardization committee testing methods and techniques should follow standardized approaches. This has been recognized in the context of mobile communication. Since many years certification has been based on standardized test catalogues and test implementations using test descriptions and implementations defined with ETSI languages TDL and TTCN-3.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Types of Requirements:

Edge computing technologies and standards should be accompanied by corresponding unique definitions of test scenarios and catalogues using standardized and well-known specification techniques. This applies for any test activities, including functional conformance, interoperability scenarios or non-functional testing types (like security or performance).

Upcoming infrastructures and applications are characterized by

- Distributed, heterogeneous architectures and interfaces (interoperability and security requirements, multiple vendor devices/platforms, domains specific applications, objects and functions, use cases, reusable test harness from different verticals)
- Management at the edge nodes (mobility of devices, Elasticity and fluctuation of data workload due to container/kubernetes pods etc., provisioning, orchestration and coordination of deterministic capabilities and SDN)
- Performance/resource restrictions at IoT layer (big number of devices, critical ultra-low latency in milliseconds (ms) for real-time applications, limited connectivity, power consumption and autonomy)

These challenges demand for application of several testing types, systematic test definitions and justified testbed and software architecture of test solutions.

2.10.2 Source

The ETSI committee on Methods for Testing and Specifications (TC MTS) has completed a first set of test specification standards addressing the IoT MQTT and CoAP protocols, and the foundational security IoT-Profile. These new standards fill the gaps for the quality assessment of some of the most relevant communication protocols and system requirements of today's industrial IoT systems using standardized testing techniques defined by ETSI. Please refer to ETSI: MTS Test specifications for IoT: https://www.etsi.org/standards/get-standards#page=1&TB=860&sort=3.

2.10.3 Application/Industry domain

Those standardisation challenges are applicable horizontally and as well to most of the vertical industry domains, such as manufacturing, energy, smart cities, health, agrifood, mobility. Samples include

- IoT devices in buildings supporting e.g. heating distribution/regulation, energy saving, air conditioning or simply maintenance of the infrastructure elements.
- Traffic supervision in urban areas supporting rush hour traffic regulation, precedence of emergency vehicles or management of parking space.

2.11 Multi Access Edge Computing (MEC) standardisation challenges

2.11.1 Description of standardisation challenges

Edge application management is an essential part of the edge computing environment, and ETSI ISG MEC has put a lot of efforts (research and standardization) in this area, which can provide a valuable input for further identifying the gaps and requirements.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Functional requirements:

- Requirements on the framework
  - Utilize the modern virtualized infrastructure to support edge computing
  - It should be possible to deploy edge computing applications using the same infrastructure as NFV based VNFs
  - Multiple access options should be supported, for example, fixed, mobile and wireless network, etc.
  - The edge computing system should be able to interact with the 5G core network
- Application lifecycle
  - In response to a request by the operator or an authorized third-party, the edge computing system should support management of the edge applications, including instantiation, termination, etc.
- Support of mobility
  - The edge computing system should maintain the connectivity between a UE and an application instance when the UE performs a handover.

Non-functional requirements:

- Application environment
  - It shall be possible to deploy MEC applications on different MEC hosts in a seamless manner, without a specific adaptation to the application.
  - The MEC system shall support distributed edge cloud deployments and in doing so horizontally and vertically distributed applications, where horizontal implies peer to peer connectivity of the application components and vertical implies hierarchical connectivity between different application components.
  - The edge computing system should provide a secure environment for running services.
  - The edge computing system should support collection of charging related information.

In addition, there are service requirements defined in ETSI MEC, relating to the platform essential functionalities (e.g. MEC services, connectivity, storage, traffic routing, DNS support and timing) and features (e.g. smart relocation, radio network information, location service, bandwidth manager, MEC federation, etc.).

2.11.2 Source

This requirement comes from the ETSI ISG MEC, Work Item: MEC 002, Name of Specification: Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements
Other relevant information is related to the introduction of ISG MEC and related reports/specifications, see: https://www.etsi.org/technologies/multi-access-edge-computing

2.11.3 Application/Industry domain

- Horizontal and targeting Mobility industry domain. However, can be applied as well in other vertical industry domains, such as: Health, Energy, Buildings, Agriculture, Manufacturing, Urban Society, etc.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.12 MEC Application instantiation in neighbouring MEC hosts

2.12.1 Description of standardisation challenges

There are multiple use-cases where the continuity of low-latency interactivity is required for a good user experience. As an example we can consider the following use case:

- An AR/VR gaming use-case, where processing is being offloaded to a MEC Server service, while having the low-latency enabling the necessary interactivity for such a use-case. When facing mobility, current standards make provisions for a re-scheduling by the orchestrator (MEO) such that the application will transition from a MEC host to a different one, closer to the current UE position.
- This process happens as a best-effort and in reaction to a latency increase after a RAN handover has already occurred.

Issue:

This latency increase and application transference from the state/data/VM from MEC host to MEC host is a process that will take at least some seconds and likely much longer. A period during which the user experience will suffer adversely.

As another use case example: A CDN/cache use-case that wants to optimize its storage usage elastically, optimizing the cached content in function of the users being serviced. This service wants to cache a certain user-specific content for servicing a mobile user.

Issue:

To guarantee that the user is always physically close to a MEC host with said content cached, it has to be cached either “everywhere”, which is a less efficient usage of resources, or upon a user transitioning to a different MEC host, there will be a data transfer period. Said period can be large, depending on the size of the data.

The ability to obtain the set of neighbouring MEC hosts to a particular MEC Host or UE, or the ability to instantiate services specifically in that set, in a new type of per-user “zoned deployment”. Ideally this functionality would integrate with the more recent efforts towards inter-MEC federation, and this set of hosts would cross MNO domains.

Standardisation challenge: Interoperability: standardisation work across MNO domains in inter-MEC federation scenarios is needed.

Functional requirements:

- Instantiate an application not only on the MEC host closest to an user, but the surrounding ones as well
- In case of an application that runs per MEC host, in all hosts, be able to identify the instances that are closest to an user and all the neighbouring ones

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.12.2 Source

This requirement comes from research being done by Ubiwhere in the R&D project SNOB-5G (https://snob-5g.com/), which Ubiwhere is coordinating.

2.12.3 Application/Industry domain

Application/Industry domain: Horizontal (targeting Smart Cities)

2.13 Horizon 2020 NGIoT Assist-IoT research and standardisation challenges

2.13.1 Description of research/standardisation challenges

Next Generation Internet of Things field is urgently requiring the creation of a robust, formal, valid, useful and standardized architecture to build deployments upon. Several initiatives are detected, as well as classic concepts of architecture definition are varyingly meeting requirements. However, the blueprint is yet to come.

In the early deployment stages, IoT applications were simple, and the number of IoT elements involved were small, so that IoT developers typically shared the burden of contributing to and maintaining the codebase. As the Next Generation Internet of Things (NGIoT) grows, new features shall be added to the applications, leading to (i) an increase in the operational workload, and (ii) a necessary horizontal and/or vertical scaling, requiring that more servers host the application. The complexity of the NGIoT applications is growing steadily, and hundreds of tests shall be carried out to guarantee that any minimum change made does not compromise the integrity of the existing code.

ASSIST-IoT architecture and solutions are based on: (i) the use of microservices, (ii) their instantiation in containers, (iii) their grouping into “enablers”, (iv) and their further orchestration using Kubernetes technology.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

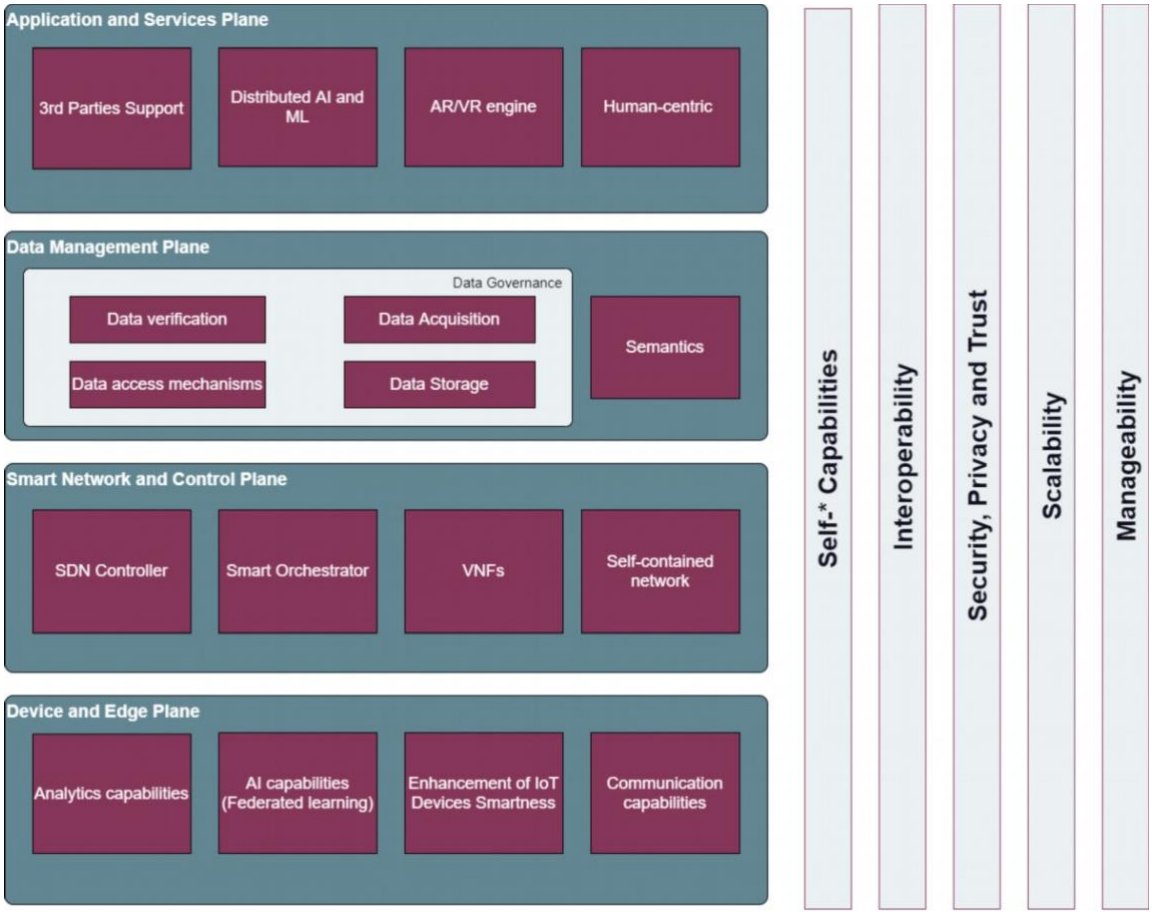

Figure 1: **ASSIST-IoT Functional Architecture**

Horizontal Planes

A high-level Functional View of the ASSIST-IoT is presented on Figure 1. The Planes of the ASSIST-IoT architecture are as follows:

Device and Edge plane describes the collection of functions that can be logically appointed to physical components of IoT, including, but not limited to, smart devices, sensors and actuators, wearables, edge nodes, as well as network hardware, such as hubs, switches and routers. Note that this plane, like all the others, represents a Functional View. So even though e.g., functions related to self-contained network could be naturally associated with network devices, there is a group of functions that can be identified and separated into functional blocks that belong squarely on the Device and Edge plane. The aforementioned functions include any physical connectivity and interfaces (e.g., Ethernet), low-level security functions (e.g., firewalling). This plane directly interfaces the hardware capable of executing specific functions designed on higher planes.

The Device and Edge plane is the logical abstraction of ASSIST-IoT for the functionalities that will interface with sensors and actuators along with network functions. The innovations to be carried out in the architecture of ASSIST-IoT associated with this plane will fall under four different functional blocks:

(i) Analytics capabilities,

(ii) AI capabilities (federated learning),

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

(iii) enhancement of IoT devices smartness and

(iv) communication capabilities.

Smart Network and Control plane manages virtual and wireless aspects of network connectivity. The key functions handled on this plane are encompassed by technologies that deliver software-related and virtualised networks, such as SDN (SD-WAN), NFV, MANO, and anything related to virtualised or self-contained networking. Any direct and logical connection in the communication infrastructure is provided on this plane. The functions on this plane follow the access-network-agnostic approach, in which the network connections are highly flexible. Features, such as dynamic configuration, routing and addressing, and high-level intelligent firewalling help deliver the required flexibility.

Data Management plane handles all functions related to a virtual shared data ecosystem, in which data are acquired, delivered and processed to provide key data-related functions. Those include data interoperability, provenance, fusion and aggregation, but also content-independent functions, such as resilience (e.g., redundancy). Security functions for access grants and trust management also belong to this plane. Moreover, this plane is empowered by semantics and might be supported by judiciously selected DLT.

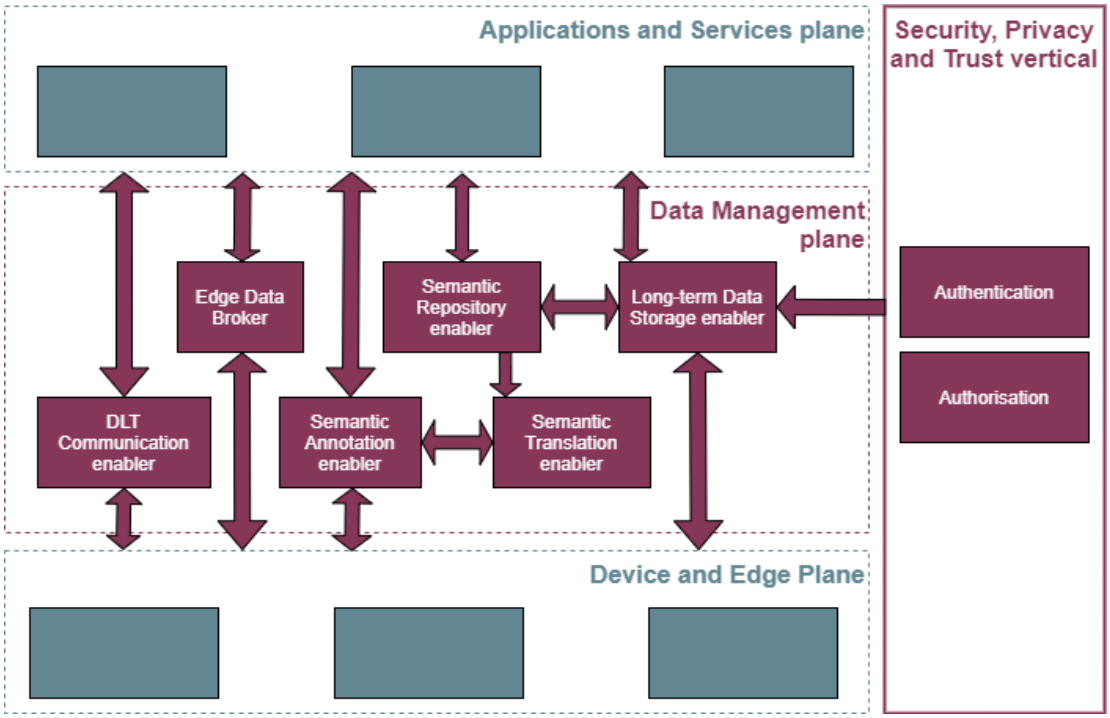

Figure 2: ASSIST-IoT Data Management plane draft interconnections diagram

Application and Services plane crowns the Functional View with end-user and administrative functions and services. It delivers a layer of abstraction that manages functions offered by lower planes. Moreover, it combines them to provide synergistic value for the whole system. Its functions, aided by the Verticals, aim to offer a unified point of access, and provide system-wide intelligence and configuration capabilities. Because of the high level of abstraction, this plane enables the creation of advanced and intelligent applications, including configurable autonomous systems, that benefit from the lower planes, and their interconnection.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Vertical functionalities

The following Verticals have been identified in ASSIST-IoT: (i) Self-* capabilities, (ii) Interoperability, (iii) Security, Privacy and Trust, (iv) Scalability and (v) Manageability.

In each vertical set of required functionalities and capabilities were specified:

1) **Self-*System** is a system that is autonomous or semi-autonomous alongside some dimension. Autonomous in this context means that there is no need for constant overview from human operators. Required Self-* features are:

    i) **Self-diagnosis:** is a capability of a system to detect erring behavior within itself,

    ii) **Self-healing: -** building on top of self-diagnosis, ability to fix faulty elements ability,

    iii) **Self-aware:** when it is able to interpret its own state based on some internal domain knowledge,

    iv) **Self-organization:** is the ability of a system to adapt to changing conditions and various problems that the system faces in a given moment,

    v) **Self-configuration:** allows the system to autonomously configure and reconfigure itself and its resources when faced with changing environments to maintain its functionalities.

2) **Interoperability:** is the ability of equipment from different manufacturers (or different systems) to communicate together on the same infrastructure (same system), or on another while roaming. Interoperability will be undertaken at three levels:

    i) **Technical interoperability: –** means the ability of two or more information and communication technology applications, to accept data from each other and perform a given task in an appropriate and satisfactory manner without the need for extra operator intervention.

    ii) **Syntactic interoperability:** – allows two or more systems to communicate and exchange data in case that the interface and programming languages are different (e.g. by using of a standardisation of the communication between a software client and a server).

    iii) **Semantic interoperability:** – is the highest level of interoperability which denotes the ability of different applications/artefacts/systems/… to understand exchanged data in a similar way, implying a precise and unambiguous meaning of the exchanged information.

3) **Security, Privacy and Trust:** will provide the following functionalities along the ASSIST-IoT architecture:

    i) Authorised registration of the IoT devices joining the network.

    ii) Security, privacy, and trust on access and when sharing data for multiple domains.

    iii) Security and privacy for data storage.

    iv) Security monitoring and incident response to avoid cyberthreats.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

In ASSIST-IoT, privacy and trust per design will be addressed by the introduction of DLT-related enablers. DLT is a novel technology that has numerous uses. DLT is known for the opportunity to decentralise procedures, resilience to changes, anonymity, and immutability to data. The implementation of carefully selected DLT mechanisms within ASSIST-IoT will be tackled from various viewpoints, both purely technological (for the architecture) and dependent on the use cases.

4) **Scalability:** vertical in ASSIST-IoT is a property of the system that is present due to (i) the design principles followed, (ii) the container orchestration technologies leveraged, and (iii) the functionalities covered by the Planes and other verticals of the architecture. From ASSIST-IoT, and following OpenFog RA, Scalability will involve three main dimensions:

    i) software,

    ii) hardware and

    iii) communication capabilities.

5) **Manageability:** in ASSIST-IoT refers to managing nodes and every configuration option over any enabler running in a particular deployment of the architecture. ASSIST-IoT will consider the introduction of certain components that involve autonomous decision making (see previous verticals). These components may rely on complex observations (human-centric, image) that require advance management characteristics. Additionally, drawing from the decentralisation approach of ASSIST-IoT, special manageability traits must be researched so that the control of this autonomy and reconfiguration can be done in a distributed way. Besides, the different outcomes of the enablers may feed other enablers' parameters located at diverse locations. All the previous drives the need of introducing manageability features beyond the classic centralised approach (controlling the deployment from a single, cloud data centre).

2.13.2 Source

D3.5 ASSIST-IoT Architecture Definition – Initial, see: https://assist-iot.eu/

2.13.3 Application/Industry domain:

Application in the IoT platforms for different industry domains.

2.14 From Interoperability to Shared Reality - Consensus, Coherence and Context in the Spatial Web standardisation challenges

2.14.1 Description of edge computing research/standardisation requirement

As the world transitions from Web 2.0. to Web 3.0, the most urgent and difficult challenge involves the interoperability of multiple technologies and hardware devices. Indeed, with the advent of technologies like XR (e.g., AR, VR), AI, IoT and DLT, cyberspace has extended to encompass more and more aspects of the physical world even as the elements of the physical world increasingly find themselves digitized.

The goal here would be the integration of these disparate but increasingly mutually reliant technologies into a single, cohesive network for information exchange that is as coherent with our logical understanding of the world as it is with the physical features of the world.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Achieving this goal requires enabling interoperability and governance of digitally mediated systems and their operations through the mechanism of a universal language uniquely designed to maintain coherence across data models, logical structures and experiential representations.

This requires a new class of standards suitable for the operation and governance of cyber-physical information and activities that is universally interoperable, discoverable, private, and secure. It involves exploring:

- new ways to represent data that maintains model coherency through all three layers of an n-tier compute stack at the Interface Layer, the Logic Layer, and the Data Layer.
- new communication and transaction protocols that serve as the communication and verification protocol between all three layers.

This approach would maintain a verifiable and consensus-based “shared reality” across the Data, Logic, and Interface layers of the stack in near real-time in a manner that is empirically coherent, logically consistent and verifiably compliant.

Due to the lack of Interoperability across proprietary ecosystems, open standards are critical for enabling interoperability across ecosystems of services and are needed.

Description of the requirement:

New standards are therefore necessary to enable an open, secure, and interoperable Internet of things (of everything). They would enable real-world and virtual spaces to become addressable and connected spaces, allowing users to track, interact, and collaborate with 3D content, physical objects and their digital representations (digital twins).

Key Requirements:

- At the network level, the requirements are :
    - Ensuring interoperability across platforms, devices, and locations, enabling assets to be securely purchased and transferred between virtual and real-world locations, authenticated and validated using various consensus methods that support the validation of identity, ownership, and usage rights of any asset subject to relevant rights.
    - Enabling the interoperability of search, trade, transaction, trackability, and transfer of assets by and between users within and across physical or virtual locations across digital and physical supply chains.
    - Providing secure authenticated human identities and virtual identities and their relevant profile information, transaction, and location histories for representative agents and avatars.
    - Tracking location-based asset provenance, persistence, and validation
    - Allowing assets to maintain and prove their uniqueness, ownership, location and history.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

- At a user level, the requirement is allowing a user to:
    - securely register, find, buy, sell, and transfer virtually anything between individuals within and across virtual web “spaces” (physical, cyber-physical or purely digital and immersive)
    - connect spaces together to organically grow a new internet space that both visitors and virtual and physical items can securely and reliably move between.
- At the context (meta-data) level, key requirements are:
    - New data meta-models and communication protocols need to define a common method to describe, express, share and update that notion of context between all the edges of a network. They also need to allow a secure and privacy preserving governance of people, places and things. This is not possible without having a network that is “context-aware”.
    - Context in this instance is the semantic, societal, situational and environmental meta-data model about people, places and things over time.
    - Context needs to be shared between networks of heterogeneous devices and applications empowering them to proactively offer enriched, situation-aware and usable content, instructions and experiences: a situational communal garden of context information if you will.

These new meta-models need to support context-aware applications that in turn are able to support interoperable, cross-platform networking between disparate hardware (e.g. autonomous drones, sensors, smart devices, robots) and software systems (e.g. enterprise services, cloud platforms, mobile applications, artificial intelligence) across different vendors and suppliers.

The challenges in modelling context are linked to - and not limited to - a set of constraints : they need to represent the relationship between the identity of the actor, the scope and authorisation of his permissioned activities and the place and time where they may happen. The model needs to coherently describe the “where and when” of any scenario (dimensions, space, time and channel), the “why and how” (i.e. conditions or governance)- (right, credential, claim and activity), and the “who and what” (i.e. objects) - (authority, domain, actor and asset). The result is a context graph.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Its description also needs to:

- Be Stateful
- Be machine readable and executable
- Be shareable between heterogeneous networks, devices and applications
- Maintain coherence over time and space for all actors / edges involved in a use case

Types of Requirements:

The above are a mix of functional and non-functional requirements. However, the details will depend on further study. This is an opportunity for Horizon Europe, for SDO's and for industry alliances.

2.14.2 Source

A number of different SDOs are already working on related standards, here are just a few:

- IEEE: P2874 Spatial Web WG
- W3C: Web of Things, RDF-star, decentralized identifiers, signed graphs, etc.
- ETSI: ISG CIM: NGSI-LD

2.14.3 Application/Industry domain:

Implementing these standards and models with these characteristics can pave the way for the possibility of spatial "smart contracting" applications that can govern a rule-based permission of various physical IoT devices and digital information systems in cyber-physical space. Those smart contracts can enable the management of location-based data and device policy, spatial computing content, and the physical programming and automation of Human, IoT, AI and Robotic field activities.

They would be applicable across almost any domain: from smart cities, smart supply chain, smart mobility, smart healthcare, smart retail, smart construction, or smart farming or metaverse-scale virtual actions and transactions

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

2.15 AIOTI identified research and standardisation challenges

2.15.1 Description of research and standardisation challenges

1. **Interoperability in IoT and edge computing systems:** IoT and edge computing ecosystems involving complex systems with many organisations. Interoperability at the semantic, policy and behavioral level is complex. Interoperability of meta data (i.e. knowledge) is not well addressed.

2. **Standardization & regulation framework, and interoperability**, rules for the coexistence of intelligent IoT and edge computing devices and systems in different environments and across sectors, where computing continuum plays a significant role
3. **Enhanced approach to certification for IoT and edge computing devices and systems** needed within a common framework consistent with the standardization work in different enabling technologies domains
4. **Trustworthiness and dependability in IoT and edge computing systems**: Complex IoT and edge computing systems must support many non-functional properties. Handling properly these properties, their relations and their evolution is not well addressed.

5. **IoT and edge computing in Digital service transformation**: The envisaged trend is the convergence of future networks, cloud computing, any type of connected object and the strategic use of data and analytics in an ICT continuum platform. We expect the edge, clouds, networks, IoT and data to form dynamic and intelligent collectives (swarms), featuring localised and temporal interactions between compute nodes each with their own autonomy, but working together for the benefit of the collective community. Examples of this Swarm Computing can be found in autonomous vehicles but also in many other domains. The challenge is to adapt the legacy to be ready for the digital economy and smoothly manage the end-to-end ICT continuum. These end-to-end management platforms should be on one hand modular **with a high level of resource abstraction** so that they can be based on multiple vendor combinations and on the other hand, also offer service capability exposure functions via **open APIs** to enable telecommunication providers to partner with enterprises in vertical sectors. IoT and edge computing is an enabler for the digital service transformation. However, the need of converging ICT and OT technologies for the support of digital service transformation, impose standardisation challenges on the IoT and edge computing architecture, such as **interfaces, data models and ontologies**

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

6. **IoT and edge computing coexistence across sectors:** Due to the fact that the ecosystem of Edge computing systems consists of a collection of different processing/computing points, i.e., cloud data centre, edge computing systems and end devices, and different underlying communication infrastructures, makes the collaboration between such systems a **standardisation challenging task from the point of interoperability (interfaces, data models and ontologies), security and privacy models**.

7. **AI/ML enabled Network and Services**: AI/ML will enable innovative features when provisioning future digital cognitive services for homes, businesses, transportation, manufacturing, and other industry verticals, including the smart cities. This drive the move of computational and memory/storage resources from huge data centres towards the edge of the network thereby changing network designs. At the same time, we expect a significantly increase in the amount of machine-to-machine (sensor) communications monitoring smart cities, Industry 4.0, smart energy, etc. AI will play an increasing role in network management reducing costs, increasing productivity, and driving more value and customer experience. Different learning techniques will be used to predict the behaviour of the network. This will lead to better provisioning of resources in the network, avoiding the nowadays-typical situation where the networks are over-dimensioned. Eventually, regarding OPEX optimisation, it is well known that energy consumption is one of the major cost items for Network Operators: AI/ML methods and systems will allow using the data lake for implementing performance analysis and optimisation methods for energy consumption versus quality of service. **New services powered by AI/ML will bring significant socio-economic impacts**, together with improved sustainability models for Network Operators. Personal data platforms tightly connected with the network service are expected to allow Internet users the control of their data. Future networks have to address security challenges with a new and IT-oriented perspective. Integration of AI/ML will provide new instruments to mitigate the risks. Applications of AI/ML methods and systems in future network scenarios are likely to require multi-domain orchestration of distributed processing. To this **end, end-to-end interoperability is a must** and it requires more standardisation efforts and further progress in functional architecture of 5G networks and beyond. Hardware and software vendors will need to participate in standardisation bodies and collaborate with Open Source communities.

8. **Service discovery is essential**. Existing mechanisms are not sustainable and alternative routing algorithms may help scale the routing infrastructure, but there are many open questions on how these will work. **The architecture** will have to become much more dynamic, since the network of the future will be addressing billions of sophisticated data management and processing services within the network.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Service provisioning, management, and security are critical. We must learn how to effectively manage billions of devices, ensuring that they are suitably configured, running appropriate software, kept up-to-date with security updates and patches, and run only properly authenticated and authorised applications. **Security models must evolve**. Tools for secure boot, code signing, and cryptographic verification of the execution environment will become critical. As will tools to manage and control data access, management, and provenance.

9. **Authentication of services and service providers**, while accounting for resource usage, is an essential part of the economics of the network of the future. Micropayments will become a key part of the system as the infrastructure to support in-network services and applications is not free.

10. **Privacy and data management**, location of processing and data to match legal and moral restrictions on data distribution, access, and processing become increasingly important. Many of the services and applications envisaged operate on, process, and deal with personal data that is increasingly – and rightly – subject to strict regulation, control, and limitation. We do not have good tools to describe how data can be processed, located and distributed – not in human language, legal language, nor code.

11. **Policy descriptions, rules, and constraints** will need to be urgently specified in a form that can be enforced by the infrastructure on the services, since direct human oversight is not feasible at the scales considered.

12. **Novel programming models and languages** will be needed to support these services, applications, and deployments.

13. **Devices and open device management**: Deploying and managing a large set of distributed devices with constrained capabilities is a complex task. Moreover, updating and maintaining devices deployed in the field is critical to keep the functionality and the security of the IoT systems. To achieve the full functionality expected of an IoT system, **new interoperable advanced network reorganization and dynamic function reassignment** mechanism are needed. Moreover, **new IoT interoperable device management techniques are needed that are adapted to the evolving distributed architectures** for IoT and edge systems based on an open device management ecosystem.

14. **Edge, Mobile Edge Computing and Processin**g: Edge, mobile edge computing or Multi-access Edge Computing (MEC) and processing requires responsive network connectivity to allow things and humans to touch, feel, manipulate, or control objects in real or virtual environments. These edge processing in the network architecture is essential for ultra-low latency and reliability, while the AI processing is transferred at the mobile/IoT device. **These changes will impose standardisation challenges on the open distributed edge computing architectures, interfaces and data models, end-to-end distributed security, trustworthiness and privacy models.**

15. **IoT and X-Continuum Paradigm:** Due to huge increase of connected devices and systems, several computing deployments are embracing the notion of computing continuum, where the right compute resources are placed at optimal processing points, i.e., cloud data center, edge computing systems and end devices, This requires the support of:

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

- continuum of technologies across sensors, connectivity, gateways, edge processing, robotics, platforms, applications, Al, and analytics, including underlying technologies like optical, wireless (cellular and non-cellular) and satellite communications;
- continuum of intelligence and IoT edge capabilities
- continuum of IoT edge applications across vertical sectors and seamless integration

16. The use of end-to-end capabilities of IoT technologies across the edge granularity and beyond impose continuum **standardisation challenges, such as support of interoperability by the means of new interfaces, data models, security and privacy models and security and privacy models.**

17. **IoT Swarm Systems:** Concepts for IoT intelligence clustering to promote collaboration and share of resources and functions for performing specific tasks. These concepts impose standardisation challenges in the required architecture, such as interfaces, data models and ontologies and as well security and privacy models.

18. **Decentralized Distributed IoT Edge Systems:** IoT architectures considering the requirements of distributed intelligence at the edge, cognition, artificial intelligence, context awareness, tactile applications, heterogeneous devices, end-to-end capabilities.

19. **Federated Learning and Al for IoT Edge:** Federated Learning brings Al models close to the edge to enhance data protection, improve inference reliability, and increase autonomy of end clusters (e.g., end IoT/IIoT devices, on-premises servers, etc.). The cloud plays a federation role for aggregating insights from different IoT edge distributed clusters to generate a federated model shared with each individual cluster:

    - Collaborative work for IoT devices and services discovery
    - Standardisation Challenges - **workflow standardization, interfaces edge/cloud, orchestration, model contamination, and pipes for handling distributed traffic**

20. **OSs and Autonomous Orchestration Concepts**: New orchestration paradigms to support distributed IoT edge based on internet-enabled automation concepts, virtualization, multi-state analytics, digital twins to improve end-to-end response time and swarm paradigms integration
21. **IoT Systems integration**: IoT intelligent systems integration through federation of platforms and distributed systems including many heterogeneous IoT devices and smart systems to provide resilience, security and trust for Al-based IoT edge applications. This will require a **standardized reference architecture with new/modified interfaces.**
22. **IoT sectorial and Cross-Sectorial Open Platforms:** These concepts will impose federated and distributed identity management for authentication, authorization policies, the access control mechanisms, and facilitates the exchange and coordination among several cross sectorial open platforms. Moreover, a common framework is needed for verification, validation, testing, and certification of different IoT implementations based on agreed performance requirements. Moreover, validation verification methods for task development of edge IoT intelligent multi-agent system architecture.
23. **IoT and edge computing Platforms**: IoT platforms require interoperability at multiple levels and a federation of platforms will allow optimising the use of the resources, improving service quality and most likely reducing costs. Research on IoT platforms and integration of the functions of the platforms in the intelligent infrastructure as well as research on a layer-oriented approach and semantic interoperability in heterogeneous systems is required to address interoperability at all

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

layers. The inclusion of a programmable, software defined network layer is critical for merging IoT and 5G and future architectures. Emerging industrial IoT applications, Tactile Internet, digital twin and autonomous/robotic systems solutions will require much faster reactivity at the edges of the networks as it becomes increasingly inefficient to extract insights from the cloud with growing numbers of IoT devices. These trends impose as well standardisation challenges such as modification of interfaces, data models, security, and privacy models.

24. **IoT Distributed and Federated Reference Architectures** integrated with the 5G architecture and AI. Further research is needed in the area of novel IoT *distributed* architectures for addressing the convergence of (low latency) Tactile Internet, Digital Twin edge processing, AI, and distributed security based on ledger or other technologies and the use of multi-access edge computing.
25. **Charging aspects for Edge Computing Systems** for End User of IoT edge application usage over the mobile networks as well as for Inter-Provider considering different business roles. The charging scenarios specification is needed for different business requirements with potential impact on charging architecture, functions and procedures.
26. **Security by Design:** Secure IoT and edge computing systems define security as a part of trustworthiness and demand the inclusion of dedicated security related functionalities and concepts. Details do depend on the specific application domains and use cases. Samples may include the introduction of dedicated functional domains like e.g.:
    - Resource Access and Interchange by introducing a novel Frontend Access Control;
    - Operations & Management Domain by designing and implementing a security-focused Runtime Monitoring system;
    - Sensing and Controlling Domain by implementing an advanced Attack Detection and Honeypots.

2.15.2 Source

AIOTI identified challenges, see:

- Smart Networks and IoT - Common topics for research and innovation in Horizon Europe

  https://aioti.eu/wp-content/uploads/2019/09/5G-IA-AIOTI-Common-Topics-190930-Web.pdf

2.15.3 Application/Industry domain

Those standardisation challenges applied as well to horizontal industrial domains and as well to all possible vertical industry domains.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

3 High-level description and Categories of Standards challenges

3.1 Introduction

The previous section introduced edge computing research and standardisation challenges that have been identified either from the edge computing activities of the AIOTI members or from literature studies. Challenges and groups of challenges were presented in various degrees of detail and for specific applications and domains. The previous section can be identified as the "brainstorming" phase for the identification of standardization gaps, forming the basis of future activities.

In this section, based on the above results, all of the above input will be mapped to specific Categories of Standards Challenges. This will make it easier to acquire a high-level and homogeneous view of the various standards challenges, and provide structure that will be essential to identify specific gaps (which are going to be presented in Section 4).

3.2 Standards Challenges Categories

3.2.1 Standards Challenge Category #1: Regulations, Rules, and Processes - Having common goals and procedures

Interoperability in complex IoT and edge computing systems, involving many organisations, is lacking, when it comes to a) the identification and b) adoption of) **policies** in different verticals that may have common targets. An example of such policies are the ones set in the maritime sector by IMO (International Maritime Organization) for reduction of CO_2 emissions vs similar policies set in IIoT and Smart Cities environments (Section 2.15.1). Likewise, there is a need for a standardization and regulation **framework**, and standardized **rules** and **processes**, for the interoperability of horizontal solutions (at the policy and **behavioural level**), i.e. the coexistence of intelligent IoT and edge computing devices and systems in different environments and across sectors, where computing continuum plays a significant role (Section 2.15.2).

Complex IoT and edge computing systems must support many **non-functional properties**, which are not yet well addressed (Section 2.15.4). Indicative recurring issues for example are those of "privacy by design" and "data security/privacy", and the compliance to related regulations such as GDPR (Section 2.1, Section 2.5, Section 2.6, Section 2.8). Another common issue is that of ensuring (and defining) trust in specific systems and entities, something that makes necessary the existence of frameworks facilitating e.g., digitally signed attestations by third parties and immutable logs and data sharing policies, as well as smart contracts for agreements (Section 2.9).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Moreover, policies and regulations may refer to Green Deal and as well Environmental, Social, and Corporate Governance (ESG) policies taking under consideration social and environmental factors (Section 2.4, Section 2.5, Section 2.6), legal and moral restrictions on e.g., data distribution (Section 2.15.10), and even ethical principles and standards of normative behaviour as part of common sense (Section 2.7) that could be adopted by future human-like AI systems.

3.2.2 Standards Challenge Category #2: Semantics, Models, and Languages - Talking about the same things in the same manner

Interoperability at the **semantic** and **metadata** (i.e. knowledge) level is complex (Section 2.1, 2.15.1).

This refers to the standardized definition and **description** of policies, rules, processes, and behaviours, Things, data, meta-data, information, and knowledge. Policies, rules, and constraints descriptions will need to be specified in a form that can be enforced by the infrastructure on the services (Section 2.1, Section 2.6, Section 2.15.11).

It also refers to the standardized definition and description of abstract constructs and goals set in different domains, so as to properly model context (Section 2.14). For example, the topic of ensuring *Trust* on Edge computing and on computing continuum systems is common, while there is still no standardized way to define (and then, to measure) Trust, Reputation, Trustworthiness, Popularity, Reliability, Dependability, SLAs, etc. in such systems. Another example is that of digital twins and explainable artificial intelligence, providing tools (such as high fidelity physics-based simulators, data-driven models, etc.) for physical realism and future projections (Section 2.7, Section 2.8, Section 2.9).

Novel **programming models** and (e.g., policy) **languages** are needed to support the corresponding services, applications, and deployments (Section 2.2, Section 2.15.12, Section 2.15.23). A universal language uniquely designed to maintain coherence across data models, logical structures, and experiential representations is required and can be extracted by finding new ways to represent data (Section 2.14).

3.2.3 Standards Challenge Category #3: Taxonomies, Ontologies, Data Models, and Architectures - Setting a common structure

As an extension to Standards Challenge Categories #1 and #2, there is a need to develop (or reuse**) data models**, **taxonomies**, and **ontologies** required by IoT and edge computing solutions (Section 2.4).

These have to be aligned to already established and globally identified initiatives, such as the Green Deal and ESG Data Taxonomy (Section 2.5, Section 2.6). The challenge for standardized data (meta-) models and ontologies is imposed by the need of converging ICT technologies and systems for the support of digital service transformation (Section 2.9, Section 2.14, Section 2.15.5, Section 2.15.6, Section 2.15.23). A framework for data integration across different ontologies should also be considered, given that it may be unrealistic to expect everyone to use the same ontologies given differences in requirements and perspectives (Section 2.9).

The Next Generation Internet of Things field is requiring the creation of a robust, formal, valid, useful and standardized **reference architecture** to build deployments upon. The IoT intelligent systems integration through federation of platforms and distributed systems will require new reference designs and/or a standardized architecture with new/modified interfaces (Section 2.15.21). Research is still

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

needed in novel IoT distributed architectures to address the convergence of Tactile Internet, edge processing, AI and distributed security based on ledger or other technologies, the use of MEC, and the 5G architecture (Section 2.2, Section 2.4, Section 2.13, Section 2.15.7, Section 2.15.24).

3.2.4 Standards Challenge Category #4: Metrics, KPIs, Benchmarks, and Tests - Quantifying and Measuring in the same way

As an extension to Standards Challenge Category #1 and #2, to complete the definition and description of policies, constraints, abstract constructs (such as Trust), etc., there is a need for standardized/common, well-defined (performance and other non-functional requirements) metrics and KPIs for edge, cloud, and edge-to-cloud solutions (benchmarking, SLAs, etc.). This refers to both domain verticals (e.g., to define the CO_2 footprint of ICT installations) and horizontals (R&I activities for reference designs and benchmark platforms). An example is that of Green Deal and ESG **scores compiled from the data that are collected from surrounding specific metrics** related to intangible assets within the enterprise and could be considered a form of corporate social credit score. The existence of such metrics are enablers for evaluation and monitoring of activities of interest (Section 2.2, Section 2.4, Section 2.5, Section 2.6).

On the same spirit, the introduction and/or use of any edge computing communication protocols and configurations requires high quality and confidence in the implementations. This includes the application of various types of **tests**, e.g., conformance, interoperability and robustness/security test scenarios. From the viewpoint of a standardization committee, testing, validation, verification, and certification methods and techniques should follow standardized approaches (Section 2.10, Section 2.15.3, Section 2.15.22).

3.2.5 Standards Challenge Category #5: Identification, Authentication, and Discovery - Common access

Distributed and federated edge computing systems require service **discovery** and delivery support, in particular, for scenarios where multiple mobile devices are used that require services simultaneously and uninterruptedly. The corresponding mechanisms may not be sustainable, and alternative routing algorithms may help scale the routing infrastructure. There is a challenge of effectively managing billions of devices, ensuring that they are suitably configured, running appropriate software, kept up-to-date with security updates and patches, and run only properly authenticated and authorised applications (Section 2.3, Section 2.14, Section 2.15.8).

Authentication of services and service providers, while accounting for resource usage, is also an essential part of the economics of the network of the future. There is a need of ensuring interoperability across platforms, devices, and locations, by enabling assets to be securely purchased and transferred between virtual and real-world locations, authenticated and validated, using various consensus methods that support the validation of identity, ownership, and usage rights of any asset subject to relevant rights (Section 2.14, Section 2.15.9, Section 2.15.22).

3.2.6 Standards Challenge Category #6: Management, Comms, Protocols, Interfaces, and Platforms - Using the same tools

As a large number of players in the IoT ecosystem are driving the development and deployment of their own IoT platforms and solutions, there is a need for standardized communication and transaction **protocols** and **interfaces**, to avoid lock in and fragmentation and support of operational

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

interoperability among systems and solutions (Section 2.4, Section 2.5, Section 2.6, Section 2.14, Section 2.15.5, Section 2.15.6, Section 2.15.14, Section 2.15.5, Section 2.15.16, Section 2.15.17).

To achieve interoperability and governance of digitally mediated systems and their operations a new class of standards suitable for the operation and governance of cyber-physical information and activities is required (Section 2.14). **Scheduling and Management Mechanisms** have to be defined and the corresponding **platforms** have to be developed in a standardized manner so as to enable the future operation of collectives/swarms (Section 2.15.5, Section 2.15.19), collaboration and federation between such systems (Section 2.15.6, Section 2.12, Section 2.15.2), responsive network connectivity (Section 2.3, Section 2.15.14), interoperability and collaboration between heterogeneous Edge Computing Systems (Section 2.13, Section 2.15.16, Section 2.15.7, Section 2.15.18), IoT intelligence clustering (Section 2.15.17), efficient scheduling (Section 2.2, Section 2.12) and device management (Section 2.2, Section 2.15.13), coordination of distributed processing (Section 2.8, Section 2.9), seamless application lifecycle and handover (Section 2.11, Section 2.15.15), orchestration (Section 2.15.20), and overall manageability (Section 2.13).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

3.3 Bringing everything together

Figure 3 presents in a hierarchical manner the six (6) categories of Standards Challenges presented in Section 3.2. As it can be inferred, there is a natural flow, starting from the identification and definition of rules, continuing with the semantic description, classification, and quantification of entities of interest, and finishing with access and management related mechanisms.

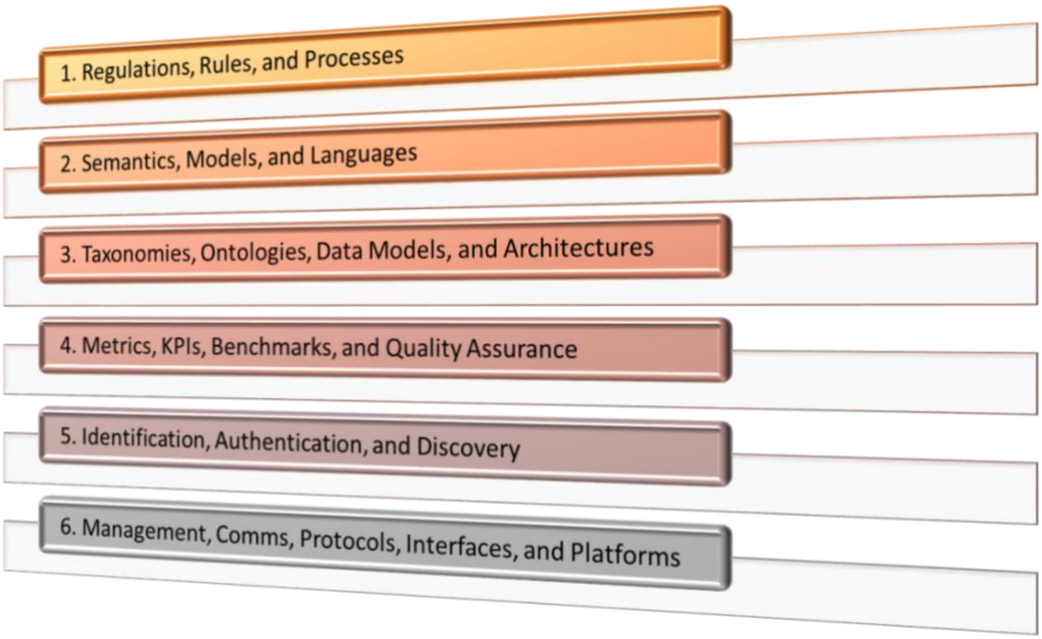

Figure 3: The Standards Challenges Categories

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 1 provides the showcase on how the several research challenges groups presented in Section 2 map to the Standards Challenges Categories. As it can be identified, the current categorization covers all of the identified challenges. Each of the cells in this table incudes keywords to identify the relevant standardisation challenge.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 1: Mapping of Research Challenges groups to Standards Challenges Categories (SCC)

Challenges presented in detail in	SCC1 – Rules	SCC2 – Semantics	SCC3 – Structure	SCC4 – Measuring	SCC5 – Accessing	SCC6 – Managing
Section 2.1	legal/ethical/ social adoption	semantic interoperability				
Section 2.2		novel model & languages	distributed architectures	edge-specific constraints		device/agents management
Section 2.3					service discovery	infrastructure interoperability
Section 2.4	EU Green Deal			CO_2 footprint measurability		energy-efficient protocols
Section 2.5	EU Green Deal		data-models, ontologies	CO_2 footprint measurability		comms. energy usage control
Section 2.6	ESG regulations (e.g., SFDR)	impact definition	ESG Data Taxonomy	define ESG scoring/ratings		connectivity, interoperability
Section 2.7	ethical principles	meaningful explanations				
Section 2.8	data privacy	semantic annotation				large-scale computation
Section 2.9		models	knowledge graph			
Section 2.10				testing methods/ techniques		
Section 2.11						seamless MEC deployment
Section 2.12						seamless MEC transition
Section 2.13			NGIoT architecture			orchestration, interoperability
Section 2.14		context/models coherency	data meta-models		search, trade, trackability	connect spaces, interoperability
Section 2.15.1	interoperability on policy level	interoperability on meta-data				
Section 2.15.2	regulation framework					coexistence of intelligent IoT
Section 2.15.3				IoT/edge certification		
Section 2.15.4	non-functional properties					
Section 2.15.5			data-models, ontologies			Interfaces & APIs
Section 2.15.6			data-models, ontologies			IoT/edge coexistence
Section 2.15.7			5G networks architecture			network management
Section 2.15.8					service discovery	
Section 2.15.9					services authentication	
Section 2.15.10	legal/moral restrictions					
Section 2.15.11		policy description				
Section 2.15.12		models, languages				
Section 2.15.13						devices management
Section 2.15.14						responsive connectivity

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Challenges presented in detail in	SCC1 – Rules	SCC2 – Semantics	SCC3 – Structure	SCC4 – Measuring	SCC5 – Accessing	SCC6 – Managing
Section 2.15.15						computing continuum
Section 2.15.16						computing continuum
Section 2.15.17						IoT intelligence clustering
Section 2.15.18						decentralized IoT-edge
Section 2.15.19						Federation, orchestration
Section 2.15.20						autonomous orchestration
Section 2.15.21			reference architecture			
Section 2.15.22				testing, validation	AAA[8] mechanisms	
Section 2.15.23		semantic interoperability	layer-oriented approach			
Section 2.15.24			IoT reference architecture			

[8] Authentication, Authorization, and Access

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

4 Standards Gaps

This section provides the method of identifying and prioritizing the AIOTI identified edge computing challenges in standardisation gaps.

4.1 Definition and classification of standards gaps

The definition of a Standard Gap are based on [AIOTI-IoT-Gaps] and STF 505 document [ETSI TR 103.375]:

- **standardization gaps**: missing or duplicate elements in the edge computing 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.

Beyond the aforementioned in Section 3.2 and Section 3.3 categories of standardisation challenges, an additional categorisation that is used in this section is based on the mapping of the identified standardisation challenges into technology trends. The identified technology trends are listed below:

- **Green Deal**
- **Security and Data Privacy**
- **Social Challenges and Monetization**
- **The Digitalization struggle, including Digital Twins**
- **Computing Continuum**
- **Artificial Intelligence**

The above challenges/needs topics can be split in smaller domain- or technology-specific areas (e.g., one area is that of Security and Data Privacy, which can be supported by e.g., Trust & Reputation Management Systems which can extend to Consensus systems).

4.2 Standards Gaps: Identification

This section provides a collection of the identified edge computing standards gaps. The identification of standards gaps is an important activity for the edge computing community and has been a subject of interest and work in a number of projects, groups, etc.

The collected edge computing standardisation challenges identified in Section 3.2 and Section 3.3 are used as a basis for the identification of these edge computing standard gaps.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 2 provides the showcase on how the several research challenges groups presented in Section 2 mapped to the above technology trends. Each of the cells in this table incudes keywords to identify the relevant standardisation challenge.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 2: Mapping of Research & Standardisation Challenges groups to Technology Trends

Challenges presented in detail in	Green	Security/ Data Privacy	Social	Digital/Digital Twin	Computing Continuum	AI
Section 2.1		intelligent approaches			interoperability, orchestration	
Section 2.2	energy costs balance	distributed security			federation, cross-platform	network optimization
Section 2.3		users trust, fault tolerance	agile pricing		systems' collaboration	
Section 2.4	energy /CO_2 footprint	solutions evaluation		massive IoT applications		green AI
Section 2.5	energy /CO_2 footprint	solutions evaluation				
Section 2.6	environmental impact score	GDPR compliance	ESG monitoring	metrics collection		performance acceleration
Section 2.7						explainable AI, common sense
Section 2.8		confidentiality, non-repudiation		digital twins, physics realism		explainable AI, interpretability
Section 2.9		digital attestations		digital twins, data spaces		federated learning
Section 2.10				new solutions certification		
Section 2.11					MEC, connectivity	
Section 2.12					MEC hosts, interoperability	
Section 2.13		access, share, store, threats	human-centric		microservices, scaling, planes	distributed AI, fed. learning
Section 2.14	environmental meta-model		societal context, buy-sell	model coherency	interoperability, internet space	
Section 2.15.1					interoperability, ecosystems	
Section 2.15.2					coexistence rules	
Section 2.15.3				devices/systems certification		
Section 2.15.4		trustworthiness, dependability		non-functional properties		
Section 2.15.5				digital service transformation		
Section 2.15.6		security/privacy models			interoperability, coexistence	
Section 2.15.7						cognitive digital services
Section 2.15.8			socio-economic impact	service discovery	end-to-end interoperability	
Section 2.15.9		service security, security models				
Section 2.15.10		services authentication	micropayments			
Section 2.15.11	policy descriptions		policy descriptions			
Section 2.15.12				novel models/ languages		
Section 2.15.13				distributed devices	reorganization, reassignment	

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Challenges presented in detail in	Green	Security/ Data Privacy	Social	Digital/Digital Twin	Computing Continuum	AI
Section 2.15.14					responsive connectivity	AI on the edge
Section 2.15.15					X-continuum paradigm	
Section 2.15.16					granularity, interoperability	
Section 2.15.17					swarm systems	intelligence clustering
Section 2.15.18				distribution, decentralisation		cognition
Section 2.15.19						fed. learning, AI for edge
Section 2.15.20				virtualisation, automation		
Section 2.15.21					systems integration	AI-based edge applications
Section 2.15.22		federated AAA[9]		digital twin, IoT certification	infrastructures merging	
Section 2.15.23					interoperability, merging	
Section 2.15.24		distributed/ ledger security		digital twin		distributed AI

[9] Authentication, Authorization, and Access

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

4.3 Standards Gaps: Prioritisation

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

To capture a more quantitative view of the extent to which existing standardization initiatives cover (or not cover) the AIOTI identified standardization challenges, we go a step further and identify how many of these 96 standardization specifications address fully or partially the said challenges. In particular, Annex IV provides a mapping of 96 SDOs specifications to the 39 (14+25) standardization challenges identified by AIOTI and presented in Section 2. This mapping facilitates the identification of standardization gaps. The four first columns provide the source, title, url, and abstract of each standardization specification, whereas the last column maps each specification to the specific standardization challenges (sections) and labels, as identified by AIOTI in Sections 2, 3, and 4.2 of this document.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

5 Gap analysis and resolution work in SDOs

5.1 Gap Resolution

The identification and prioritisation of gaps, and in particular standards 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 edge computing community, depending on the breadth and complexity of the gap.

The resolution of the (standards) gaps is the work of the relevant organizations of the edge computing community, in particular the Standards Developing Organisations (SDOs) and Standards Setting Organisations (SSOs) [AbLa18]. This section addresses the work done in some of the SDOs/SSOs involved in AIOTI WG Standardisation.

5.2 Maintaining an overview of standardisation activities and specifications related to edge computing

History shows that many organisations have devoted resources to surveying the edge computing 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.

AIOTI plans to improve the efficiency by collaborating and applying the approach used by the EUOS project, which is designed to improve collaboration and timeliness and re-use. The simple tool used is an excel document (originally contributed under CC4 licensing to SF-SSCC [SF SSCC]) containing a macro and two lists (worksheets) which provide the basic information on (a) IoT organisations, (b) their specifications (see example in Figure 4). The lists are designed to show in the first few columns the public information on each organisation or specification, and then in additional columns the added analysis, keywords or categorisation which AIOTI finds appropriate. Obviously, the list can be filtered or ordered to fit various types of analysis. The macro (within the spreadsheet) is able to export the key information and chosen categories into a mind map (see example Figure 5) which has been found to aid discussions and drill-down analysis. The details stored in the mind map can be viewed via the following mind map document (see link) that was generated using EUOS owned tools.

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
3GPP	3GPP TR 28.815 V17.0.0 (2021-12): Study on charging aspects of edge computing	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3758	The present document studies the charging aspects of Edge Computing based on architecture, procedures and information flows for enabling Edge Applications over 3GPP network as well as capabilities for 5GS to support edge computing. The investigation includes different charging scenarios with potential business requirements, alternative solutions with potential impact on charging architecture, charging functions and charging procedures.	scenarios, architectural considerations (Section 2.15.25)
3GPP	3GPP TR 23.803 V7.0.0 (2005-09): Evolution of policy control and charging	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.as	The document studies: a) the complete harmonization and merger of the policy control and flow based charging architecture and procedures; b) possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control; c) alternative solutions for binding bearers to services (provided	policy control architecture (Section 2.11, 2.15.25)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
		px?specificationId=883	today by the authorization token). This includes studying solutions for the network to control bearer usage by service flows.	

Figure 4: Sample view of worksheet on Edge Computing organisations

Importantly, each organisation which may in future re-use this excel sheet for other purposes can replace or add to the categories provided by AIOTI, enormously reducing the effort needed to make their own analysis or update. There is no necessity that other organisations re-publish their confidential material, but the objective is that additional public material (new organisations or specifications) will be shared. It would also be useful to collaborate with the main SDOs to similarly obtain regular updates to the benefit of all. Further information about using the excel sheet and the definitions of the categories applied in this report are provided in Annex II.

It is possible to import specifications metadata into the excel file by e.g. copying or importing a CSV file with a few simple fields per row:

<comment>;<SDO and WG>;<title>;<url of landing page>; <optional categories>

Note: The term "landing page" is meant to indicate the overview html page (which e.g., for ETSI has the scope and publishing dates and the pdf link, and for ISO or CENELEC has similar info plus a "BUY HERE" button for the pdf). This is actually better than a direct link to a pdf document because the landing pages are more stable.

The excel sheet contains a list of SDO databases, see Table 3, which are capable of exporting such CSV files, using site-specific filtering functions if desired, which is reproduced below for convenience.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

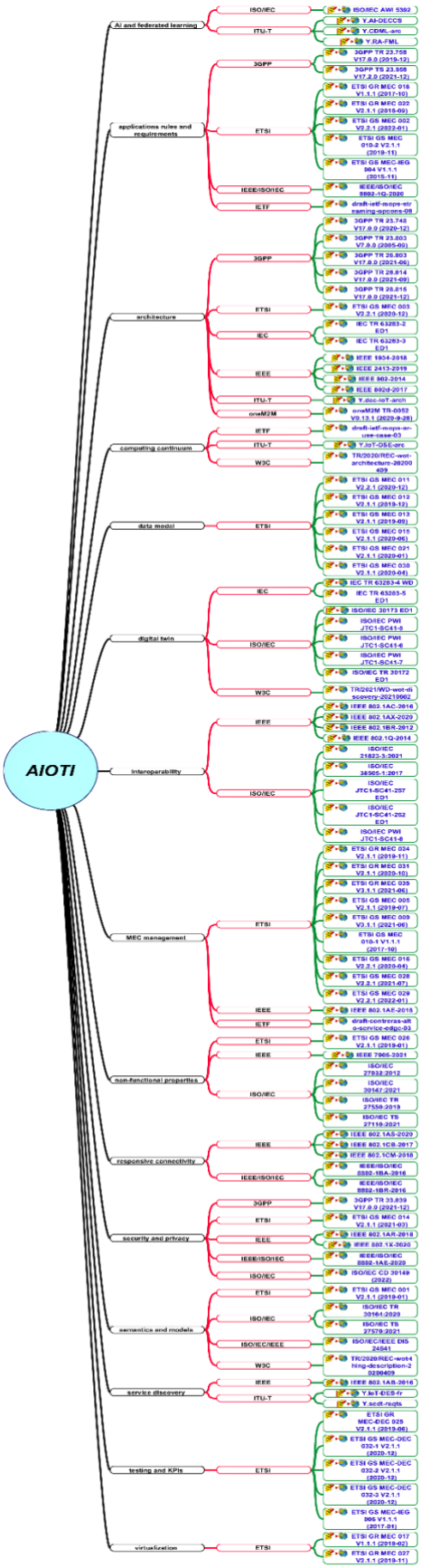

Figure 5: Sample view of the mind map

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 3: SDO Databases of Specifications

Org	Webpage_URL	Org_Full	Abstract
3GPP	https://www.3gpp.org/specifications		The 3GPP project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network and for interworking with non-3GPP networks. The different versions are named: GSM, GPRS (2G), EDGE, UMTS (3G), HSPA, LTE (or 4G), LTE Advanced, 5G.
5G-ACIA	https://www.5g-acia.org/	5G Alliance for Connected Industries and Automation	5G Alliance for Connected Industries and Automation ensures the best possible applicability of 5G technology and 5G networks for the manufacturing and process industries by addressing, discussing and evaluating relevant technical, regulatory and business aspects.
AIOTI	https://aioti.eu/resources/standardisation-resources/	AIOTI Reports on IoT Standards	We aim to lead, promote, bridge and collaborate in IoT & Edge Computing and other converging technologies research and innovation, standardisation and ecosystem building providing IoT deployment for European businesses creating benefits for European society. We co-operate with other global regions to ensure removal of barriers to development of the IoT & Edge Computing market, while preserving the European values, including privacy and consumer protection.
CEN	https://standards.cen.eu/dyn/www/f?p=CENWEB:105	European Committee for Standardization (CEN)	Live search of CEN using title/summary but no export to file.
CENELEC	https://www.cenelec.eu/dyn/www/f?p=104:103	European Committee for Electrotechnical Standardization	Live search of CENELEC. Use "documents" tab.
CEPT-ECO	https://www.ecodocdb.dk/	CEPT Electronic Communications Office Database	The ECO Documentation Database provides an easily accessible (searchable, exportable) library of ECC deliverables (decisions, recommendations and reports) in the field of radio spectrum, numbering and networks regulation. Related documents, including relevant EC legal acts and ETSI technical standards are also provided for information, where applicable. All related EC deliverables, technical standards produced by ETSI and technical guidance notes developed by RED-CA, can be downloaded from their respective websites. A brief description of the features of this database is available here.
CESIP	https://webgate.ec.europa.eu/cesip/Index.aspx	Europe-China Standardisation Information Platform	The Europe-China Standardization Information Platform has information on standards in 10 sectors:
EC JOINUP	https://joinup.ec.europa.eu/collection/ict-standards-procurement/energy	Standards under Reg.1025-2012	Categorized list of specifications
ETSI	https://www.etsi.org/standards#page=1&search=IOT	ETSI Standards Search	The advanced search allows export of a file which includes SCOPE information for documents. It also can limit the search to keywords like OR(SAREF, IoT, SmartCity, M2M. ETSI has published TR 103 375 [ETSI TR 103.375] which contains a landscape of IoT standardisation.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Org	Webpage_URL	Org_Full	Abstract
IEC	https://webstore.iec.ch/advsearchform	International Electrotechnical Commission	The search covers title and abstracts as well as IEC categories. No export found.
IEC	http://www.electropedia.org/	IEC Electropedia of Terminology	
IEEE	https://standards.ieee.org/search-results.html?q=smart+city		You may retrieve, download and print one (1) copy of the Materials in this Program for your personal use. You may retain one (1) additional copy of the Materials as your personal archive copy.
IETF	https://www.rfc-editor.org/search/rfc_search.php	Internet Engineering Task Force (IETF)	IETF RFCs cover many aspects of computer networking, including protocols, procedures, programs, and concepts, as well as meeting notes, opinions, etc.
IIC	https://www.iiconsortium.org/vocab/index.htm		IoT Terminology
ISO	http://www.iso.org/obp		ISO Online Browsing Platform
ISO/IEC/IEEE	https://pascal.computer.org/sev_display/index.action		Joint vocabulary of computing terms
ITU-T	https://www.itu.int/net4/ITU-T/landscape	ITU-T Standards Landscape	Lists of IoT specs sorted by origin and keywords
ITU-T	http://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en#lang=en	ITU-T Terminology	
JoinUp	https://joinup.ec.europa.eu/collection/ict-standards-procurement/identified-ict-specifications-procurement	EU list of ICT Standards for Procurement	In order to allow the EU to respond to the fast evolution of technology in ICT, while also ensuring competition, promoting interoperability and innovation, the European Commission has developed a flexible approach to standardisation and can identify/cite ICT technical specifications that are not national, European, or international standards, provided they meet precise requirements. Once identified and approved, these specifications can then be referenced in European public procurement. This website displays the (short) list.
StandICT.eu	https://www.standict.eu/standards-watch		EU project has title/scope info on several hundreds of standards documents, various domains
UNBIS	https://lib-thesaurus.un.org/LIB/DHLUNBISThesaurus.nsf/MultiEng/85759FD34196A99A85256AA0005FBD0B?OpenDocument	UNBIS Terminology	

The idea of using CC4.0 open license should enable any users (e.g. AIOTI) to import the lists into excel or a mind map or whatever, and annotate it according to their own ideas, as was proposed for this report.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

6 Standards Gaps Analysis and Recommendations

Annex IV provides a mapping of 96 SDOs specifications to the 39 (14+25) standardization challenges identified by AIOTI and presented in Section 2. This mapping facilitates the identification of standardization gaps. The four first columns provide the source, title, url, and abstract of each standardization specification, whereas the last column maps each specification to the specific standardization challenges (sections) and labels, as identified by AIOTI in Sections 2, 3, and 4 of this document.

To capture a more quantitative view of the extent to which existing standardization initiatives cover (or not cover) the AIOTI identified standardization challenges, we go a step further and identify how many of these 96 standardization specifications address fully or partially the said challenges.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 4 presents the corresponding results (for ease of reference, sections numbers are cross-referenced to the corresponding sections of the document).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Table 4: Number of standards specifications covering the identified challenges of Section 2

Section	Standards	Section	Standards	Section	Standards	Section	Standards
2.1	26	2.11	30	2.15.7	1	2.15.17	0
2.2	41	2.12	15	2.15.8	3	2.15.18	5
2.3	12	2.13	9	2.15.9	2	2.15.19	1
2.4	1	2.14	3	2.15.10	7	2.15.20	3
2.5	1	2.15.1	7	2.15.11	1	2.15.21	2
2.6	2	2.15.2	6	2.15.12	0	2.15.22	4
2.7	1	2.15.3	6	2.15.13	0	2.15.23	4
2.8	7	2.15.4	6	2.15.14	14	2.15.24	6
2.9	1	2.15.5	4	2.15.15	2	2.15.25	2
2.10	6	2.15.6	4	2.15.16	3		

From the above analysis, it can be concluded that, for the given list of standardization specifications, there are considerable standardisation gaps related to the AIOTI identified edge computing challenges of:

- **Digital Twins** (Sections 2.4, 2.5, 2.9);
- ICT/IoT and policies description and languages supporting the **Environmental, Social and Governance (ESG) monitoring** (Sections 2.6, 2.15.11, 2.15.12);
- **Federated Learning and AI** (Sections 2.7, 2.15.7, 2.15.19);
- and **devices and IoT swarm systems management** (Sections 2.15.13, 2.15.17).

Similarly, it can be identified that activities could be initiated for the creation of standardization specifications covering the challenges of:

- IoT and edge computing coexistence/integration/interoperability and continuum across several sectors and platforms (Sections 2.14, 2.15.6, 2.15.5, 2.15.6, 2.15.15, 2.15.16, 2.15.20, 2.15.21, 2.15.22, 2.15.23);
- and Services discovery and authentication (Sections 2.15.8, 2.15.9).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

7 Conclusion

This report introduced an approach for the definition and identification of key edge computing and/or combination of IoT/IIoT, edge computing and cloud computing gaps in several initiatives. Based on the prioritisation of these gaps, the deliverable starts to address the work done within the relevant SDOs that need to cooperate in order to solve these gaps.

The purpose of this document is to reflect a structured discussion within the AIOTI WG Standardisation community and to provide consolidated technical elements as well as guidance and recommendations.

In particular, Section 2 describes the research and standardisation key edge computing challenges, Section 3 describes the high-level description and the categories of standards challenges, Section 4 describes the identification and prioritisation of the AIOTI identified edge computing challenges in standardisation gaps, Section 5 describes the gap analysis work in SDOs and Section 6 describes the standards gaps analysis and recommendations. In particular, Annex IV includes the mapping of 96 SDOs specifications to the 39 (14+25) standardization challenges identified by AIOTI and presented in Section 2. Based on this analysis it can be concluded that, for the given list of standardization specifications, there are considerable standardisation gaps related to the AIOTI identified edge computing challenges of:

- **Digital Twins** (Sections 2.4, 2.5, 2.9);
- ICT/IoT and policies description and languages supporting the **Environmental, Social and Governance (ESG) monitoring** (Sections 2.6, 2.15.11, 2.15.12);
- **Federated Learning and AI** (Sections 2.7, 2.15.7, 2.15.19);
- and **devices and IoT swarm systems management** (Sections 2.15.13, 2.15.17).

Similarly, it can be identified that that activities could be initiated for the creation of standardization specifications covering the challenges of:

- IoT and edge computing coexistence/integration/interoperability and continuum across several sectors and platforms (Sections 2.14, 2.15.6, 2.15.5, 2.15.15, 2.15.16, 2.15.20, 2.15.21, 2.15.22, 2.15.23);
- and Services discovery and authentication (Sections 2.15.8, 2.15.9).

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Annex I References

[AbLa18] Abdelkafi N., Lanting C.J.M., Thuns M., Bolla R., Rodriguez-Ascaso A., Wetterwald M., Understanding ICT Standardization: Principles and Practice, ETSI ed, November 2018. ISBN 978-3-7482-4742-5. Available at https://www.etsi.org/standardization-education.

[AIOTI-BY5G] "IoT and Edge Computing impact on Beyond 5G: enabling technologies and challenges", Release 1.0, AIOTI WG Standardisation, September 2021, see: https://aioti.eu/wp-content/uploads/2021/10/AIOTI-Beyond-5G-R1-Report-Published.pdf

[AIOTI_DfG_2021] "AIOTI Vision: IoT and Edge Computing impact on Green Deal", Release 1.0, November 2021, see: https://aioti.eu/wp-content/uploads/2022/01/AIOTI-IG-Digital-for-Green-Vision-R1-Final.pdf

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

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

[AIOTI-IoT-Edge-Computing] Ovidiu Vermesan, "AIOTI Strategic Foresight Through Digital Leadership - IoT and Edge Computing Convergence", AIOTI position paper, October 2020, to be retrieved via: https://aioti.eu/wp-content/uploads/2020/10/IoT-and-Edge-Computing-Published.pdf

[Edge-ISO] "Information Technology - Cloud Computing - Edge Computing Landscape", ISO/IEC TR 23188, 2018.

[Edge- ETSI_MEC] ETSI, "Multi-access Edge Computing (MEC); Terminology", ETSI GS 001 , 2019, https://www.etsi.org/deliver/etsi_gs/MEC/001_099/001/02.01.01_60/gs_MEC001v020101p.pdf

[Edge-OpenFog] "OpenFog Reference Architecture for Fog Computing", OpenFog Consortium , 2017.

[ETSI TR 103.375] "SmartM2M; IoT Standards landscape and future evolution", ETSI TR 103 375 (STF 505), 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

[IETF-T2TRG] J. Hong, Y-G. Hong, X. de Foy, M. Kovatsch, E. Schooler, D. Kutscher, "IoT Edge Challenges and Functions", IETF Internet draft, draft-irtf-t2trg-iot-edge-02 (work in progress), 2 May 2021.

[Networld2020-SRIA] “Smart Networks in the context of NGI”, SNS SRIA, Networld2020, September 2020, https://bscw.5g-ppp.eu/pub/bscw.cgi/d367342/Networld2020%20SRIA%202020%20Final%20Version%202.2%20.pdf

[RaSa20] A. Rasheed, O. San and T. Kvamsdal, "Digital Twin: Values, Challenges and Enablers From a Modeling Perspective," in IEEE Access, vol. 8, pp. 21980-22012, 2020, doi: 10.1109/ACCESS.2020.2970143.

[SF SSCC] SF SSCC, Overview of Standards and Specifications relevant to Smart Cities (DRAFTv28: modified 20180419). See CEN/CENELEC pages https://www.cencenelec.eu/standards/Sectorsold/SmartLiving/smartcities/Pages/default.aspx and the provided document link ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/SmartLiving/City/SF-SSCC_Overview_of_Standards_for_SmartCities.pdf

[ZaAh19] Wazir Zada Khan, Ejaz Ahmed, Saqib Hakak, Ibrar Yaqoob, Arif Ahmed, "Edge Computing: A Survey", Elsevier, Future Generation Computer Systems, Volume 97, August 2019, Pages 219-235. see: https://www.sciencedirect.com/science/article/pii/S0167739X18319903

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Annex II Readme worksheet of the excel sheet presented in Section 5.2

This .xlsm file contains a few macros (MakeMindMap) in order to generate mindmap files.

Mind maps consist of a central node with a "tree structure" of tags attached. In the excel sheet, the hierarchical string of tags starts after column E.

The formatting for the mind map file fits the open source www.freeplane.org software, but also others like www.xmind.net can read it.

In the excel sheet, the hierarchical string of tags starts after column E and each row (until blank) creates a new branch on the mind map.

Sheet 1 in this excel file is this "ReadMe". Sheet "DefaultMM" is protected against changes because it is used to fill in default mind map initial text. Sheet "Organisations" is an example mind map for SmartCity relevant organisations, Sheet "References" is an incomplete list of references (not checked). Sheets Test1, Test2, Test3 are simple test sheets to allow users to try out different changes.

WARNING: in excel, be EXTREMELY careful (i.e. Backup before) when sorting/filtering/hiding data, to avoid scrambling rows.

The macros are started by setting the cursor anywhere inside any sheet with appropriate information, and typing CTRL-m

The name of that current sheet is used as the name of the created mind map file, ending with .mm, over-writing any previous one.

- The user is asked for some inputs when the macro runs:
- If debugging is enabled (not this version) then "DebugMsg depth" is requested (0 means no messages and is best choice. -999 outputs first 999 messages to a file .log. +999 prints to screen, so don't.)
- "First column to use" is asked for creating nodes or categories (tags) in the mind map, e.g. "j" for excel column J
- (Note that checking for tags (categories) stops at the first later column where a tag is empty in Row 1)
- The macro closes with the message "Done."

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

The formatting of the excel sheet of information must be:

- Row 1 contains headers describing each column. If a blank header is encountered it will stop processing of later columns.
- (That is a feature: you can insert a blank column to "truncate" the mind map so not all the depth is processed.)
- Any later rows which are "hidden" in the excel sheet will be skipped over during processing (nice for ignoring unneeded rows)
- Columns are A <optional index>, B <Name>, C <optional weblink>, D <should be full title>, E <optional abstract>, FGH etc <optional tags>
- Column A is optionally numbers, intended to remind of some consistent index of items, independent of re-sorting etc. It is not used in the mind map.
- Column B must contain a short Name or Title to show in a box in the mind map. Preferably a descriptive one!
- (If a blank is found, processing will stop This is a feature: you can insert a blank row in the middle of the list to truncate processing for the mind map.)
- Column C, if not blank, is used as a weblink to the document or organisation described. Links are NOT checked.
- Column D is currently not used in the mind map but SHOULD contain the full official name of the organisation of title of a document
- Column E must be blank OR contain an Abstract of the reference. It is shown in the mind map as a yellow button which shows the text when the mouse is moved over it.
- Column F and later columns are all user-defined, for making your mind map. DO NOT USE '&' IN Tag NAMES !
- Note that the mind map formatting looks logical if rows are ordered so tag combinations are without gaps i.e. If you have tags in ColF and ColG then a tag in ColI will not appear on the mind map at the same place as if you had put it in ColH.

Collaboration

The excel sheet can be a collaborative tool where new material can be added, sorted, hidden, abbreviated without deleting anything unnecessarily

- Columns F and later ("your tags") can be moved and re-sorted to create whatever desired hierarchy of tags is needed, without deleting any information.
- The ordering of the "tags" columns sets how the rows are grouped together under common categories: shifting ordering can make a big emphasis change.
- Rows (except Row 1) can be hidden so that only the rows of current interest are shown

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Known bugs

- Putting the character "&" inside of a tag (e.g. Water & Waste) crashes the mind map. Until the bug is fixed please use Water_and_Waste or some other way
- The algorithm to generate the mind map assumes that in the declared set of columns of categories (e.g. G-J) there will be no gaps i.e. If columns G and H have categories, and column "I" does not, then also J does not. There is no error message, and all nodes in the mind map are generated, but the arrangement is a bit mixed up. I am still considering what SHOULD the algorithm do, just jump across to the next category?

Licensing

"Creative Commons License and Disclaimer

The original source version v30 of this material is licensed under CCI4 (see below).

External contributions and distributions are welcomed. If you change the original version you MUST update the first line of this disclaimer and the title and central node of any exported mind map and keep this disclaimer.

This document is a living document with the aim to give an overview of useful information on work related to smart and sustainable cities, and to reference initiatives and standardization activities. Web links to original material are given, but there are no guarantees that the links are maintained or contain the same information as originally viewed. Categories and labels in the document are defined by you and previous users. Please consider the categories like the shelf areas in a library: you may not agree with the topics but at least similar things are nearby.

This work is licensed under a Creative Commons Attribution 4.0 International License https://creativecommons.org/licenses/by/4.0/legalcodehttps://creativecommons.org/licenses/by/4.0/legalcode and you are free to (a) share, copy and redistribute the material in any medium or format, and (b) adapt, remix, transform, and build upon the material for any purpose, even commercially, provided that you follow the following terms: (c) you must give appropriate credit, provide a link to the license, and indicate if changes were made in the licensed material, and you can do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use, (d) no additional legal terms or technological measures are added that legally restrict others from doing anything the license permits."

Annex III Template used for edge computing research/standardisation requirement

Please fill in the yellow field

X. Title of edge computing research/standardisation requirement

<<Title>>

X.1 Description of edge computing 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

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

- 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.

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Annex IV Mapping of SDOs specifications to AIOTI identified challenges

The following table provides a mapping of SDOs specifications to AIOTI identified challenges, so as to facilitate the identification of standardization gaps. The four first columns provide the source, title, url, and abstract of each standardization specification, whereas the last column maps each specification to the specific standardization challenges (sections) and labels, as identified by AIOTI in Sections 2, 3, and 4of this document.

Table 5: Mapping of SDOs specifications to AIOTI identified challenges

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
3GPP	3GPP TR 28.815 V17.0.0 (2021-12): Study on charging aspects of edge computing	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3758	The present document studies the charging aspects of Edge Computing based on architecture, procedures and information flows for enabling Edge Applications over 3GPP network as well as capabilities for 5GS to support edge computing. The investigation includes different charging scenarios with potential business requirements, alternative solutions with potential impact on charging architecture, charging functions and charging procedures.	scenarios, architectural considerations (Section 2.15.25)
3GPP	3GPP TR 23.803 V7.0.0 (2005-09): Evolution of policy control and charging	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=883	The document studies: a) the complete harmonization and merger of the policy control and flow based charging architecture and procedures; b) possible architectures and solutions for adding end-user subscription differentiation and general policy control aspects to the policy- and charging control; c) alternative solutions for binding bearers to services (provided today by the authorization token). This includes studying solutions for the network to control bearer usage by service flows.	policy control architecture (Section 2.11, 2.15.25)
3GPP	3GPP TR 23.748 V17.0.0 (2020-12): Study on enhancement of support for Edge Computing in 5G Core network (5GC)	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3622	The Technical Report studies and performs evaluations of potential architecture enhancements to support Edge Computing (EC) in the 5G Core network (5GC). Specifically, two objectives are included: a) to study the potential system enhancements for enhanced Edge Computing support, and b) to provide deployment guidelines for typical Edge Computing use cases, e.g. URLLC, V2X, AR/VR/XR, UAS, 5GSAT, CDN, etc.	use cases, 5G networks architecture (Section 2.2, 2.3)
3GPP	3GPP TR 26.803 V17.0.0 (2021-06): Study on 5G Media Streaming Extensions for Edge Processing	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3742	The document is a study of use cases for multimedia processing in the edge and the potential 5G media streaming architecture extensions to enable them.	use cases, architecture (Section 2.2, 2.3)
3GPP	3GPP TS 23.558 V17.2.0 (2021-12): Architecture for enabling Edge Applications	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3723	The document specifies the application layer architecture, procedures and information flows necessary for enabling edge applications over 3GPP networks. It includes architectural requirements for enabling edge applications, application layer architecture fulfilling the architecture requirements and procedures to enable the deployment of edge applications.	requirements, architecture, layer-oriented approach (Section 2.2, 2.3, 2.11, 2.13, 2.15)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
3GPP	3GPP TR 33.839 V17.0.0 (2021-12): Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC)	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3759	The document studies the security enhancements on the support for Edge Computing in the 5G Core network defined in TR 23.748, and application architecture for enabling Edge Applications defined in TR 23.758 and TS 23.558. Potential security requirements are provided and possible security enhancements to 5GS and edge application architecture are proposed that meet these security requirements.	security for 5G core (Section 2.2, 2.3, 2.13)
3GPP	3GPP TR 23.758 V17.0.0 (2019-12): Study on application architecture for enabling Edge Applications	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3614	The document is a technical report capturing the study on application architecture for enabling edge applications over 3GPP networks. The aspects of the study include identifying architecture requirements (e.g. discovery of edge services, authentication of the clients), supporting application layer functional model and corresponding solutions to enable the deployment of applications on the edge of 3GPP networks, with no impact to edge-unaware applications on the UE and minimal impact to edge-aware applications on the UE.	requirements, architecture, layer-oriented approach (Section 2.2, 2.3, 2.15)
3GPP	3GPP TR 28.814 V17.0.0 (2021-09): Study on enhancements of edge computing management	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3744	The document studies the potential use cases, requirements, and solutions for the management of edge computing architecture and requirement defined by TS 23.558 and TS 23.501. The document provides conclusions and recommendations on the next steps in the standardization.	use cases, requirements, architecture (Section 2.8, 2.13)
ETSI	ETSI GS MEC 001 V2.1.1 (2019-01): Multi-access Edge Computing (MEC); Terminology	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/001/02.01.01_60/gs_mec001v020101p.pdf	The document provides a glossary of terms relating to the conceptual, architectural and functional elements within the scope of work on Multi-access Edge Computing. The purpose of this glossary is to ensure that all terminology defined in the document is used in a consistent way by all ETSI MEC deliverables as well as in wider industry discussions on Multi-access Edge Computing	terminology (Section 2.2, 2.15.14)
ETSI	ETSI GS MEC 021 V2.1.1 (2020-01): Multi-access Edge Computing (MEC); Application Mobility Service API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/021/02.01.01_60/gs_mec021v020101p.pdf	The document provides a specification for end-to-end MEC application mobility support in a multi-access edge system. The document describes information flows, required information and operations. The document also specifies the necessary API with the data model and data format.	data-model, API, application mobility (Section 2.2, 2.11, 2.12)
ETSI	ETSI GR MEC 018 V1.1.1 (2017-10): Mobile Edge Computing (MEC); End to End Mobility Aspects	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/018/01.01.01_60/gr_mec018v010101p.pdf	The document focuses on mobility support provided by Mobile Edge Computing. It documents mobility use cases and end to end information flows to support UE and Application mobility for Mobile Edge Computing. When necessary, the document describes new mobile edge services or interfaces, as well as changes to existing mobile edge services or interfaces, data models, application rules and requirements. The document identifies gaps to support mobility that are not covered by existing WIs, documents these gaps and recommends the necessary normative work to close these gaps.	application rules, data-models, interfaces, service continuity (Section 2.2, 2.11, 2.12)
ETSI	ETSI GS MEC 030 V2.1.1 (2020-04): Multi-access Edge Computing (MEC); V2X Information Service API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.01.01_60/gs_mec030v020101p.pdf	The document focuses on a MEC Vehicular-to-Everything (V2X) Information Service (VIS), in order to facilitate V2X interoperability in a multi-vendor, multi-network and multi-access environment. It describes the V2X-related information flows, required information and operations. The document also specifies the necessary API with the data model and data format.	data-model, API, information service, V2X interoperability (Section 2.2, 2.11, 2.14, 2.15.15)
ETSI	ETSI GR MEC 017 V1.1.1 (2018-02): Mobile Edge Computing (MEC); Deployment of Mobile	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/017/01.01.01_60/gr_mec017v010101p.pdf	The document describes solutions that allow the deployment of MEC in an NFV environment. For each solution, it describes the motivation for the solution, its architectural impacts and the necessary work to enable it. The document provides recommendations as for where the specification work needs to be done.	virtualization infrastructure (Section 2.11, 2.12, 2.15.14)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
	Edge Computing in an NFV environment			
ETSI	ETSI GR MEC 027 V2.1.1 (2019-11): Multi-access Edge Computing (MEC); Study on MEC support for alternative virtualization technologies	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/027/02.01.01_60/gr_mec027v020101p.pdf	The document focuses on identifying the additional support that needs to be provided by MEC when MEC applications run on alternative virtualization technologies, such as containers. The document collects and analyses the use cases relating to the deployment of such alternative virtualization technologies, evaluates the gaps from the currently defined MEC functionalities, and identifies new recommendations. As ETSI NFV is also working on alternative virtualization technologies, the MEC work should be aligned with NFV where applicable. The document also recommends the necessary normative work to close any identified gaps.	virtualization technologies (Section 2.11, 2.12, 2.15.14)
ETSI	ETSI GS MEC 011 V2.2.1 (2020-12): Multi-access Edge Computing (MEC); Edge Platform Application Enablement	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/02.02.01_60/gs_mec011v020201p.pdf	The document focuses on the functionalities enabled via the Mp1 reference point between MEC applications and MEC platform, which allows these applications to interact with the MEC system. Service related functionality includes registration/deregistration, discovery and event notifications. Other functionality includes application availability, traffic rules, DNS and time of day. It describes the information flows, required information, and specifies the necessary operations, data models and API definitions.	data-models, (de)registration, discovery, API (Section 2.3, 2.15.8)
ETSI	ETSI GS MEC 012 V2.1.1 (2019-12): Multi-access Edge Computing (MEC); Radio Network Information API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/012/02.01.01_60/gs_mec012v020101p.pdf	The document focuses on the Radio Network Information MEC service. It describes the message flows and the required information. The present document also specifies the RESTful API with the data model.	data-models, API (Section 2.11)
ETSI	ETSI GS MEC 016 V2.2.1 (2020-04): Multi-access Edge Computing (MEC); Device application interface	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/016/02.02.01_60/gs_mec016v020201p.pdf	The document contains the API definition for the lifecycle management of user applications over the Mx2 reference point between the device application and the User Application LifeCycle Management Proxy (UALCMP) in the MEC system. The document covers the following lifecycle management operations: user application look-up, instantiation and termination. In addition, a mechanism is specified for the exchange of lifecycle management related information between the MEC system and the device application. The intended key audience of the present document are the application developers for the MEC system, since this API provides them with a method to manage their applications.	API, lifecycle management (Section 2.11, 2.12, 2.15.14)
ETSI	ETSI GS MEC 013 V2.1.1 (2019-09): Multi-access Edge Computing (MEC); Location API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/013/02.01.01_60/gs_mec013v020101p.pdf	The document focuses on the MEC Location Service. It describes the related application policy information including authorization and access control, information flows, required information and service aggregation patterns. The document specifies the necessary API with the data model and data format. It is to be noted that the actual data model and data format which is functional for the present API re-uses the definitions in "RESTful Network API for Zonal Presence" and "RESTful Network API for Terminal Location" published by the Open Mobile Alliance.	data-models, AAA, API, service aggregation (Section 2.11, 2.15.14)
ETSI	ETSI GS MEC 010-2 V2.1.1 (2019-11): Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01002/02.01.01_60/gs_mec01002v020101p.pdf	The document provides information flows for lifecycle management of applications running on a MEC host, and describes interfaces over the reference points to support application lifecycle management. It also describes application rules and requirements, application-related events, mobility handling and MEC service availability tracking. The document specifies the necessary data model, data format and operation format when applicable.	application rules, data-model, interface, lifecycle management (Section 2.11, 2.12, 2.15.14)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI GS MEC 002 V2.2.1 (2022-01): Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/02.02.01_60/gs_mec002v020201p.pdf	The document specifies the requirements for Multi-access Edge Computing with the aim of promoting interoperability and deployments. It contains normative and informative parts. The document also contains an annex describing example use cases and their technical benefits, for the purpose of deriving requirements.	requirements, interoperability (Section 2.1, 2.11)
ETSI	ETSI GR MEC 031 V2.1.1 (2020-10): Multi-access Edge Computing (MEC) MEC 5G Integration	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/031/02.01.01_60/gr_mec031v020101p.pdf	The document describes the key issues, solution proposals and recommendations for MEC integration into 3GPP 5G system. The following aspects are addressed: MEC System interactions with the 5G System, including the correspondence of the current MEC procedures to procedures available in 3GPP 5G system specification, options for the functional split between MEC and 5G Common API framework, realization of MEC as 5G Application Function(s). In addition the document addresses the scope and the preferred way of proceeding with the identified future technical work, as well as the identification of any missing 5G system functionality for MEC integration	MEC-5G common API (Section 2.11, 2.15.23)
ETSI	ETSI GR MEC 024 V2.1.1 (2019-11): Multi-access Edge Computing (MEC); Support for network slicing	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/024/02.01.01_60/gr_mec024v020101p.pdf	The document focuses on identifying the MEC functionalities to support network slicing. It first analyses the relevant network slicing concepts as defined by external organizations. Next, it collects relevant use cases based on the identified network slicing concepts when applied in the context of MEC and it evaluates the gaps from the defined MEC functional elements. When necessary, the document identifies new MEC functionalities or interfaces as well as changes to existing MEC functional elements, interfaces and requirements. It will also recommend the necessary normative work to close these gaps if identified.	network slicing (Section 2.2, 2.11, 2.12)
ETSI	ETSI GS MEC 009 V3.1.1 (2021-06): Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/009/03.01.01_60/gs_mec009v030101p.pdf	The document defines design principles for RESTful MEC service APIs, provides guidelines and templates for the documentation of these, and defines patterns of how MEC service APIs use RESTful principles.	RESTful MEC service APIs (Section 2.2, 2.11)
ETSI	ETSI GR MEC 035 V3.1.1 (2021-06): Multi-access Edge Computing (MEC); Study on Inter-MEC systems and MEC-Cloud systems coordination	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/035/03.01.01_60/gr_mec035v030101p.pdf	The document studies the applicability of MEC specifications to inter-MEC systems and MEC-Cloud systems coordination that supports e.g. application instance relocation, synchronization and similar functionalities. Another subject of this study is the enablement and/or enhancement of functionalities for application lifecycle management by third parties (e.g. application developers).	synchronization, instance relocation (Section 2.2, 2.11, 2.12)
ETSI	ETSI GS MEC 010-1 V1.1.1 (2017-10): Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System, host and platform management	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/01001/01.01.01_60/gs_mec01001v010101p.pdf	The document defines the management of the mobile edge system, mobile edge hosts and mobile edge platforms. This includes platform configuration, performance and fault management, application monitoring, remote service configuration and service control, information gathering regarding the platform features, available services, and available virtualised resources.	system management (Section 2.2, 2.11, 2.12, 2.15.14)
ETSI	ETSI GS MEC 015 V2.1.1 (2020-06): Multi-Access Edge Computing (MEC); Traffic Management APIs	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/015/02.01.01_60/gs_mec015v020101p.pdf	The document focuses on the Traffic Management multi-access edge service. It describes the related application policy information including authorization and access control, information flows, required information and service aggregation patterns. The document specifies the necessary API with the data model and data format.	data-model, traffic management, API (Section 2.2, 2.11, 2.12, 2.15.14)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI GS MEC 029 V2.2.1 (2022-01): Multi-access Edge Computing (MEC); Fixed Access Information API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/029/02.02.01_60/gs_mec029v020201p.pdf	The document describes a MEC service on Fixed Access Information for Fibre (e.g. G-PON, XG-PON, NG-PON2, XGS-PON), Cable (DOCSIS 3.1), xDSL, and Point-to-Point Fibre Ethernet access networks. It describes the information flows, required information, and as applicable, specifies the necessary operations, data model and data format. The present document also specifies the RESTful API.	wired communications (Section 2.2, 2.11, 2.12, 2.15.14)
ETSI	ETSI GS MEC-IEG 006 V1.1.1 (2017-01): Mobile Edge Computing; Market Acceleration; MEC Metrics Best Practice and Guidelines	https://www.etsi.org/deliver/etsi_gs/MEC-IEG/001_099/006/01.01.01_60/gs_mec-ieg006v010101p.pdf	The document describes various metrics which can potentially be improved through deploying a service on a MEC platform. Example use cases are used to demonstrate where improvements to a number of key performance indicators can be identified in order to highlight the benefits of deploying MEC for various services and applications. Furthermore, the document describes best practices for measuring such performance metrics and these techniques are further exemplified with use cases. Metrics described in the present document can be taken from service requirements defined by various organizations (e.g. 5G service requirements defined by Next Generation Mobile Networks (NGMN) or 3rd Generation Partnership Project (3GPP)). An informative annex is used to document such desired and/or achieved ranges of performance which could be referenced from the main body of the present document.	KPIs, metrics (Section 2.2, 2.10, 2.11, 2.12, 2.15.3, 2.15.14)
ETSI	ETSI GS MEC 005 V2.1.1 (2019-07): Multi-access Edge Computing (MEC); Proof of Concept Framework	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/005/02.01.01_60/gs_mec005v020101p.pdf	The document defines a framework to be used by ETSI ISG MEC to coordinate and promote multivendor Proofs of Concept (PoC) projects and MEC Deployment Trial (MDT) projects illustrating key aspects of MEC technology. Proofs of Concept are an important tool to demonstrate the viability of a new technology during its early days and or pre-standardization phase. MDTs are seen as the next step of PoC to demonstrate the viability of MEC in a commercial trial/deployment and to provide feedback to the standardization work.	PoC/trials framework (Section 2.2, 2.11)
ETSI	ETSI GR MEC-DEC 025 V2.1.1 (2019-06): Multi-access Edge Computing (MEC); MEC Testing Framework	https://www.etsi.org/deliver/etsi_gr/MEC-DEC/001_099/025/02.01.01_60/gr_mec-dec025v020101p.pdf	The document lists the functionalities and capabilities required by a MEC compliant implementation. In addition, the document specifies a testing framework defining a methodology for development of interoperability and/or conformance test strategies, test systems and the resulting test specifications for MEC standards. In additional, the testable requirements are listed and prioritized.	testing framework (Section 2.2, 2.10, 2.11, 2.15.3)
ETSI	ETSI GS MEC-DEC 032-1 V2.1.1 (2020-12): Multi-access Edge Computing (MEC); API Conformance Test Specification; Part 1: Test Requirements and Implementation Conformance Statement (ICS)	https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03201/02.01.01_60/gs_mec-dec03201v020101p.pdf	Based on the testing methodology guidelines and framework specified in ETSI GR MEC-DEC 025, the document specifies part 1 of a multi-part deliverable test specification. Part 1 (the present document) provides the Test requirements and Implementation Conformance Statement (ICS) for: Application Package Management and Application Lifecyle Management as specified in ETSI GS MEC 10-2; MEC Application Enablement as specified in ETSI GS MEC 011; and the MEC service APIs.	testing framework (Section 2.2, 2.10, 2.11, 2.15.3)
ETSI	ETSI GS MEC-DEC 032-2 V2.1.1 (2020-12): Multi-access Edge Computing (MEC); API Conformance Test	https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03202/02.01.01_60/gs_mec-	Based on the testing methodology guidelines and framework specified in ETSI GR MEC-DEC 025, the document specifies part 2 of a multi-part deliverable test specification for the MEC service APIs (currently ETSI GS MEC 012, ETSI GS MEC 013, ETSI GS MEC 014, ETSI GS MEC 015, ETSI GS MEC 016, ETSI GS MEC 021 and ETSI GS MEC 029) and the MEC Application Enablement API (ETSI GS MEC 011). The document includes the Test Suite Structure (TSS) and	testing framework (Section 2.2, 2.10, 2.11, 2.15.3)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
	Specification; Part 2: Test Purposes (TP)	dec03202v020101p.pdf	Test Purposes (TPs) using the standardized notation Test Description Language - Test Objectives extension (TDL_TO).	
ETSI	ETSI GS MEC-DEC 032-3 V2.1.1 (2020-12): Multi-access Edge Computing (MEC); API Conformance Test Specification; Part 3: Abstract Test Suite (ATS)	https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03203/02.01.01_60/gs_mec-dec03203v020101p.pdf	Based on the testing methodology guidelines and framework specified in ETSI GR MEC-DEC 025, the document specifies part 3 of a multi-part deliverable on conformance test specification. Part 3 provides the Abstract Test Suites (ATS) in TTCN-3 and the Robot Framework for the MEC Application Enablement API specified in ETSI GS MEC 011 and the MEC service APIs.	testing framework (Section 2.2, 2.10, 2.11, 2.15.3)
ETSI	ETSI GR MEC 022 V2.1.1 (2018-09): Multi-access Edge Computing (MEC); Study on MEC Support for V2X Use Cases	https://www.etsi.org/deliver/etsi_gr/MEC/001_099/022/02.01.01_60/gr_mec022v020101p.pdf	The document focuses on identifying the MEC features to support V2X applications. It collects and analyses the relevant V2X use cases (including the findings from external organizations), evaluates the gaps from the defined MEC features and functions, and identifies the new requirements including new features and functions. When necessary, this may include identifying new multi-access edge services or interfaces, as well as changes to existing MEC services or interfaces, data models, application rules and requirements. It will also recommend the necessary normative work to close these gaps if identified.	applications rules, requirements, data-models (Section 2.15.14, 2.15.15)
ETSI	ETSI GS MEC 003 V2.2.1 (2020-12): Multi-access Edge Computing (MEC); Framework and Reference Architecture	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.02.01_60/gs_mec003v020201p.pdf	The document provides a framework and reference architecture for Multi-access Edge Computing that describes a MEC system that enables MEC applications to run efficiently and seamlessly in a multi-access network. The document also describes the functional elements and the reference points between them, and a number of MEC services that comprise the solution. It finally presents a number of key concepts related to the multi-access edge architecture.	reference architecture (Section 2.2, 2.11, 2.12, 2.15.14)
ETSI	ETSI GS MEC 014 V2.1.1 (2021-03): Multi-access Edge Computing (MEC); UE Identity API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/014/02.01.01_60/gs_mec014v020101p.pdf	The present document focuses on the UE Identity functionality. It describes the related application policy information (including authorization, access control and traffic rule pattern format), information flows, required information and service aggregation patterns. The present document specifies the necessary API, data model and data format, considering existing API(s) if applicable.	AAA (Section 2.11, 2.15.9)
ETSI	ETSI GS MEC 026 V2.1.1 (2019-01): Multi-access Edge Computing (MEC); Support for regulatory requirements	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/026/02.01.01_60/gs_mec026v020101p.pdf	The document focuses on the support of regulatory requirements for Lawful Interception (LI) and Retained Data (RD) when implementing MEC into the network. It describes the problems, constraints, interfaces and additional capabilities needed for the different deployment scenarios, to ensure full support of LI & RD regulatory requirements when implementing MEC.	regulatory requirements (Section 2.11, 2.15.3)
ETSI	ETSI GS MEC 028 V2.2.1 (2021-07): Multi-access Edge Computing (MEC); WLAN Access Information API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/028/02.02.01_60/gs_mec028v020201p.pdf	The document focuses on the WLAN Access Information MEC service. It describes the message flows and the required information. The document also specifies the RESTful API with the data model.	WLAN Access Information (Section 2.2, 2.11)
ETSI	ETSI GS MEC-IEG 004 V1.1.1 (2015-11): Mobile-Edge Computing (MEC); Service Scenarios	https://www.etsi.org/deliver/etsi_gs/MEC-IEG/001_099/004/01.01.01_60/gs_mec-ieg004v010101p.pdf	The document introduces a number of service scenarios that would benefit from the introduction of Mobile-Edge Computing (MEC) technology. The focus of the document is to introduce or provide a non-exhaustive set of service scenarios. It is not the intent nor does the present document provide any requirements.	scenarios (Section 2.2)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC TR 63283-2 ED1: Industrial-process measurement, control and automation – Smart Manufacturing – Part 2: Use cases	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,103914	The document presents Use cases that describe IIoT platform and edge device usage with the "roles" around them e.g., in the use case cluster "IT-infrastructure and software", use case "Device configuration".	use cases, distributed architecture (Section 2.1, 2.2, 2.15.5, 2.15.6)
IEC	IEC TR 63283-3 ED1: Industrial-process measurement, control and automation – Smart Manufacturing – Part 3: Challenges for Cybersecurity	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,103915	The document addresses roles of IIoT platforms and edge computing in the context of architecture-related transition from classical automation pyramid to automation networks, particularly related to security issues.	distributed architectures, distributed security (Section 2.1, 2.2, 2.3, 2.15.10, 2.15.6)
IEC	IEC TR 63283-5 ED1: Industrial-process measurement, control and automation – Smart Manufacturing – Part 5: Market and innovation trends analysis	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,107051	Industrial IoT, (I)IoT devices, Edge, Cloud, 6G and AI are the key topics and sections, including edge management, edge providers etc. Standardization needs are addressed.	distributed architectures, digital twin (Section 2.1, 2.2, 2.3, 2.4, 2.5, 2.6)
IEC	IEC TR 63283-4 WD : Industrial-process measurement, control and automation – Smart Manufacturing – Part 4: New technologies	https://www.iec.ch/ords/f?p=103:23:523507370720228:::FSP_ORG_ID,FSP_LANG_ID:1250,25	This document is a "Smart manufacturing trend analysis". Some of the new technologies are related to AI, Edge computing, Cloud technology, Digital twin, New communication protocols, 5G, TSN, Big data and data analytics, IoT and IIoT, Privacy technology, etc. Each chapter has a subchapter on "Technology description", "Use case analysis" and "Standardization needs".	distributed architectures, digital twin (Section 2.1, 2.2, 2.7, 2.13, 2.15.7, 2.15.10, 2.15.22, 2.15.23, 2.15.24)
IEEE	IEEE 802.1AC-2016: IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Service Definition	https://standards.ieee.org/standard/802_1AC-2016.html	The MAC Service and the Internal Sublayer Service (ISS) are defined in this standard. This standard specifies media-dependent convergence functions that map IEEE 802(R) MAC interfaces to the ISS. The MAC Service is derived from the ISS.	data and infrastructure interoperability (Section 2.1)
IEEE	IEEE 802d-2017: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 1: Allocation of Uniform Resource Name (URN) Values in IEEE 802(R) Standards	https://standards.ieee.org/standard/802d-2017.html	How Uniform Resource Name (URN) values are allocated in IEEE 802(R) standards is described in this amendment to IEEE Std 802(R)-2014.	architecture, devices management (Section 2.1, 2.15.1)
IEEE	IEEE 1934-2018: IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing	https://standards.ieee.org/standard/1934-2018.html	OpenFog Consortium--OpenFog Reference Architecture for Fog Computing is adopted by this standard. OpenFog Reference Architecture [OPFRA001.020817] is a structural and functional prescription of an open, interoperable, horizontal system architecture for distributing computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum of communicating, computing, sensing and actuating entities. It encompasses various approaches to disperse Information Technology (IT), Communication Technology (CT) and Operational	reference architecture (Section 2.1)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
			Technology (OT) Services through information messaging infrastructure as well as legacy and emerging multi-access networking technologies	
IEEE	IEEE 2413-2019: IEEE Standard for an Architectural Framework for the Internet of Things (IoT)	https://standards.ieee.org/standard/2413-2019.html	An architecture framework description for the Internet of Things (IoT) which conforms to the international standard ISO/IEC/IEEE 42010:2011 is defined. The architecture framework description is motivated by concerns commonly shared by IoT system stakeholders across multiple domains (transportation, healthcare, Smart Grid, etc.). A conceptual basis for the notion of things in the IoT is provided and the shared concerns as a collection of architecture viewpoints is elaborated to form the body of the framework description.	reference architecture (Section 2.1)
IEEE	IEEE 802.1Q-2014: IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks	https://standards.ieee.org/standard/802_1Q-2014.html	This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms.	infrastructure interoperability (Section 2.1)
IEEE	IEEE 802.1BR-2012: IEEE Standard for Local and metropolitan area networks--Virtual Bridged Local Area Networks--Bridge Port Extension	https://standards.ieee.org/standard/802_1BR-2012.html	This standard specifies the operation of Bridge Port Extenders, including management, protocols, and algorithms. Bridge Port Extenders operate in support of the MAC Service by Extended Bridges.	orchestration, interoperability (Section 2.1)
IEEE	IEEE 802-2014: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture	https://standards.ieee.org/standard/802-2014.html	This standard provides an overview to the family of IEEE 802® standards. It describes the reference models for the IEEE 802 standards and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of IEEE 802 MAC addresses; it provides a standard for identification of public, private, prototype, and standard protocols; it specifies an object identifier hierarchy used within IEEE 802 for uniform allocation of object identifiers used in IEEE 802 standards; and it specifies a method for higher layer protocol identification.	architecture, orchestration, interoperability (Section 2.1)
IEEE	IEEE 802.1AB-2016: IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery	https://standards.ieee.org/standard/802_1AB-2016.html	This document defines a protocol and a set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802(R) LANs.	service discovery (Section 2.1, 2.13, 2.15.8)
IEEE	IEEE 802.1AS-2020: IEEE Standard for Local and Metropolitan Area Networks--Timing and Synchronization for Time-Sensitive Applications	https://standards.ieee.org/standard/802_1AS-2020.html	Protocols, procedures, and managed objects for the transport of timing over local area networks are defined in this standard. It includes the transport of synchronized time, the selection of the timing source (i.e., best master), and the indication of the occurrence and magnitude of timing impairments (i.e., phase and frequency discontinuities).	responsive connectivity (Section 2.1)
IEEE	IEEE 802.1CB-2017: IEEE Standard for Local and metropolitan area networks--Frame Replication and Elimination for Reliability	https://standards.ieee.org/standard/802_1CB-2017.html	This standard specifies procedures, managed objects, and protocols for bridges and end systems that provide identification and replication of packets for redundant transmission, identification of duplicate packets, and elimination of duplicate packets. It is not concerned with the creation of the multiple paths over which the duplicates are transmitted.	transfer, responsive connectivity (Section 2.1, 2.15.9)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
IEEE	IEEE 802.1CM-2018: IEEE Standard for Local and metropolitan area networks -- Time-Sensitive Networking for Fronthaul	https://standards.ieee.org/standard/802_1CM-2018.html	This standard defines profiles that select features, options, configurations, defaults, protocols, and procedures of bridges, stations, and LANs that are necessary to build networks that are capable of transporting fronthaul streams, which are time sensitive.	responsive connectivity (Section 2.1)
IEEE	IEEE 802.1AR-2018: IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity	https://standards.ieee.org/standard/802_1AR-2018.html	This document presents a Secure Device Identifier (DevID), an ID cryptographically bound to a device and supports authentication of the device's identity. An Initial Device Identifier (IDevID) provided by the supplier of a device can be supplemented by Local Device Identifiers (LDevIDs) facilitating enrollment (provisioning of authentication and authorization credentials) by local network administrators.	devices management, AAA (Section 2.1, 2.15.8)
IEEE	IEEE 802.1AE-2018: IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security	https://standards.ieee.org/standard/802_1AE-2018.html	The document describes how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.	connectivity, interoperability, distributed security (Section 2.1, 2.15.16)
IEEE	IEEE 7005-2021: IEEE Standard for Transparent Employer Data Governance	https://standards.ieee.org/standard/7005-2021.html	Specific methodologies to help employers in accessing, collecting, storing, utilizing, sharing, and destroying employee data are described in this standard. Specific metrics and conformance criteria regarding these types of uses from trusted global partners and how third parties and employers can meet them are provided in this standard. Certification processes, success criteria, and execution procedures are not within the scope of this standard.	legal/ethical/ social adaption, KPIs, metrics, access, share, store (Section 2.1, 2.14, 2.15.10, 2.15.11)
IEEE	IEEE 802.1X-2020: IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control	https://standards.ieee.org/standard/802_1X-2020.html	Port-based network access control allows a network administrator to restrict the use of IEEE 802(R) LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE(TM) MAC Security.	network management, security and privacy (Section 2.1)
IEEE	IEEE 802.1AX-2020: IEEE Standard for Local and metropolitan area networks -- Link Aggregation	https://standards.ieee.org/standard/802_1AX-2020.html	Link Aggregation allows parallel point-to-point links to be used as if they were a single link and also supports the use of multiple links as a resilient load-sharing interconnect between multiple nodes in two separately administered networks. This standard defines a MAC-independent Link Aggregation capability and provides general information relevant to specific MAC types.	data and infrastructure interoperability (Section 2.1)
IEEE/ ISO/ IEC	IEEE/ISO/IEC 8802-1Q-2020: IEEE/ISO/IEC International Standard - Telecommunications and exchange between information technology systems--Requirements for local and metropolitan area networks--Part 1Q: Bridges and bridged networks	https://standards.ieee.org/standard/8802-1Q-2020.html	This standard specifies how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms.	requirements, orchestration, interoperability (Section 2.1, 2.15.1, 2.15.2)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
IEEE/ ISO/ IEC	IEEE/ISO/IEC 8802-1BA-2016: ISO/IEC/IEEE International Standard - Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 1BA: Audio video bridging (AVB) systems	https://standards.ieee.org/standard/8802-1BA-2016.html	Profiles that select features, options, configurations, defaults, protocols and procedures of bridges, stations and LANs that are necessary to build networks that are capable of transporting time-sensitive audio and/or video data streams are defined in this standard.	requirements, responsive connectivity (Section 2.1)
IEEE/ ISO/ IEC	IEEE/ISO/IEC 8802-1BR-2016: ISO/IEC/IEEE International Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 1BR: Virtual bridged local area networks — Bridge port extension	https://standards.ieee.org/standard/8802-1BR-2016.html	This standard specifies the operation of Bridge Port Extenders, including management, protocols, and algorithms. Bridge Port Extenders operate in support of the MAC Service by Extended Bridges.	requirements, responsive connectivity (Section 2.1)
IEEE/ ISO/ IEC	IEEE/ISO/IEC 8802-1AE-2020: IEEE/ISO/IEC International Standard - Telecommunications and exchange between information technology systems--Requirements for local and metropolitan area networks--Part 1AE:Media access control (MAC) security	https://standards.ieee.org/standard/8802-1AE-2020.html	How all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.	distributed security (Section 2.1)
IETF	draft-ietf-mops-streaming-opcons-08: Operational Considerations for Streaming Media	https://datatracker.ietf.org/doc/draft-ietf-mops-streaming-opcons/	This document provides an overview of operational networking issues that pertain to quality of experience when streaming video and other high-bitrate media over the Internet.	requirements (Section 2.2)
IETF	draft-contreras-alto-service-edge-03: Use of ALTO for Determining Service Edge	https://datatracker.ietf.org/doc/draft-contreras-alto-service-edge/	Service providers are starting to deploy and interconnect computing capabilities across the network for hosting network functions and applications. In distributed computing environments, both computing and topological information are necessary in order to determine the more convenient infrastructure where to deploy such a service or application. This document proposes an initial approach towards the use of ALTO to provide	seamless MEC deployment/ transition (Section 2.2, 2.11, 2.12)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
			such information and assist the selection of appropriate deployment locations for services and applications.	
IETF	draft-ietf-mops-ar-use-case-03: Media Operations Use Case for an Augmented Reality Application on Edge Computing Infrastructure	https://datatracker.ietf.org/doc/draft-ietf-mops-ar-use-case/	A use case describing transmission of an application on the Internet that has several unique characteristics of Augmented Reality (AR) applications is presented for the consideration of the Media Operations (MOPS) Working Group.	use cases, distributed architecture, edge-specific constraints, computing continuum (Section 2.2, 2.12)
ISO/ IEC	ISO/IEC AWI 5392: Information technology — Artificial intelligence — Reference architecture of knowledge engineering	https://www.iso.org/standard/81228.html	This document defines a reference architecture of Knowledge Engineering (KE) in Artificial Intelligence (AI). The reference architecture describes KE roles, activities, constructional layers, components and their relationships among themselves and other systems from systemic user and functional views. This document also provides a common KE vocabulary by defining KE terms	reference architecture, distributed and explainable AI (Section 2.13)
ISO/ IEC	ISO/IEC CD 30149 (2022): IoT Trustworthiness principles	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104432	This document provides principles for IoT trustworthiness based on ISO/IEC 30141 – IoT Reference Architecture. The current content and scope is based on the premise that Internet of Things is an application and can use a software development lifecycle as a means to address trust in IoT.	trustworthiness (Section 2.3, 2.15.2)
ISO/ IEC	ISO/IEC PWI JTC1-SC41-8: Internet of Things (IoT) - Behavioral and policy interoperability	https://www.iec.ch/dyn/www/f?p=103:38:17567799116988::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108353	Based on ISO/IEC 21823-1, this document provides the basic concepts for IoT systems and digital twin systems behavioral and policy interoperability. This includes - requirements - guidance on how to identify points of interoperability - guidance on how to express behavioral and policy information on capabilities - guidance on how to achieve trustworthiness interoperability, and - use cases and examples .	interoperability on policy level (Section 2.15.1)
ISO/ IEC	ISO/IEC 21823-3:2021: Internet of Things (IoT) - Interoperability for IoT systems - Part 3: Semantic interoperability	https://webstore.iec.ch/publication/61088	ISO/IEC 21823-3:2021 provides the basic concepts for IoT systems semantic interoperability, as described in the facet model of ISO/IEC 21823-1, including: (1) requirements of the core ontologies for semantic interoperability; (2) best practices and guidance on how to use ontologies and to develop domain-specific applications, including the need to allow for extensibility and connection to external ontologies; (3) cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies; (4) relevant IoT ontologies along with comparative study of the characteristics and approaches in terms of modularity, extensibility, reusability, scalability, interoperability with upper ontologies, and so on; and (5) use cases and service scenarios that exhibit necessities and requirements of semantic interoperability.	semantic interoperability (Section 2.15.1)
ISO/ IEC	ISO/IEC 38505-1:2017: Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data	https://www.iso.org/standard/56639.html	ISO/IEC 38505-1:2017 provides guiding principles for members of governing bodies of organizations on the effective, efficient, and acceptable use of data within their organizations by - applying the governance principles and model of ISO/IEC 38500 to the governance of data, - assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organization's governance of data, - informing and guiding governing bodies in the use and protection of data in their organization, and - establishing a vocabulary for the governance of data.	interoperability on policy level, data governance interoperability (Section 2.15.1, 2.15.2)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC	ISO/IEC TS 27570:2021: Privacy protection — Privacy guidelines for smart cities	https://www.iso.org/standard/71678.html	The document takes a multiple agency as well as a citizen-centric viewpoint. It provides guidance on: smart city ecosystem privacy protection; how standards can be used at a global level and at an organizational level for the benefit of citizens; and processes for smart city ecosystem privacy protection.	models, privacy (Section 2.15.1, 2.15.2, 2.15.4, 2.15.10)
ISO/ IEC	ISO/IEC JTC1-SC41-257 ED1: Internet of Things (IoT) – Device model for IoT device interoperability	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108033	This document defines a structured description method, which describes the functionalities of IoT devices, including what functionalities an IoT device can provide, and how to use the functionalities of IoT device. In details, the contents: 1. Define concept of IoT Device Model: what is IoT Device Model, and how it works with underlying IoT communication protocols; 2. Specify structure of IoT Device Model: define the elements of Status, Profile, and Resource; Furthermore, specify the structure of Resource element, to describe the functionalities of IoT devices through Property, Service, and Event; 3. Specify construction method of IoT Device Model: how to build IoT device functionalities based on IoT Device Model; 4. Describe the device interoperability based on the IoT Device Model: IoT Device Model discovery, remote query, remote controlling, subscription and data uploading.	device model, interoperability (Section 2.15.2, 2.15.16)
ISO/ IEC	ISO/IEC JTC1-SC41-262 ED1: Internet of Things (IoT) – Functional architecture for resource ID interoperability	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108552	This document specifies functional requirements and architecture about the following items for resource interoperability among heterogeneous IoT platforms (e.g., oneM2M, GS1 Oliot, IBM Watson IoT, OCF IoTivity, and FIWARE, etc.) through the conversion of resource identifiers (IDs) and paths (e.g., uniform resource identifier (URI)): Requirements for interoperability of resource IDs in the heterogeneous IoT platforms; Functional architecture for converting IDs and paths of resources on heterogeneous platforms; and, Functional architecture for mapping and managing resource IDs among heterogeneous platforms.	platfom interoperability (Section 2.15.2, 2.15.5)
ISO/ IEC	ISO/IEC TS 27110:2021: Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines	https://www.iso.org/standard/72435.html	This document specifies guidelines for developing a cybersecurity framework. It is applicable to cybersecurity framework creators regardless of their organizations' type, size or nature.	non-functional properties, security and privacy (Section 2.15.4)
ISO/ IEC	ISO/IEC 30147:2021: Information technology — Internet of things — Methodology for trustworthiness of IoT system/service	https://www.iso.org/standard/53267.html	This document provides system life cycle processes to implement and maintain trustworthiness in an IoT system or service by applying and supplementing ISO/IEC/IEEE 15288:2015. The system life cycle processes are applicable to IoT systems and services common to a wide range of application areas.	non-functional properties, trustworthiness (Section 2.15.4)
ISO/ IEC	ISO/IEC 27032:2012: Information technology — Security techniques — Guidelines for cybersecurity	https://www.iso.org/standard/44375.html	ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides: an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.	non-functional properties, trustworthiness, security/privacy models (Section 2.15.4, 2.15.10)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC	ISO/IEC TR 27550:2019: Information technology — Security techniques — Privacy engineering for system life cycle processes	https://www.iso.org/standard/72024.html	This document provides privacy engineering guidelines that are intended to help organizations integrate recent advances in privacy engineering into system life cycle processes. It describes: the relationship between privacy engineering and other engineering viewpoints (system engineering, security engineering, risk management); and privacy engineering activities in key engineering processes such as knowledge management, risk management, requirement analysis, and architecture design.	non-functional properties, trustworthiness, security/privacy models (Section 2.15.4, 2.15.10)
ISO/ IEC	ISO/IEC TR 30164:2020 : Internet of Things (IoT) - Edge computing	https://webstore.iec.ch/publication/62522	The document describes the common concepts, terminologies, characteristics, use cases and technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware/software optimization) of edge computing for IoT systems applications. This document is also meant to assist in the identification of potential areas for standardization in edge computing for IoT. The document describes several use cases from different domains: Smart elevator, Smart video monitoring, Intelligent transport systems, Process control in smart factory, Virtual power plant, Automated crop monitoring and management system, Smart lightning system.	use cases, terminology (Section 2.2, 2.15.1, 2.15.14, 2.15.18)
ISO/ IEC	ISO/IEC PWI JTC1-SC41-7: Digital Twin – Maturity model	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108352	This document provides a standardized generic Digital Twin maturity model, definition of assessment indicators, guidance for a maturity assessment, and other practical classifications of Digital Twin capabilities, etc.	model, maturity assessment, digital twin (Section 2.8, 2.10, 2.15.1, 2.15.16)
ISO/ IEC	ISO/IEC PWI JTC1-SC41-5: Digital Twin - Reference Architecture	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,20,104896	This document provides an overview of Digital Twin, describes the capabilities, range, characteristics and requirements, and establishes a well-defined conceptual model, reference model and reference architectural views including usage view, functional view, and network view. This document is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).	reference architecture, digital twin (Section 2.8, 2.15.21)
ISO/ IEC	ISO/IEC 30173 ED1: Digital Twin - Concepts and terminology	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104883	This document establishes terminology for Digital Twin (DT) and describes concepts in the field of Digital Twin, including the terms and definitions of Digital Twin, concepts of Digital Twin (e.g., Digital Twin ecosystem, lifecycle process for Digital Twin, and classifications of Digital Twin), Functional view of Digital Twin and Digital Twin stakeholders.	terminology, distributed architectrue, interoperability, digital twin (Section 2.8, 2.15.22)
ISO/ IEC	ISO/IEC TR 30172 ED1: Digital Twin - Use cases	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104881	This document provides a collection of representative use cases of Digital Twin applications in a variety of domains.	use cases, distributed architecture, interoperability, digital twin (Section 2.8, 2.15.22)
ISO/ IEC	ISO/IEC PWI JTC1-SC41-6 : Guidance for IoT and Digital Twin use cases	https://www.iec.ch/ords/f?p=103:38:523507370720228:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PR	The document defines a conceptual model for the building of use cases; specifies a use case template ontology, i.e. vocabulary as well as conventions for describing and representing use case contents; provides guidance on building use case templates and on extending a use case ontology to cover the targeted standard; provides examples of use case templates and use	use cases, digital twin (Section 2.8, 2.15.22)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
		OJECT_ID:20486,20,104897	cases; and specifies an implementation scheme that will allow use cases to be stored and shared in a repository.	
ISO/ IEC/ IEEE	ISO/IEC/IEEE DIS 24641: Systems and Software engineering — Methods and tools for model-based systems and software engineering	https://www.iso.org/standard/79111.html	This International Standard, within the context of methods and tools for MBSSE: (1) Provides terms and definitions related to MBSSE; (2) Defines MBSSE-specific processes for model-based systems and software engineering; the processes are described in terms of purpose, inputs, tasks, and outcomes; (3) Defines methods to support the defined tasks of each process; and (4) Defines tool capabilities to automate/semi-automate tasks or methods.	models (Section 2.15.10)
ITU-T	Y.RA-FML : Requirements and reference architecture of IoT and smart city & community service based on federated machine learning	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16676	This Recommendation defines the reference architectural framework and requirements of IoT and Smart City & Community services based on federated machine learning.	requirements, reference architecture, access, share, store, threats, digital twin, federated learning (Section 2.2, 2.13, 2.15.18, 2.15.20, 2.15.24)
ITU-T	Y.CDML-arc : Reference architecture of collaborative decentralized machine learning for intelligent IoT services	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16865	This recommendation aims to propose the reference architecture of collaborative decentralized machine learning for intelligent IoT services.	reference architecture, distributed AI, federal learning, performance acceleration (Section 2.2, 2.13, 2.6, 2.15.6, 2.15.20, 2.15.24)
ITU-T	Y.dec-IoT-arch : Decentralized IoT communication architecture based on information centric networking and blockchain	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14650	This Recommendation describes a decentralized, IoT communication reference architecture based on ICN and blockchain.	reference architecture, distributed architecture, non-repudiation, DLT (Section 2.2, 2.15.24)
ITU-T	Y.AI-DECCS : Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16856	This Recommendation specifies Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city.	federated learning, distributed AI (Section 2.2, 2.3, 2.13, 2.15.4, 2.15.20, 2.15.24)
ITU-T	Y.IoT-DES-fr : Framework of decentralized service by using DLT and edge computing technologies for IoT devices	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16855	This draft Recommendation introduces a decentralized service by using DLT and edge computing technologies for IoT devices, and analyses its characteristics and high-level requirements, and provides its functional framework and relevant common capabilities, functionalities and general procedures.	distributed architecture, non-repudiation, DLT, security (Section 2.2, 2.3, 2.15.18, 2.15.24)
ITU-T	Y.scdt-reqts: Requirements and capabilities of a digital twin system for smart cities	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16396	This Recommendation provides concept of digital twin federation and defines requirements for digital twin federation in smart cities and communities.	requirements, distributed architecture, service discovery, digital twin (Section 2.2, 2.3, 2.15.5, 2.15.18)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

SDO	Specification			Relevant AIOTI identified challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	Y.IoT-DSE-arc : Reference architecture of service exposure for decentralized services for IoT applications	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16862	This draft Recommendation introduces a concept of service exposure for decentralized services (DSE) for IoT applications, analyses its common characteristics and high-level requirements, and provides a reference architecture of DSE and relevant common capabilities.	reference architecture, service discovery, Interfaces & APIs, federation, computing continuum (Section 2.2, 2.3, 2.15.5, 2.15.19)
oneM2M	oneM2M TR-0052 V0.13.1 (2020-9-28): Study on Edge and Fog Computing in oneM2M systems	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32633	The document studies how to Edge and Fog computing leverage in oneM2M architecture. It also includes architectural and gap analysis, including key issues and solutions. Based on the result of the study, it will identify possible advanced features and enhancements which the next oneM2M release(s) could support.	oneM2M architecture, edge and fog (Section 2.15.14, 2.15.23)
W3C	TR/2020/REC-wot-architecture-20200409: Web of Things (WoT) Architecture	https://www.w3.org/TR/2020/REC-wot-architecture-20200409/	The document describes the abstract architecture for the W3C Web of Things. This architecture is based on a set of requirements that were derived from use cases for multiple application domains, both given in this document. A set of modular building blocks are also identified whose detailed specifications are given in other documents. This document describes how these building blocks are related and work together. The WoT abstract architecture defines a basic conceptual framework that can be mapped onto a variety of concrete deployment scenarios, several examples of which are given. However, the abstract architecture described in this specification does not itself define concrete mechanisms or prescribe any concrete implementation.	distributed architecture, edge-specific constraints, computing continuum (Section 2.14, 2.15.2, 2.15.6, 2.15.21)
W3C	TR/2021/WD-wot-discovery-20210602: Web of Things (WoT) Discovery	https://www.w3.org/TR/wot-discovery/	The document presents a process for WoT discovery with two phases: introduction and exploration. The Introduction phase leverages existing discovery mechanisms but does not directly expose metadata; they are simply used to discover Exploration services, which provide metadata but only after secure authentication and authorization. This document normatively defines two Exploration services, one for WoT Thing self-description with a single WoT Thing Description and a searchable WoT Thing Description Directory service for collections of Thing Descriptions. A variety of Introduction services are also described and where necessary normative definitions are given to support them.	things discovery, digital twin (Section 2.15.8)
W3C	TR/2020/REC-wot-thing-description-20200409: Web of Things (WoT) Thing Description	https://www.w3.org/TR/2020/REC-wot-thing-description-20200409/	The document describes a formal model and a common representation for a Web of Things (WoT) Thing Description. A Thing Description describes the metadata and interfaces of Things, where a Thing is an abstraction of a physical or virtual entity that provides interactions to and participates in the Web of Things. Thing Descriptions provide a set of interactions based on a small vocabulary that makes it possible both to integrate diverse devices and to allow diverse applications to interoperate. Thing Descriptions, by default, are encoded in a JSON format that also allows JSON-LD processing. The latter provides a powerful foundation to represent knowledge about Things in a machine-understandable way. A Thing Description instance can be hosted by the Thing itself or hosted externally when a Thing has resource restrictions (e.g., limited memory space) or when a Web of Things-compatible legacy device is retrofitted with a Thing Description.	model, ontologies, interoperability on meta-data, interoperability (Section 2.8, 2.9, 2.15.23)

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

Annex V Editors and Contributors to this Deliverable

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

Editors:

- Georgios Karagiannis, Huawei
- Orfeas Voutyras, Institute of Communication and Computer Systems (ICCS)/ National Technical University of Athens (NTUA)

Authors and key contributors:

Name	Company/Organisation
Tom de Block	Navigio
David Boswarthick	ETSI
Marco Carugi	Huawei
Andre Duarte	Ubiwhere
Stephan Fertig	Panasonic
Damir Filipovic	AIOTI Secretary General
Ronal Freund	Fraunhofer HHI
Lindsay Frost	NEC
Nikolaos Giannakakos	Unisystems
Sascha Hackel	Fraunhofer FOKUS
Asbjørn Hovstø	Hafenstrom
Georgios Karagiannis	Huawei
Thomas Klein	IBM
Kent Kong	Huawei
Joachim Koss	ETSI
Artur Krukowski	RSFAT
Antonio Kung	Trialog
Zbigniew Kopertowski	Orange
Alice Li	Huawei
Antonis Litke	Institute of Communication and Computer Systems
Sean McGrath	University of Limerick
Dave Raggett	W3C
Axel Rennoch	Fraunhofer FOKUS
Aitor Corchero Rodriguez	Eurecat
Rita Santiago	Ubiwhere
Philippe Sayegh	VERSES
Erwin Schoitsch	Austrian Institute of Technology
George Suciu	BEIA Consult
Giacomo Tavola	Politecnico di Milano
Xu Yang	Huawei
Ricardo Vittorino	Ubiwhere
Orfeas Voutyras	Institute of Communication and Computer Systems
Michelle Wetterwald	FB Consulting, France

© All rights reserved, Alliance for Internet of Things Innovation (AIOTI) 2022

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, 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 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 Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.

AIOTI is a partner for the European Commission on IoT policies and stimulus programs, helping to identifying and removing obstacles and fast learning, deployment and replication of IoT Innovation in Real Scale Experimentation in Europe from a global perspective.

AIOTI is a member driven organisation with equal rights for all members, striving for a well-balanced representation from all stakeholders in IoT and recognizing the different needs and capabilities. Our members believe that we are the most relevant platform for connecting to the European IoT Innovation ecosystems in general and the best platform to find partners for Real Scale Experimentation.

All rights reserved, Alliance for Internet of Things Innovation (AIOTI). The content of this document is provided 'as-is' and for general information purposes only; it does not constitute strategic or any other professional advice. The content or parts thereof may not be complete, accurate or up to date. Notwithstanding anything contained in this document, AIOTI disclaims responsibility (including where AIOTI or any of its officers, members or contractors have been negligent) for any direct or indirect loss, damage, claim, or liability any person, company, organisation or other entity or body may incur as a result, this to the maximum extent permitted by law.