Alliance for AI, IoT and Edge Continuum Innovation

StandICT.eu Report

IoT Standardisation Gaps Release 2

JULY 2026

Powered by

standICT.eu 2026

ICT Standardisation Observatory and Support Facility in Europe

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating AI, IoT and Edge Continuum Innovation in Europe, bringing together small and large companies, academia, researchers, policy makers, end-users and representatives of society in an end-to-end approach. We strive to leverage, share and promote best practices in the AI, IoT and Edge Continuum ecosystems, be a one-stop point of information to our members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of the AI, IoT and Edge Continuum Innovation in society. AIOTI contributions go beyond technology and address horizontal elements across application domains, such as matchmaking and stimulating cooperation by creating joint research roadmaps, defining policies and driving the convergence of standards and interoperability.

Legal notice

The document has been prepared for the Europen Commission and SDOs however it reflects the views only of the authors, and neither the European Commission nor the Standards Development Organisations can be held responsible for any use which may be made of the infomation contained therein. More infomation on the European Union is available on the internet (http://europa.eu).

About StandICT.eu

The StandICT.eu 2026 Coordination and Support Action project is funded by the European Union under grant agreement no. 101091933. The project is coordinated by Trust-IT Srl (IT) in quality of Technical Coordinator and Dublin City University (IE) in quality of Financial Coordinator, supported by the partners European Digital SME Alliance (BE), OpenForum Europe (BE), Australo (ES) and Fraunhofer ISI (DE). The content of the present report does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

Table of Contents

List of Tables

Table of Figures

Executive Summary

This report presents an approach reported in AIOTI, for the definition and identification of key IoT standardisation gaps in several initiatives. This report then starts to address the work done within the relevant SDOs that need to cooperate in order to solve these standardisation gaps.

The purpose of this document is to promote a structured discussion within the EUOS, AIOTI and IoT standardisation community and to provide consolidated technical elements as well as guidance and recommendations.

Release 2 of this report uses the approach that has been defined in Release 1, for the definition and identification of key IoT standardisation gaps in several initiatives. In particular, this release of the report:

- included 16 additional challenges that are covering Edge Internet of Things (IoT) Industrial Immersive Technologies;
- listed any additional specifications that were published by SDOs that might cover the identified IoT challenges;
- identified and selected the SDOs and specifications that might cover the identified IoT challenges;
- selected which of the identified challenges are intensively covered by the SDOs and specifications and which are less intensively covered by the SDOs and specifications.

Contributors of EUOS StandICT.eu / AIOTI IoT and Edge Computing Standardisation Gap reports 2025

Name	Affiliation
Georgios Karagiannis (editor)	AIOTI WG Standardisation co-Chair & Huawei
Noleen Campbell	NSAI Standards
Maria Ines Robles	Aalto University
Michelle Wetterwald	Netellany
Orfeas Voutyras	Institute of Communication and Computer Systems
Antonio Kung	Trialog
Lindsay Frost	NEC
George Suciu	BEIA Consult
Amelié Gyrard	Trialog
Jens Gayko	VDE Association for Electrical, Electronic & Information Technologies
Axel Rennoch	Fraunhofer FOKUS
Edward C. Zimmermann	NONMONOTONIC Networks
Marco Carugi	Consultant
Amanda Suo	UNE - Spanish Standardisation Body
XiaoRui Zhang	Dublin City University
Richard Pitwon	Resolute Photonics
Damir Filipovic	BluSpecs
Damiano de Rosa	AIOTI Communication Manager
Shen Bin	CAICT
Samir Medjiah	Laas-CNRS Toulouse
Mihai Penica	University of Limerick
Valentina Peniche	AIOTI Secretary General
Dave Raggett	W3C/ ERCIM
Natalia Stathakarou	Massive Dynamic Sweden

Name	Affiliation
Alissa Zaccaria	Intellimech
Ana Petrache	BEIA Consult
Asbjørn Hovstø	Hafenstrom
Artur Krukowski	RFSAT
Zbigniew Kopertowski	Orange Poland
Mari-Anais Sachian	BEIA Consult
Sascha Hackel	Fraunhofer FOKUS
Erwin Schoitsch	Austrian Institute of Technology
Vasileios Karagiannis	Austrian Institute of Technology

1. Goal and motivation

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

There are now several IoT Standards Landscape reports available, including the work done by EUOS and AIOTI in "Landscape of Internet of Things (IoT) Standards V2" and by AIOTI in "High Priority IoT Standardisation Gaps and Relevant SDOs Release 2.0" and by ETSI in STF 505, on standards identification, that have identified a number of standards that are available, i.e. which have reached a final stage (Technical standard (TS) or TR, etc.) in a Standards Developing Organisation (SDO) or industrial consortia, and can be used for the work and developments of the IoT community.

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

The purpose of this document is to start a structured discussion within the EUOS (European Observatory) community and AIOTI community to provide consolidated technical elements as well as guidance and recommendations.

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

The EUOS/AIOTI "Landscape of Internet of Things (IoT) Standards V2" report has been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives.

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

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

Release 2 of this report uses the approach that has been defined in Release 1, for the definition and identification of key IoT standardisation gaps in several initiatives. In particular, this release of the report:

- included 16 additional challenges that are covering Edge Internet of Things (IoT) Industrial Immersive Technologies;
- listed any additional specifications that were published by SDOs that might cover the identified IoT challenges;
- identified and selected the SDOs and specifications that might cover the identified IoT challenges;
- selected which of the identified challenges are intensively covered by the SDOs and specifications and which are less intensively covered by the SDOs and specifications.

2. Possible IoT challenges

This section introduces IoT research and standardisation challenges that have been identified either from the IoT activities of the EUOS community, or from literature studies. The goal of this IoT challenges collection is to form the basis of identifying the IoT standards gaps.

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

Furthermore, each of the described IoT research and standardisation challenges are mapped to specific Categories of Standards Challenges. This has been done on making it easier to acquire a high-level and homogeneous view of the various standards challenges, and provide a structure that will be essential to identify specific gaps. These categories of IoT research and standardisation challenges are:

- **Data Models & Formats (Interoperability):** This challenge involves creating and adopting uniform data models and formats to ensure seamless interoperability between different systems and technologies.
- **Data Exchange APIs (Interoperability):** Concerns the development of standardized APIs (Application Programming Interfaces) for efficient and compatible data exchange across diverse platforms.
- **Provenance and traceability (Interoperability):** Focuses on tracking the origin and history of data to maintain its authenticity and integrity across various systems.
- **Identity Management (Trust):** Involves establishing systems for securely managing digital identities to ensure that users and entities are who they claim to be.
- **Access and usage control / policies (Trust):** Pertains to establishing standardized protocols and policies for controlling access to data and regulating its usage.
- **Trusted exchange (Trust):** Ensures that data exchange between entities is secure and reliable to maintain trust in digital interactions.
- **Metadata & Discovery Protocol (Data Value):** Deals with creating effective metadata (data that describes the data) and discovery protocols to enhance the findability and value of data.
- **Data Usage Accounting (Data Value):** Involves tracking and reporting the usage of data to attribute value and possibly levy charges appropriately.
- **Publication and Marketplace Services (Data Value):** Concerns the standardisation of services for publishing data and its transaction in digital marketplaces.
- **Overarching cooperation agreement (Governance focusing on standardisation):** Relates to developing comprehensive agreements that govern cooperative efforts in standardisation.
- **Operational (e.g., SLA) (Governance focusing on standardisation):** Involves setting operational standards, such as Service Level Agreements (SLAs), to ensure quality and reliability in services.
- **Continuity model (Governance focusing on standardisation):** Focuses on establishing models to ensure the continuity and sustainability of operations and services.
- **Device certification:** Entails the process of certifying devices for compliance with established standards to ensure quality and interoperability.
- **Solution deployment and maintenance tools:** Concerns standardizing the tools and methods used for deploying and maintaining technological solutions.
- **Scalable device deployment:** Involves challenges in scaling device deployment efficiently and effectively in varying environments.
- **Green technologies:** Focuses on standardizing and promoting technologies that are environmentally sustainable. Methodologies to measure carbon emissions are as well included.
- **Usability (easy accessibility and usage to a large non-technical public):** Pertains to making technologies easily usable and accessible to people without technical backgrounds.
- **Security and Data Privacy:** Involves developing and adhering to standards that ensure the security of systems and the privacy of data.

- **Social/Societal:** Relates to addressing the social and societal implications of technologies and ensuring they meet societal needs and standards.
- **Digital/Digital Twin in the context of IoT and Edge:** Concerns the challenges in standardizing digital representations or twins of physical entities in IoT and Edge computing.
- **Artificial Intelligence in the context of IoT and Edge:** Involves standardisation challenges related to the integration and application of AI in IoT and Edge computing environments.
- **Industrial Immersive Technologies in the context of IoT and Edge**: the edge Internet of Things (IoT) industrial immersive technologies are necessary for the creation of an industrial real-digital-virtual continuum. In particular, it requires the convergence of edge IoT, artificial intelligence (AI), digital twins (DT), immersive triplets (IMT), intelligent mesh connectivity, IoT of senses (IoTS), software-defined automation (SDA) and spatial computing technologies.

2.1 Smooth interoperability between Data Models

Mapping of the described challenge into the class/group/category of challenges

- Data Models and Formats (Challenge 1)

Description of IoT challenge-research/standardisation requirement

- Currently, there is an unnecessary diversity in the data and interaction models of IoT devices across various industry standards development organizations (SDOs). This can cause problems for interoperability, as different systems and devices may use varying data models, resulting in difficulties communicating and exchanging data effectively. Additionally, this can lead to challenges in data management, analysis, and security, as data may need to be converted or transformed before it can be used or protected. The gap in data models can also limit the scalability and flexibility of the system, while increasing its complexity. Furthermore, this can cause inconsistencies in the quality of data, making it hard to effectively analyze and utilize. Moreover, a gap in data format refers to the lack of standardisation or consistency in the way that data is organized and represented.
- A gap in data model refers to a lack of standardisation or consistency in the way that data is structured and represented in the Internet of Things (IoT) ecosystem.

Source

https://datatracker.ietf.org/wg/asdf/about/

Application/Industry Domain

Applicable to all the use cases that require data modeling

Horizontal

2.2 Assurance a RESTFUL Data Exchange APIs_

Mapping of the described challenge into the class/group/category of challenges

- Data Exchange APIs (interoperability)

Description of IoT challenge-research/standardisation requirement

- The Representational State Transfer (REST) architectural style refers to a collection of recommendations and top practices that are utilized for constructing distributed hypermedia systems. REST is based on a set of limitations that, when followed, enable favorable characteristics for distributed software systems, such as scalability and modifiability. The application of REST principles to system design leads to the creation of a RESTful system, with a RESTful API being a specific example of a system that follows these principles.
- A gap in RESTful data exchange APIs refers to a lack of standardisation or consistency in the way that data is exchanged between devices, systems and servers in the Internet of Things (IoT) ecosystem.

Source

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-rest-iot-10

Application/Industry Domain

Applicable to all the use cases that implement REST

Horizontal

2.3 Need for real-time or near real-time processing and decision-making

Mapping of the described challenge into the class/group/category of challenges

- Scalable device deployment

Description of IoT challenge-research/standardisation requirement

- Various industrial control systems, including oil and gas systems, smart grids, and manufacturing systems, necessitate strict end-to-end latency between the sensor and control node. While some IoT applications may require low latency of a few tens of milliseconds, industrial robots and motion control systems require cycle times in the order of microseconds. In certain situations, the speed-of-light constraints may preclude a cloud-based solution, but that's not the sole issue in terms of time sensitivity. Industrial IoT applications also demand guarantees for bounded latency and jitter, meaning control packets must arrive with minimum variation and within a strict timeframe. Given the best-effort nature of the Internet, tackling this issue is nearly impossible without utilizing end-to-end guarantees for both individual message delivery and continuous data flows.
- To meet the time-sensitive challenge, IoT systems need to be designed to handle large amounts of data in real-time and make decisions quickly. This requires high-speed data processing, low-latency communication networks, and efficient algorithms for data analysis. Additionally, it also requires the ability to process data locally on the device, reducing the need for communication with the cloud.

Source

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

Application/Industry Domain

Horizontal, Manufacturing

2.4 Connectivity Cost

Mapping of the described challenge into the class/group/category of challenges

- Scalable device deployment

Description of IoT challenge-research/standardisation requirement

- Certain IoT deployments do not confront the problem of a restricted network bandwidth to the cloud. Both 5G and Wi-Fi 6, which are fifth-generation mobile networks, can theoretically reach a maximum speed of 10 gigabits per second, or 4.5 terabytes per hour, allowing for high-bandwidth uplinks. Nevertheless, the expense of high-bandwidth connectivity required to upload all data to the cloud is impractical and unjustifiable for the majority of IoT applications. Additionally, in certain contexts such as aeronautical communication, high communication expenses may further limit the amount of data that can be practically uploaded.
- The connectivity cost gap in IoT refers to the cost associated with connecting IoT devices and systems to the Internet and other networks. This can include the cost of devices, network infrastructure, and data plans.

Source

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

Application - Industry Domain

Horizontal

2.5 Resilience to Intermittent Services

Mapping of the described challenge into the class/group/category of challenges

- Solution deployment and maintenance tool

Description of IoT challenge-research/standardisation requirement

- Many IoT devices such as sensors, data collectors, actuators, controllers, etc. have very limited hardware resources and cannot rely solely on their limited resources to meet all their computing and/or storage needs. They require reliable, uninterrupted, or resilient services to augment their capabilities in order to fulfill their application tasks. This is hard and partly impossible to achieve with cloud services for systems such as vehicles, drones, or oil rigs that have intermittent network connectivity. The dual is also true, a cloud back-end might want to have a reading of the device even if it's currently asleep
- To address this challenge, IoT systems need to be designed with resilience in mind, by implementing techniques such as local data storage, local processing capabilities, and alternative communication channels. For instance, IoT devices can be designed to store data locally and transmit it to the cloud once the network connectivity is restored. Additionally, IoT devices can also be equipped with backup communication channels, such as Bluetooth or Wireless Sensor Networks (IEEE 802.15.4), which can be used to transmit data in cases of intermittent network disruptions. By adopting such measures, IoT systems can continue to function and provide reliable performance even in the face of intermittent network disruptions.

- Resilience to intermittent services in IoT refers to the ability of IoT systems to remain functional and reliable even in cases where there are intermittent network disruptions, such as temporary outages or poor signal strength.
- The Gap in IoT devices often rely on network connectivity to send and receive data, which can be disrupted due to various reasons such as environmental interference, network congestion, or even physical obstructions. In such cases, IoT devices may not be able to send data to the cloud or receive commands from the cloud, which can lead to system downtime and impact the performance of the IoT application.

Source

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

Application - Industry Domain

Horizontal

Manufacturing

2.6 Assurance Privacy and Security

Mapping of the described challenge into the class/group/category of challenges

- Security and Data Privacy

Description of IoT challenge-research/standardisation requirement

- IoT services that are used in homes can reveal personal information through the data they collect, such as employment status, family situation, age, and income. Policy-makers have introduced regulations to limit the usage of personal data and enforce strict requirements for those who handle and control the data. Storing data in the Cloud for an extended period of time increases the risk of data breaches, especially if the target is valuable to attackers. In General, Industrial systems do not gather personal data, but the information they generate is sensitive and could expose trade secrets like the setup of production lines. Therefore, owners of these systems are usually hesitant to upload their IoT data to the Cloud. Moreover, passive attackers can analyze the device-to-cloud path and detect traffic patterns associated with sensor networks. To address this concern, edge computing may be necessary to hide such traffic patterns.
- The gap in assurance privacy and security in IoT refers to the challenge of ensuring that personal and sensitive data collected and transmitted by IoT devices and systems is protected against unauthorized access, use, or disclosure.

Source:

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

https://datatracker.ietf.org/doc/html/rfc8576

Application/Industry Domain

Horizontal

2.7 Deployment and management of large-scale distributed networks of devices

Mapping of the described challenge into the class/group/category of challenges

- 15. Scalable device deployment

Description of IoT challenge-research/standardisation requirement

- With the large-scale number of IoT devices, we need methods and approaches for large scale firmware and software deployment. Device Management platforms must adapt to the new volume of connected devices. To that end, "campaign management" tools allow to define operations for large numbers of devices using rules.
- Reactive operations: Possibility to dynamically enroll devices based on their state, which triggers automatic provisioning or firmware upgrade operations. For instance, target only devices with a specific firmware, or a specific type.
- Pro-active operations:
  - when a vulnerability is detected on a family of devices, require a prompt firmware upgrade.
  - Hold smart inventories, storing the relevant data for an efficient targeting of devices.
  - Monitor and control the execution of these massive campaigns.
  - Rollout tools to trigger operations on devices following specific strategies balancing operational and functional risks
  - Divide the targeted device population into sub-groups, whose size may increase as the operation proves to be successful in the earlier test groups. However, in the case of a security crisis, the small time overhead induced by this cautious strategy may prove more harmful than potential dysfunctions, motivating a more direct approach with simultaneous upgrades.
- Existing activities: These requirements are partly described in the BBF TR-131, which specifies the use cases and functional requirements for a DM solution Northbound interface, without specifying the interface itself (lack of the specification). It includes requirements for architecture, provisioning devices, device operations, file management, device grouping, events, error management, security and access control. However, these specifications may need some adaptation for the IoT context.
  - See also: ETSI IoT Week 2022; AI, IoT & Device Management: the Indispensable Collaboration; Presented by: Samuel Berlemont, Orange; 14/10/2022. Available at https://docbox.etsi.org/Workshop/2022/10ETSIIOTWEEK/SESSION14/ORANGE_BERLEMONT.pdf.
  - Here the focus is on unified model/tools and strategies for deployment and management of large-scale distributed networks of devices

Type of Requirements

Non-Functional Requirements

- Performance
- Flexibility
- Scalability
- Reliability
- Safety

Source

Information copied from AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf.

Application/Industry domain:

Horizontal (Deployment/ Device-sensor technology).

2.8 Sustainability, energy consumption, rare minerals and raw materials provisioning

Mapping of the described challenge into the class/group/category of challenges

- 16. Green technologies

Description of IoT challenge-research/standardisation requirement

This challenge is related to green technologies. In particular, to sustainability, energy consumption, rare minerals and raw materials provisioning. It covers several topics:

- First topic: using IoT technologies to improve the environmental impact of other domains. This topic covers for example smart homes and buildings, pollution measurements or waste reduction in smart cities, soil moisture and weather monitoring in smart agriculture, or the smart energy domain aiming to meter and optimize overall energy consumption. There are many stakeholders' initiatives, such as the call for action that resulted from the ITU-T green standards week [74]. Standards are defined for smart metering in the domain of Utilities. For example, IEC 62056 family of standards [76] specifies "electricity metering data exchanges".
- Second topic: improving the energy footprint of IoT based systems, including its use and energy consumption, the disposal or refurbishing of obsolete devices, the design and manufacturing of energy and environment-friendly new devices.
- Existing activities: ITU-T Study Group 5 has established a Focus Group on "Environmental Efficiency for Artificial Intelligence and other Emerging Technologies" (FG-AI4EE). Its objective is to support the development of technical reports and technical specifications to address the environmental efficiency, as well as water and energy consumption of emerging technologies, and provide guidance to stakeholders on how to operate these technologies in a more environmentally efficient manner to meet the 2030 Agenda for Sustainable Development and its 17 Sustainable Development Goals.
- See also: ETSI IoT Week 2022; IoT and edge computing for green transformation; Presentations in Session 3 (https://docbox.etsi.org/Workshop/2022/10ETSIIOTWEEK/SESSION03) and Session 7 (https://docbox.etsi.org/Workshop/2022/10ETSIIOTWEEK/SESSION07).

Type of Requirement

Non-Functional Requirement

- Performance
- Safety

Source

Information Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (IoT Architecture)

2.9 Developing Standards for IoT Security Testing and Validation

Mapping of the described challenge into the class/group/category of challenges

- Security and Data Privacy
- Trusted exchange (Trust)

Description of IoT challenge-research/standardisation requirement

- IoT system architectures include multiple modules with separated and specific functional scopes. It is therefore important that in particular those modules that are security relevant will be tested and validated using a systematic and standardized approach. Thus, assembling of security related generic functional modules within an IoT architecture, that support Security by Design and trustworthiness need to be performed. In this context it is also required to retrieve relevant security testing methods and specific detailed test purposes. Using standardized notations for test purposes like the ETSI Test description language (TDL-TO) can support this approach. The focus on generic modules within IoT architectures ensures the application and support within multiple industrial domains.
- Short description of the requirement: Testing and validation of security functions as well as the protection of IoT interfaces and modules is one of the preconditions regarding a secure IoT infrastructure and IoT devices.

Type of Requirement

Functional requirements

- Quality and validation of security functions
- Reliable communication between the stakeholders.

Non-functional requirements

- Reliability
- Security and privacy
- Trust

Source

ETSI TC MTS, WG TST: IoT Security Functional Modules; IoT security module testing: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66187

ETSI TC MTS, WG TST: Security validation of IoT architecture application and conformity Case Study Experiences: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66188

Application/Industry domain:

Horizontal (cross-domain)

2.10 Developing and Implementing Trustworthiness for IoT Systems

Mapping of the described challenge into the class/group/category of challenges

- Access and usage control / policies (Trust)
- Trusted exchange (Trust)

Description of IoT challenge-research/standardisation requirement

- Architects along with other stakeholders need to develop trustworthiness models, e.g. by introducing concepts for characteristics, assurance and risks. In this context a risk management approach can help to identify risk aspects and ensure that the trustworthiness view has been considered and implemented through the development process. A risk-based approach includes the identification of specific security risks and can lead to the enrichment of the standardized IoT functional domains using appropriate standardized functional modules within an IoT system. The following gives examples of relevant IoT functional modules related to dedicated IoT functional domains:
  - Resource access and interchange;
    - Example: Introducing a frontend access control
  - Operations and management domain; or
    - Example: Introducing a specific Runtime Monitoring system
  - Sensing and controlling domain.
    - Example: Attack detection system
    - Example: Honeypots
- Short description of the requirement: Trustworthiness is an essential basic requirement for users to accept, consider and work with dedicated IoT devices and/or infrastructures.

Type of Requirement

Functional requirements

- Reliable communication between the stakeholders.

Non-functional requirements

- Reliability
- Trust

Source

- ISO/IEC JTC1 SC41, WG3: ISO/IEC 30141 ED2; Internet of Things (IoT) - Reference architecture: https://www.iec.ch/dyn/www/f?p=103:38:617227331288265::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104064
- ISO/IEC JTC1 SC41, WG3: ISO/IEC 30149 ED1; Internet of Things (IoT) - Trustworthiness Principles: https://www.iec.ch/dyn/www/f?p=103:38:617227331288265::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104432

Application/Industry domain:

Horizontal (cross-domain)

2.11 IoT and Ethics

Mapping of the described challenge into the class/group/category of challenges

- Security and Data Privacy

Description of IoT challenge-research/standardisation requirement

- As IoT systems continue to grow in popularity and adoption, there is a growing concern about the privacy and ethical implications of these systems. IoT systems involve the collection and processing of large amounts of personal and sensitive data, which can potentially be used for nefarious purposes or in ways that are not consistent with the expectations of individuals. Additionally, IoT systems may raise ethical concerns related to issues such as data ownership, consent, and transparency.
- To address these concerns, it is important to develop privacy and ethical guidelines, policies, and standards for the design, deployment, and operation of IoT systems. This may involve the implementation of privacy-by-design principles, the use of encryption and other security measures to protect data, and the development of transparency and accountability mechanisms to ensure that individuals are aware of how their data is being used.
- Therefore, the gap of IoT and Ethics highlights the need for the development of comprehensive ethical frameworks for IoT systems, as well as the need for ongoing research and development in this area. This includes the development of privacy-enhancing technologies, the exploration of new models of data ownership and control, and the establishment of ethical guidelines and principles for the design, deployment, and operation of IoT systems.
- IoT and Ethics refer to the need to address the privacy and ethical concerns associated with the collection, storage, and use of personal and sensitive data in IoT systems. This gap highlights the need for the development of privacy and ethical guidelines, policies, and standards for the design, deployment, and operation of IoT systems.

Source

- https://datatracker.ietf.org/doc/html/draft-lukianets-open-ethics-transparency-protocol-02
- Karale, Ashwin. "The challenges of IoT addressing security, ethics, privacy, and laws." Internet of Things 15 (2021): 100420; https://doi.org/10.1016/j.iot.2021.100420

Application - Industry Domain

All IoT applications that manipulate personal data

Horizontal

2.12 IoT Governance and Regulation

Mapping of the described challenge into the class/group/category of challenges

- Social/Societal

Description of IoT challenge-research/standardisation requirement

- The rapid growth and proliferation of IoT technologies have led to concerns about their potential negative impacts, such as privacy breaches, cyber attacks, and safety risks. To address these concerns, it is important to develop appropriate policies, laws, and regulations to govern the use of IoT technologies.
- This may involve the establishment of regulatory frameworks that can ensure the security, privacy, and ethical use of IoT technologies, alongside with spectrum regulations. Such frameworks should address issues such as data protection, privacy, security, liability, and accountability. Additionally, these frameworks should be designed to balance the benefits of IoT technologies with the risks they pose, and to ensure that they are deployed in a safe and responsible manner.
- Therefore, the gap of IoT Governance and Regulation highlights the need for the development of a comprehensive regulatory framework that can ensure the safe and responsible use of IoT technologies. This requires collaboration between government agencies, industry stakeholders, and the public to ensure that the regulatory framework is effective, efficient, and responsive to the evolving needs of IoT technologies.
- IoT Governance and Regulation refer to the need for the development of appropriate policies, laws, and regulations to govern the use of IoT technologies and ensure their safe and responsible deployment. This gap highlights the need for the establishment of a regulatory framework that can ensure the security, privacy, and ethical use of IoT technologies, alongside with the regulations of for example the radio spectrum that IoT devices operate.

Source

https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/20111028IERC-IoT-STD-Poznan/CASAGRAS2%20Establishing%20an%20International%20Framework%20for%20Structure%20&%20Governance%20v2.pdf

Application - Industry Domain

Horizontal

2.13 Zero Touch Configuration (ZTC)

Mapping of the described challenge into the class/group/category of challenges

- Identity Management

Description of IoT challenge-research/standardisation requirement

- ZTC can help to reduce deployment time, minimize human error, and improve the overall efficiency of device management.
- Zero Touch Configuration (ZTC) is an important challenge in the context of IoT because traditional methods of configuration and provisioning can be time-consuming, expensive, and error-prone, particularly when dealing with large numbers of devices. This is especially true in industrial settings, where there may be hundreds or thousands of devices deployed across a wide area, making it impractical to manually configure each one individually.
- In addition to the practical considerations of time and cost, there are also security implications to consider. Manual configuration of devices can introduce the possibility of human error, which in turn can create security vulnerabilities. This is particularly concerning in critical infrastructure or other sensitive applications where a breach could have serious consequences.
- By automating the configuration and provisioning process, ZTC can help to address these challenges, reducing the time and cost associated with device deployment, improving security by reducing the risk of human error, and enabling faster response to changing business needs. As such, ZTC is an important area of focus for IoT developers and operators.
- Zero Touch Configuration (ZTC) is an IoT challenge that refers to the ability to automatically configure, provision, and manage IoT devices and services with minimal human intervention. The goal of ZTC is to eliminate the need for manual configuration of IoT devices and reduce the time and cost associated with device deployment and management. ZTC typically involves the use of automated provisioning, configuration, and management tools and techniques, such as Device Management Protocols, Over-The-Air (OTA) Updates, and Network Function Virtualization (NFV). The challenge lies in designing and implementing effective ZTC mechanisms that can handle the complex and dynamic nature of IoT environments while ensuring security, scalability, and reliability.

Source

https://datatracker.ietf.org/doc/rfc8572/

Application - Industry Domain

Horizontal

2.14 Usability of data and services provided by IoT devices and platform

Mapping of the described challenge into the class/group/category of challenges

- 17. Usability

Description of IoT challenge-research/standardisation requirement

- Motivation: Usability of the data and services that the IoT devices and platforms deliver is a key issue. In addition to user experience (ergonomics) or the accessibility of the ICT equipment, the usability topic should also be considered from a data and service point of view, i.e. usability of the data and services that the IoT devices and platforms deliver. This topic complements other standards such as ISO 9241 or ETSI EN 301 549 for user experience (ergonomics) or the accessibility of the ICT equipment. Standardizing the usability of IoT devices and platforms may also have a strong impact on big data and AI technologies: (a) making use of AI for knowledge presentation and management (organization and visualization) for both machines and humans; (b) improving configuration and management tasks at IoT devices and platforms to increase the reliability of the data used by AI.
- Usability also means that the IoT technologies, devices and platforms can be trustily used according to their initial objectives (e.g. easy installation, configuration, operation and maintenance).
- Recent activities: ETSI has developed two standards related to data usability: TR 103 778 “SmartM2M; Use cases for cross-domain data usability of IoT devices” (12-2021), and TS 103 779 “SmartM2M; Requirements and Guidelines for cross-domain data usability of IoT devices”, (05-2022). ETSI EN 301 “549 Accessibility requirements for ICT products and services” (2021-03) also covers this topic.
- See also: ETSI IoT Week 2022; Cross-Domain Data Usability in IoT Ecosystem Comprising IoT Devices, Humans and Machines; Presented by: Michelle Wetterwald, Netellany; 14/10/2022. Available at https://docbox.etsi.org/Workshop/2022/10ETSIIOTWEEK/SESSION14/NETTELANY_WETTERWALD.pdf.
- Short description of the requirement: Easy accessibility and usage to a large non-technical public

Type of Requirement

Non-Functional Requirement

- Reliability
- Trust

Source

Copied partly from : AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Applications and data management)

2.15 User-level Service Managements of IoT Network by utilizing Artificial Intelligence

Mapping of the described challenge into the class/group/category of challenges

- Artificial Intelligence in the context of IoT and Edge

Description of IoT challenge-research/standardisation requirement

- User-level Service Management in IoT networks refers to the ability to provide personalized and high-quality services to individual users based on their specific needs and preferences. This can include services such as home automation, smart energy management, health monitoring, and more.

- Artificial intelligence (AI) can play a significant role in improving the user-level service management of IoT networks. AI algorithms can be used to analyze user data, such as usage patterns, preferences, and behaviors, and provide personalized recommendations and services accordingly. Additionally, AI can help optimize network performance and improve the reliability and efficiency of IoT services.
- However, there are several challenges to implementing AI for user-level service management in IoT networks.
- Despite these challenges, the use of AI for user-level service management in IoT networks has the potential to greatly enhance the user experience and improve the overall performance of IoT services. By leveraging AI, IoT service providers can create more personalized and efficient services that meet the unique needs of individual users.
- One major challenge is the need to collect and analyze vast amounts of data from multiple sources, including sensors, devices, and networks. Another challenge is ensuring the security and privacy of user data, as IoT networks can be vulnerable to cyberattacks and data breaches.

Source

https://datatracker.ietf.org/doc/html/draft-choi-icnrg-aiot-10

Application/Industry domain:

Horizontal

2.16 IoT over ICN

Mapping of the described challenge into the class/group/category of challenges

- Operational

Description of IoT challenge-research/standardisation requirement

- Information-Centric Networking (ICN) is a networking paradigm that focuses on the distribution and retrieval of information instead of traditional host-centric networking, which focuses on communication between devices. IoT, on the other hand, is a network of connected devices that collect, exchange, and analyze data to provide services and insights.
- While ICN has several potential advantages for IoT, such as better scalability, security, and resilience, there are also some gaps that need to be addressed to make ICN suitable for IoT applications. One Gap is the lack of support for real-time data processing and analytics
- Another gap is the need for standardisation and interoperability. IoT devices and services are often built using different technologies and protocols, which can make it challenging to integrate them into an ICN architecture. There is a need for standardized interfaces and protocols that can enable seamless communication and interoperability between IoT devices and ICN networks.
- Finally, ICN may not be suitable for IoT applications that require low-latency and high-bandwidth communication. While ICN can reduce network congestion and improve reliability, it may not be able to provide the high-speed, low-latency communication required for applications such as autonomous vehicles or real-time video streaming.
- Overall, while ICN has several potential benefits for IoT, there are also several gaps that need to be addressed to make ICN a viable option for IoT applications.
- One such gap is the lack of support for real-time data processing and analytics. ICN architectures are primarily designed for data storage and retrieval, which may not be sufficient for IoT applications that require real-time processing and analysis of data.

Source

https://datatracker.ietf.org/doc/html/draft-zhang-icnrg-icniot-requirements-01

https://datatracker.ietf.org/doc/html/rfc7927

Application/Industry domain:

Horizontal

2.17 Harmonized identification

Mapping of the described challenge into the class/group/category of challenges

- 4. Identity Management (Trust)

Description of IoT challenge-research/standardisation requirement

- Motivation: In general, no single identification scheme fits all needs and often identification is bound to a specific technologies or governance bodies.
- Examples are domain names, IP and MAC addresses that are bound to specific communication technologies and car license plates that assigned by public authorities. These different identifiers might be bound to the same entity and can be assigned in a static or dynamic way. In that case resolution between the different identifiers has to be done. Examples are the Domain Name System (DNS) which maps between domain names and IP addresses and the Address Resolution Protocol (ARP) which maps between IP and MAC addresses.
- Furthermore, specifically for the identification of Things various identifiers schemes are already in use and standardized for years. They are often application or domain specific like identification of freight containers (ISO 6346), books (ISBN/ISO2108) and animals (ISO 11784). These existing schemes will be used in IoT and a convergence to a single scheme is not expected. In case IoT applications have to deal with several identification schemes differentiation between them is needed in order to ensure uniqueness and correct interpretation and processing of the identifiers. That can be based on the specific context in which the identifier is used or on a meta-identification scheme like ISO/IEC 29161. ISO/IEC 29161 introduces an unambiguous wrapper based on URNs for the differentiation. The wrapper allows to identify identifier schemes based on various standards for which URN namespaces are defined (e.g. urn:epc, urn:oid, urn:isbn, urn:uuid). Also, proprietary identifier scheme could be covered by registering an urn namespace with IANA (see IETF RFC 8141) or a sub namespace with a registration entity that offers such a service.
- Recent activities: AIOTI has published a report on this topic: "AIOTI report on Identifiers in Internet of Things (IoT)", 02-2018. Available at: https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf.
- Short description of the requirement: Harmonized reference for unique and secured naming mechanisms

Type of Requirement

Functional Requirement

- Reliable communication between the stakeholders

Non-Functional Requirement

- Interoperability
- Reliability

Source

Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Applications Management)

2.18 Semantic interoperability

Mapping of the described challenge into the class/group/category of challenges

1. Data Models & Formats (Interoperability)

Description of IoT challenge-research/standardisation requirement

Motivation: There are currently standards and directions being followed for the semantic description of systems. As the different IoT platforms often choose one of these solutions, there is a need for (standardized) entities or reference / abstract ontologies able to perform the mapping between the different existing ontologies. The mapping can be realized directly between the ontologies used by the different systems or by translating each used ontology to a generic ontology that serves as a common reference. The mapping between different ontologies should be considered at the border of a system rather than internally to a system. Statistical approaches could be used additionally to define the mapping between ontologies and resolve the issues brought by incompleteness or uncertainties of the mapping.

Semantic interoperability is being addressed in different SDOs, which deliver ontology and semantics standards, but gaps remain and indeed, multiple approaches are increasing the fragmentation and confusion in the number of options. Further coordination between various groups would be needed to avoid a fragmented offer for IoT semantics

Existing activities: AIOTI standardisation subgroup on semantic interoperability has coordinated the preparation of several white papers with the goal of advancing the adoption of semantic technologies and achieving semantic interoperability. IEC Market strategy Board (looks at different topics, state of the art) has conducted a study on "Semantic Interoperability – Challenges in The Digital Transformation Age". oneM2M standards support different approaches for semantic interoperability: RDF/OWL serialization format, Smart Device Template (SDT), FlexContainer resources, Blackbox resources. The Smart Applications Reference Ontology (SAREF) is a standardized ontology for IoT devices and solutions published by ETSI in a series of Technical Specifications. OPC UA (Unified Architecture) provides a framework that can be used to represent complex information as Objects in an Address Space. The Semantic Sensor Network (SSN) ontology is a widely-recognized ontology published by the W3C. Schema.org Extensions for IoT (iotschema.org) is a W3C Community Group for extending Schema.org to connected Things.

Short description of the requirement: interpret and process the sensor data in an identical manner across heterogeneous platforms; convert existing information models into a machine-interpretable form; create re-usable chunks of models that can be combined for different applications

Type of Requirement

Functional Requirement

- 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

- Interoperability
- Reliability

Source

- Extracted from : AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf
- IETF RFC 8477: RFC 8477: Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016
- EC H2020-SHAPES project: https://cordis.europa.eu/project/id/857159

Application/Industry domain:

- Horizontal (Service and applications)

2.19 Ethics and trustworthiness

Mapping of the described challenge into the class/group/category of challenges

- 5. Access and usage control / policies (Trust)

Description of IoT challenge-research/standardisation requirement

- Motivation: Ethics is a well-known topic in Artificial Intelligence, but not really in IoT standardisation.
- Ethical values are defined by the societal and cultural environment and may change over time. It doesn't make sense to standardize these values and they are not a technology specific issue.
- As the use and impact of IoT and autonomous and intelligent systems (A/IS) become pervasive, we need to establish societal and policy guidelines in order for such systems to remain human-centric, serving humanity's values and ethical principles. These IoT systems must be developed and should operate in a way that is beneficial to the users and their environment, beyond simply reaching functional goals and addressing technical problems. This approach will foster the heightened level of trust between people and used IoT technology that is needed for its fruitful use in our daily lives.
- IoT technologies solve many real-life problems but they create serious ethical concerns and legal challenges related to: protection of privacy, data security, data usability, data user experience, trust, safety, etc.
- Examples of ethical challenges associated to IoT: No Way Out (the client is totally immersed in the IoT network. There is a high dependability from the user on the IoT network specially in healthcare applications); miniaturization (it will be difficult to maintain any sort of audit, quality control or traffic control, due to the nano size and huge number of devices); IoT globalization (IoT cannot be localized, especially in medical applications where the service can be offered overseas); new business models (using IoT will enforce companies that offer medical services to create new business models that take into consideration the available types of data and the high stream. Virtual hospitals will take place. Therefore, the service will be offered remotely); vagueness (the differentiation between physical and virtual devices and human being will be more difficult due to the ease of transformation from one category to another); ultra-availability (billions of devices will be always on 24/7. This will result in massive amount of data (big data), which will be more exposed to malicious attacks); autonomous and unexpected behaviour (human beings will be part of IoT networks together with other devices and sensors. Interconnected devices may interfere suddenly

in human actions. The continuous development of IoT will lead to ambiguous behaviours not completely understandable by the users); governance (due to the considerable number of routers, switches and information, the data exchanges will be faster and less expensive, difficult to be controlled or monitored. The accountability is an additional challenge to tackle);

- Trustworthiness is the degree to which users and all stakeholders have confidence that a product or system will behave as intended. Trustworthiness is a major issue for the acceptance of a technology by the society especially if applications enabled by a new technology may have negative impact on ethical values of the society.
- From an IoT point of view the following areas are of major importance when considering trustworthiness: Privacy; Information security; Safety.
- Short description of the requirement: Ethics and trustworthiness

Type of Requirement

Functional Requirement

- Reliable communication between the stakeholders

Non-Functional Requirement

- Safety
- Security and privacy
- Trust

Source

Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Service and applications / Security / Privacy)

2.20 Open Markets of Digital Services

Mapping of the described challenge into the class/group/category of challenges

- 9. Publication and Marketplace Services (Data Value)

Description of IoT challenge-research/standardisation requirement

- Motivation: The value of markets to suppliers and consumers is related to the size of the marketplace. Competition in open markets is an effective driver for the adoption of standards, and for companies to actively contribute to the development of standards.
- The Web of Things provides a basis for connecting suppliers and consumers of IoT services, decoupling applications from the underlying protocols, but further work is needed on standards in the following areas:
  - Standards for suppliers and consumers to find each other and work together
  - Standards for describing services, e.g. different kinds of sensors and actuators, and what they measure or control – this involves domain specific ontologies

- Standards for describing the software interfaces and data formats – this is fulfilled by the Thing Descriptions for the Web of Things
- Standards for terms and conditions for service contracts
- Standards for audit trails – this could be based upon block chains that record agreements on smart contracts, as well as a record of operations as required by those contracts
- Standards for payments – e.g. one off, subscription-based, or per-use payments
- Standards for security and for enabling trust between suppliers and consumers, including the regulatory framework and legal recourse

- Short description of the requirement: standards needed to enable open markets of services

Type of Requirement

Non-Functional Requirement

- Flexibility
- Interoperability

Source

Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Service and applications; business)

2.21 Certification of device classes

Mapping of the described challenge into the class/group/category of challenges

13. Device certification

Description of IoT challenge-research/standardisation requirement

- Motivation: Certification has been traditionally considered as a key process for the assessment of the management, operational, and technical security controls in an information system. In general, there are three possible levels of certification for devices and systems, as described in IEEE Conformity Assessment Program presentation:
  - Declaration of conformity by the device manufacturer
  - Compliance with requirements from the device user or customer, for example a system integrator
  - Certification by an independent organisation or dedicated laboratory.
- IoT is considered as a core enabler of the current hyper-connectivity trend, in which certification is crucial to ensure trust in the development of new digital solutions. Beyond limitations of well-known certification schemes such as cost and complexity, the massive integration of physical devices to the Internet brings new challenges to the certification process of IoT devices. Certification may apply to very different features of an IoT device: safety, security / privacy, data quality, semantics and most often its specified requirements to adhere to specific standards and regulations when available. Certification delivers trust in the devices to which they apply.

- Short description of the requirement: Certification mechanisms defining "classes of devices" and ensuring the quality of the devices and the data they handle

Type of Requirement

Functional Requirement

- Reliable communication between the stakeholders

Non-Functional Requirement

- Interoperability
- Reliability
- Safety
- Security and privacy

Source

Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Device-sensor technology)

2.22 Device Management

Mapping of the described challenge into the class/group/category of challenges

- 14. Solution deployment and maintenance tools

Description of IoT challenge-research/standardisation requirement

- Motivation: Device Management (DM) is a tool enabling telecommunications operators, manufacturers and service providers to make sure that smart objects installed on clients' premises are working correctly. In this environment, this is becoming more crucial to provide an ecosystem of reliable equipment for the countless services of the IoT, with the smart city, healthcare, agriculture, the smart home, or industry 4.0.
- Device Management consists of a set of operations remotely executed on connected devices in a secure environment: provisioning, configuration, firmware updates, and diagnostics. Current standards addressing DM will need some evolutions to fulfil IoT needs. The IoT does present challenges to be addressed for operation to be reliable and long-lasting: heterogeneity of devices, diversity of usages, security, confidentiality, and availability. IoT platforms, initially designed to collect data so as to extract information and provide recommendations, are dependent on Device Management.
- Existing activities: Current standards initiatives are at the Broadband Forum (BBF), the Open Mobile Alliance (OMA), the IETF, oneM2M and OSGi Alliance.
  - With TR-069, the BBF had a successful deployment in Digital and Smart Homes. However, regarding IoT, TR-069 cannot scale up. BBF has specified TR-369 (USP for User Service Platform) aiming at fulfilling IoT requirements.
  - OMA with OMA-DM also has a successful deployment in the mobile management domain but, as for TR-069, OMA-DM cannot scale up. OMA has specified the OMA Lightweight Machine to

Machine protocol (OMA LWM2M), a protocol more suitable for IoT constrained devices. It is worth mentioning that both BBF USP and OMA LWM2M propose a convergence of Device and Service management, so as to avoid the necessity for multiple protocol stacks on a device.

   - IETF on its side is working on two topics. COMI (CoAP Management Interface) is an initiative to transpose the IETF proposal for IT management based on NETCONF and YANG to IoT and constrained devices. SUIT (Software Updates for Internet of Things) is a proposal for defining a manifest format for software updates on IoT devices.
   - oneM2M has defined specifications for the interworking between oneM2M and different Device Management protocols, mainly BBF TR-069, OMA DM and OMA LWM2M, defining specific resources called Management Objects. While this interworking approach is a good approach for federating the heterogeneous ecosystems, the current proposal lacks flexibility.
   - OSGi Alliance specifies a standard execution environment based on Java with a SOA approach. OSGi applications are based on modules which can have dependencies and can be installed or updated at runtime. In this goal OSGi proposes a set of specifications for Device Management of OSGi devices. It mainly relies on the Device Management Tree (DMT) Admin API. The DMT is conceptually close from OMA or BBF concepts.
- Short description of the requirement: Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms

Type of Requirement

Non-Functional Requirement

- Performance
- Flexibility
- Scalability

Source

Copied from: AIOTI report: High Priority IoT Standardisation Gaps and Relevant SDOs, Release 2.0, January 2020. Available at: https://aioti.eu/wp-content/uploads/2020/01/AIOTI-WG3-High-Priority-Gaps-v2.0-200128-Final.pdf

Application/Industry domain:

Horizontal (Deployment)

2.23 Simulation and Emulation Environments

Mapping of the described challenge into the class/group/category of challenges

- Usability

Description of IoT challenge-research/standardisation requirement

- IoT Edge Computing poses unique challenges to the simulation and emulation tools used by developers and researchers. These challenges stem from the coexistence of diverse applications, networks, and computing technologies within a distributed system, which makes modeling complex. In addition, managing scale, mobility, and resources are also significant challenges. To tackle these issues, developers use simulators, which run simplified application logic on top of a fog network model, and emulators, which deploy actual applications on a cloud infrastructure running over a network that mimics network edge conditions. Hybrid federation-based approaches, which use both simulated and emulated systems, can be used to scale up. On the other hand, physical devices can be interconnected with emulated systems to increase realism. Several publicly available tools, platforms, and emulators, such as the MEC sandbox initiated by ETSI, the AdvantEDGE emulator, and EdgeNet, have been developed to address these challenges.

- The gap in IoT and Edge related to simulation and emulation environments pertains to the challenges faced by researchers and developers in accurately modeling the behavior of a distributed system that consists of a diverse set of applications, network, and computing technologies. IoT Edge Computing brings in new challenges that make it difficult to simulate and emulate edge environments due to factors such as scale, mobility, and resource management. While simulators provide a simplified application logic running on top of a fog network model, emulators enable actual application deployment over a cloud infrastructure that simulates edge network conditions. To overcome these challenges, hybrid federation-based approaches that combine emulated and simulated systems can be used. There is a need for the development of more efficient and accurate simulation and emulation tools that can cater to the complexities of IoT Edge Computing.

Source

https://datatracker.ietf.org/doc/html/draft-irtf-t2trg-iot-edge-08

https://try-mec.etsi.org/

Application/Industry domain:

Horizontal

2.24 Digital for Green

Mapping of the described challenge into the class/group/category of challenges

- Green technologies

Description of IoT research/standardisation requirement

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

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

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

Source

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

Application/Industry domain:

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

2.25 Edge Internet of Things (IoT) Industrial Immersive Technologies Challenges

Mapping of the described challenge into the class/group/category of challenges

- Industrial Immersive Technologies in the context of IoT and Edge

Description of edge computing challenge-research/standardisation requirements

- According to the AIOTI report, "Edge IoT Industrial Immersive Technologies and Spatial Computing Continuum, Release 1", the edge Internet of Things (IoT) industrial immersive technologies are necessary for the creation of an industrial real-digital-virtual continuum. In particular, it requires the convergence of edge IoT, artificial intelligence (AI), digital twins (DT), immersive triplets (IMT), intelligent mesh connectivity, IoT of senses (IoTS), software-defined automation (SDA) and spatial computing technologies.
- Such industrial real-digital-virtual continuum is made of immersive environments, which are computer-generated virtual worlds where users can sense as if they were physically embodied in that generated perception context. The convergence of these technologies into industrial immersive solutions advances the integration and application of edge intelligent immersive technologies combining augmented reality (AR), virtual reality (VR), mixed reality (MR), and extended reality (XR) with concepts like metaverses, omniverse, multiverses, next generation spatial web, Web 4.0 as part of future virtual worlds. Such convergence of industrial immersive technologies at the edge can improve efficiency, reduce downtime, enhance safety, and better decision-making in industrial settings.
- However, to be effectively deployed, it both requires a strong interdisciplinary collaboration and presents challenges like robust hardware (HW) design and cost-effective availability, data security and privacy preserving methods, and effective industrial workflow integration.

According to the AIOTI report, "Edge IoT Industrial Immersive Technologies and Spatial Computing Continuum, Release 1", the challenges associated with the edge IoT Industrial Immersive Technologies are:

- **2.25.1 Advanced HW and edge IoT devices**: Devices designed to create with reduced power envelope immersive experiences, including headsets, AI-based sensors/actuators, cameras, intelligent connectivity, controllers, and haptic devices that provide physical feedback.
- **2.25.2 New SW and CAD platform**s: Designing open and compatible platforms to create digital environments and experiences that enable seamless interaction between users and HW, ensuring a cohesive user interface.
- **2.25.3 Programming languages, libraries, and SW development kits (SDKs)**: Development for programming environments used to build immersive environments ranging from realistic simulations to advanced tools and AI frameworks for designing and creating engaging experiences.
- **2.25.4 User interface (UI)**: Improving HMI and UI to enhance interaction with the digital environment for a more immersive experience. User's ability to interact with the digital environment depends on the simplicity and intuitiveness of interfaces feedback which must be optimized to the user's task.
- **2.25.5 Intelligent connectivity**: Accelerate the advancement of multi-protocol, multi-frequency smart wireless, cellular technologies, multi-domain (satellite and terrestrial) and real-time intelligent mesh hyperconnectivity.
- **2.25.6 Blockchain and NFTs**: Blockchain may be a critical immersive technology element to ensure greater security and privacy. Blockchain digital identity technologies can enable industries to manage better with whom they interact or optimise the interactions between different machines and digital components. NFTs based on blockchain technology may prove the existence, authenticity, and ownership of content and assets in the industrial edge IoT immersive technologies that enable value creation throughout the digital asset life cycle and allow for new business models (e.g., immersive triplets, DT trading).
- **2.25.7 Edge IoT immersive platforms**: Edge IoT digital platforms and marketplaces will be important in providing open, flexible IoT industrial immersive solutions. This requires open, interoperable solutions that allow seamless, real-time, concurrent collaboration, open APIs, compatible data formats, and protocols. The goal is to integrate the edge IoT industrial immersive technologies using a common language that facilitates users' connecting their immersive triplets, avatars, and DTs in the digital, virtual, and cyber worlds. Industries can use interoperable, open systems and standard platforms to connect their immersive triplets, avatars, and DTs with the counterparts of their partners and suppliers, creating larger ecosystems that produce more profound insights and plug-and-play solutions. Appropriate regulation must ensure and encourage collaboration and interoperability by handling privacy and security concerns and protecting intellectual property in digital assets in edge IoT industrial immersive spaces.
- **2.25.8 High-quality, robust, reliable, and affordable immersive technologies**: Development of integrated and miniaturised semiconductors, IoT devices, edge processing, and AI/ML technologies for implementing intelligent IIoT immersive technologies.
- **2.25.9 Integration of immersive technology**: Development of system-of-systems concepts, approaches, and frameworks for integrating edge IoT industrial immersive technologies and the spatial computing continuum with existing systems in various industries. Development of web-based 3D immersive solutions to enhance digital experiences on web-based platforms that eliminate the need for app downloads, providing immediate and universal access on various devices.
- **2.25.10 Interoperability and Standardisation**: With a vast array of edge IoT immersive devices, platforms, and technologies, ensuring interoperability among different systems is a significant challenge. Standardisation efforts are crucial to enable seamless communication and integration across devices and platforms. Especially the interlock and synergy between the several SDOs involved in the immersive technology domain calls for a joint world-wide effort in delivering aligned and non-controversial technical specifications mandated by the different Work Groups.
- **2.25.11 Data Privacy and Security**: While edge computing can enhance data privacy, the increased distribution of data processing points expands the attack surface for potential breaches. Ensuring robust security measures that can operate effectively in decentralized environments is essential.
- **2.25.12 Scalability**: As the number of connected edge IoT immersive devices and the volume of data they generate grow, developing scalable solutions that can handle this increase efficiently without compromising performance is a significant challenge.

- **2.25.13 Complexity in Deployment and Management**: The convergence of these technologies increases the complexity of deploying and managing fully immersive systems. New skill sets and knowledge are needed to implement and maintain these integrated systems effectively.
- **2.25.14 Ethical and Societal Implications:** The widespread adoption of immersive technologies raises ethical questions concerning privacy, surveillance, and the potential displacement of jobs due to automation and AI/ML introduction. This is also a concern as the more sophisticated the HMDs get the more biodata they will collect, even reaching the point of private medical data. Addressing these concerns requires careful consideration and the development of ethical guidelines and policies. European regulations play a pivotal role in this regard and must follow close the advancement of the technology in the field of immersive technologies.
- **2.25.15 Interdisciplinary Integration**: The development of immersive technologies requires engagement in interdisciplinary activities that demand comparing disciplines, understanding disciplines, and thinking between disciplines to stimulate the co-creation of solution-oriented transferable knowledge. The immersive technology design focuses on integrated research through multidisciplinary group work of experts and non-experts interconnected into a transdisciplinary framework, as the immersive concept is a multidimensional complex of disciplinary interrelations that require learning to think at the interfaces between disciplines.
- **2.25.16 Collaboration Across the Technology Spectrum**: IoT, connectivity, computing, and AI are converging, and stakeholders in different segments of the value chain need to work together, including chip manufacturers, supply chain providers, IoT and electronic communications network equipment providers, AI solutions developers, edge, cloud service providers, and immersive applications providers

In particular, Annex I. Immersive Technologies Standardisation – SDOs Activities of the AIOTI report, "Edge IoT Industrial Immersive Technologies and Spatial Computing Continuum, Release 1", includes Immersive Technologies Standardisation – SDOs Activities in SDOs, such as the 3rd Generation Partnership Project (3GPP), the British Standards Institution (BSI), the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the Spatial Web Foundation (SWF).

Source

"Edge IoT Industrial Immersive Technologies and Spatial Computing Continuum, Release 1", AIOTI WG Research, 30 April 2024 https://aioti.eu/wp-content/uploads/AIOTI-Paper-Edge-AI-IoT-Immersive-Technologies-Published.pdf

Application - Industry Domain

Horizontal (cross-domain)

3. Standardisation Gaps

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

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

3.1 Definition and classification of standardisation gaps

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

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

3.2 Standardisation Gaps: Identification

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

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

- "2.15 User-level Service Management of IoT Network by Utilizing AI",
- "2.16 IoT over ICN",
- "2.20 Open Markets of Digital Services",
- "2.25.4 Industrial Immersive Technologies Challenges -User interface (UI)",
- "2.25.5 Industrial Immersive Technologies Challenges -Intelligent connectivity",
- "2.25.6 Industrial Immersive Technologies Challenges -Blockchain and NFTs",
- "2.25.7 Industrial Immersive Technologies Challenges - Edge IoT immersive platforms",
- "2.25.9 Industrial Immersive Technologies Challenges - Integration of immersive technology",
- "2.25.16 Industrial Immersive Technologies Challenges - Collaboration Across the Technology Spectrum".

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

3.3 Standardisation Gaps: Prioritisation

This section provides a prioritisation of IoT standardisation gaps in terms of their impact in the IoT landscape. The method of prioritising the standardisation gaps is by investigating the standardisation activities in SDOs, such as W3C, OMA, ETSI, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE, including as well key OSSs (Contiki-NG, FIT IoT-LAB Testbed, FIWARE, RIOT OS), and identifying missing or duplicate elements in the IoT standardisation landscape.

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

4. Gap analysis and resolution work in SDOs

4.1 Gap Resolution

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

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

4.2 EUOS identified IoT challenges covered/addressed by SDOs

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

The EUOS "Landscape of Internet of Things (IoT) Standards V2" report has been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives. Using the information applied in this EUOS IoT landscape report an analysis has been done on key SDOs, such as: W3C, OMA, ETSI, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE, including as well key OSSs, to identify whether the EUOS identified IoT challenges, described in Section 2, are covered or addressed by this SDOs. The complete analysis is included in tables, such as Table 1 used as an example in this section to show a short list of the AIOTI/EUOS identified IoT challenges covered/addressed by ETSI. Please note that Annex II shows the complete list of ETSI specifications that are covering the AIOTI/EUOS identified IoT challenges.

The rest of the tables that show how the AIOTI/EUOS identified IoT challenges covered/addressed by key SDOs, such as: W3C, OMA, ETSI, 3GPP, oneM2M, CEN/CENELEC, IEC, ISO/IEC JTC1, ITU-T, IETF, IEEE, including as well key OSSs, are provided in Annex II: "Tables including the AIOTI/EUOS identified IoT challenges covered/addressed by SDOs".

Tables including the EUOS identified IoT challenges covered/addressed by SDOs are shown in Annex II.

Table 1: AIOTI/EUOS identified IoT challenges covered/addressed by ETSI (short list)

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI	(Updated) ETSI TR 102 638 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Release 2	https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/02.01.01_60/tr_102638v020101p.pdf	The present document identifies ITS services, supporting ITS applications functional and system needs, as well as related use cases which are intended to be the baseline for the development of the set of ITS Release 2 and beyond standards. The identified ITS services and use cases do not constitute an exhaustive list and new ones could be included in a new version of the present document.	S2.3, S2.7, S2.14
ETSI	(NEW) ETSI TS 102 731 V2.0.0 ITS; Security; Security Services and Architecture	https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/02.00.00_60/ts_102731v020000p.pdf	The document will specify mechanisms and protocols for secure and privacy-preserving communication in vehicular environments, including vehicle-to-vehicle and vehicle-to infrastructure communication. It will provide credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. It will incorporate mechanisms such as addressing schemes building on pseudonymization concepts, the protocols for address update, and for exchanging, updating, and invalidating credentials to counterfeit attacks on security and reliability of communication. Further methods to prevent malicious tracking of identity and location will be provided.	S2.6, S2.9
ETSI	(NEW) ETSI TS 102 894-2 V2.2.1 ITS; Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	https://www.etsi.org/deliver/etsi_ts/102800_102899/10289402/02.02.01_60/ts_10289402v020201p.pdf	Definition and specifications on the common data container at the applications and facilities layer.	S2.1, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) ETSI TS 103 301 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	http://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01.03.01_60/ts_103301v010301p.pdf	The present document provides specifications of infrastructure related ITS services to support communication between infrastructure ITS equipment and traffic participants using ITS equipment (e.g. vehicles, pedestrians). It defines services in the Facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity. It has been published for both Release 1 (V1.3.1) and Release 2 (V2.1.1) of the ETSI C-ITS standards.	S2.3, S2.7, S2.14
ETSI	(NEW) ETSI TS 103 325 V1.2.1 Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN	https://www.etsi.org/deliver/etsi_ts/103300_103399/103325/01.02.01_60/ts_103325v010201p.pdf	This standard specifies the medium access control and routing for Smart Body Area Networks (Smart BANs). It defines an ultra low power medium access control protocol for on-body communications between a hub and sensor nodes. It also contains provision made for relaying of data through a relay node to the hub.	S2.5
ETSI	ETSI TS 103 596-2 V1.1.1 (2021-05): Test Specification for CoAP; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359602/01.01.01_60/ts_10359602v010101p.pdf	The document provides an introduction and guide for developers and users investigating in security testing of the COAP communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. The structure of the present document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for COAP.	S2.9
			Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the COAP protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TS 103 597-2 V1.1.1 (2021-04): Test Specification for MQTT; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359702/01.01.01_60/ts_10359702v010101p.pdf	The document provides an introduction and guide for developers and users investigating in security testing of the MQTT communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. The structure of the document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for MQTT. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the MQTT protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.	S2.9
ETSI	ETSI TR 103 537 V1.1.1 (2019-09): Plugtests preparation on Semantic Interoperability	https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf	As part of its activities towards platforms interoperability, the document aims at preparing a Plugtests event on Semantic Interoperability. For this Plugtests event, the interoperability will be based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing, with the objective to demonstrate a more practical/industrial use. The document intends to identify the testing requirements from the semantic interoperability standards, especially those collected in ETSI TR 103 535 and ETSI TR 103 536	S2.18
ETSI	ETSI TR 103 778 V1.1.1 (2021-12):	https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf	The scope of this document is to a) identify, select and describe use cases where the IoT data and services require usability specifications; b) analyse the impact of these use cases for both machines and humans.	S2.14
ETSI	(NEW) ETSI TS 103 780 V1.1.1 SmartM2M; SAREF: oneM2M usage guidelines	https://www.etsi.org/deliver/etsi_ts/103700_103799/103780/01.01.01_60/ts_103780v010101p.pdf	The objective of this standard is to provide guidelines for the usage of SAREF over oneM2M (also including the SDT interoperability) for vertical industry sectors.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) ETSI TS 103 849 V1.1.1 Smart M2M; Smart Escalators IoT System	https://www.etsi.org/deliver/etsi_ts/103800_103899/103849/01.01.01_60/ts_103849v010101p.pdf	The scope of this standard is the specification of the IoT system for Smart Escalators. It includes: the identification of the relevant roles; the information models in the Smart Lift system, including signals, alarms and commands; the mapping to the communication system (oneM2M); It is a twin specification of ETSI TS 103.735 “Smart Lift IoT System” and is expected to share most of the technical content with it in light of the similarities among lifts and escalators information systems. it is also expected to be linked with the ontology in TS 103410-11 “SAREF for Lifts”.	S2.1, S2.18
ETSI	(see Annex II for more ETSI specifications)			

5. Standards Gaps Analysis and Recommendations

Section 4.2 of this report together with the Annex II provides an analysis on whether the 40 AIOTI/EUOS identified IoT challenges, specified in Section 2 of this report are covered/worked out in the 670 SDO specifications that were listed in the AIOTI/EUOS "Landscape of Internet of Things (IoT) Standards V2" report.

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

Table 2 gives an overview of the number of specifications and SDOs that are covering / working out each of the EUOS identified IoT challenges.

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

- high intensively covered standardisation gap in SDOs, marked in Table 2 with colour green and is represented in the situation: (*high #SDOs (≥ 4) & high #specs (≥ 8));*
- medium intensively covered standardisation gap in SDOs, marked in Table 2 with colour yellow, and is represented in the situation: (*high #SDOs (≥ 4) & low #specs (< 8)) OR* (*low #SDOs (< 4) & high #specs (≥ 8));*
- low intensively covered standardisation gap in SDOs, marked in Table 2 with colour red, and is represented in the situation: (*low #SDOs (< 4) & low #specs (< 8)).*

Table 2: AIOTI/EUOS identified IoT challenges covered/addressed by SDOs

Challenge number	Description	IEC	ETSI	3GPP	ISO/IEC	CEN/CENELEC	IEEE	ITU	W3C	IETF	IRTF	OneM2M	OMA	Open Source	#SDO	#specs
2.1	Smooth Interoperability between Data Models	55	13	1	10	36	9	18	7	13		5	19		11	186
2.2	Assurance a RESTFUL Data Exchange APIs	7	3			1		2		12	1	2	6		8	34
2.3	Need for real-time or near real-time processing and decision-making	9	12		1	1	3	45							6	71
2.4	Connectiviy Cost				1			2							2	3
2.5	Resilience to Intermittent Services		6		5			9		1					4	21
2.6	Assurance Privacy and Security	13	10	1	23	5	4	23	1	28	2	5			11	115
2.7	Deployment and management of large-scale distributed network of devices	7	13	9	29		12	45	2	94	2	21	1		11	235
2.8	Sustainability, energy consumption, rare minerals and raw materials provisioning	1		1	9			46		1					5	58
2.9	Developing Standards for IoT Security Testing and Validation	7	10		20	2		5		2					6	46
2.10	Developing and Implementing Trustoworthiness for IoT Systems	4	10		12	2	10	15		3					7	56
2.11	IoT and Ethics				2					1					2	3
2.12	IoT Governance and Regulation		1		1			2	1	1					5	6
2.13	Zero Touch Configuration				2			4		1					3	7
2.14	Usability of data and services provided by IoT Devices and platform	3	20		4	1	1	62		1	1	5	1		10	99
2.15	User-level Service Management of IoT Network by Utilizing AI		6	1	1		1	21				2			6	32
2.16	IoT over ICN								3		1				2	4
2.17	Harmonized identification		1		1		1	4	2	2					6	11
2.18	Semantic Interoperability	23	13		8	4	4	3	4	1		2			9	62
2.19	Ethics and Trustoworthiness				2		1								2	3
2.20	Open Markets of Digital Services				1		1								2	2
2.21	Certification of Devices Classes	2	1		2	1	1	12							6	19
2.22	Device Management	12	5	5	4	5	3	2				10	55		9	101
2.23	Simulation and Emulation Environments		2		1			11						4	4	18
2.24	Digital for Green	2	1	2	4	5		25		1					7	40
2.25.1	*Industrial Immersive Technologies* - Advanced HW and edge IoT devices			3	7		8								3	18
2.25.2	*Industrial Immersive Technologies* - New SW and CAD platforms			3	7		7								3	17
2.25.3	*Industrial Immersive Technologies* - Programming languages, libraries, and SW development kits (SDKs)			1			8	1							3	10
2.25.4	*Industrial Immersive Technologies* - User interface (UI)			4	7		8	2							4	21
2.25.5	*Industrial Immersive Technologies* - Intelligent connectivity			5			6	3							3	14
2.25.6	*Industrial Immersive Technologies* - Blockchain and NFTs						2								1	2
2.25.7	*Industrial Immersive Technologies* - Edge IoT immersive platforms							4							1	4
2.25.8	*Industrial Immersive Technologies* - High-quality, robust, reliable, and affordable immersive technologies			7			5	10							3	22
2.25.9	*Industrial Immersive Technologies* - Integration of immersive technology			9	10		9	24							4	52
2.25.10	*Industrial Immersive Technologies* - Interoperability and Standardisation			6	7		19	7							4	39
2.25.11	*Industrial Immersive Technologies* - Data Privacy and Security			4			2	11							3	17
2.25.12	*Industrial Immersive Technologies* - Scalability			2			2	4							3	8
2.25.13	*Industrial Immersive Technologies* - Complexity in Deployment and Management			6	3		3	10							4	22
2.25.14	*Industrial Immersive Technologies* - Ethical and Societal Implications				3		3	18							3	24
2.25.15	*Industrial Immersive Technologies* - Interdisciplinary Integration			1			7	16							3	24
2.25.16	*Industrial Immersive Technologies* - Collaboration Across the Technology Spectrum			6			5	14							3	25

Figure 1 and Figure 2 provide a more detailed overview of the intensity that an IoT standardisation challenge is covered/addressed by an SDO and by specifications, respectively. The IoT challenge labels from S2.1 to S2.25.16, depicted in Figure 1 and Figure 2, are representing the descriptions of the challenges described in Section 2, from subsection 2.1 to subsection 2.25.16, respectively.

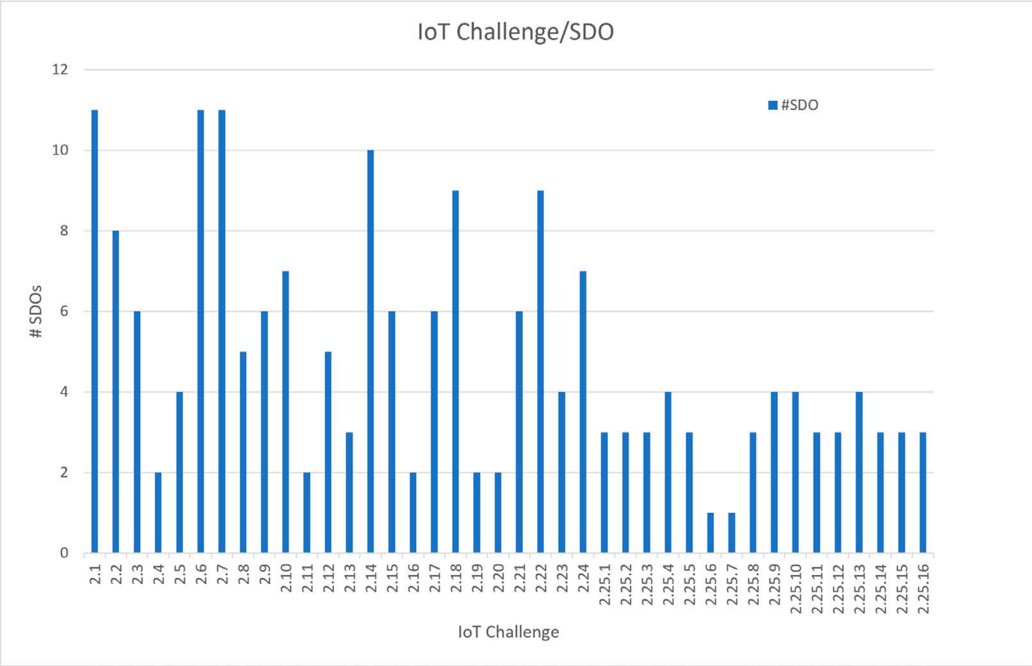

Figure 1: Number of SDOs covering / working out an EUOS IoT identified challenge

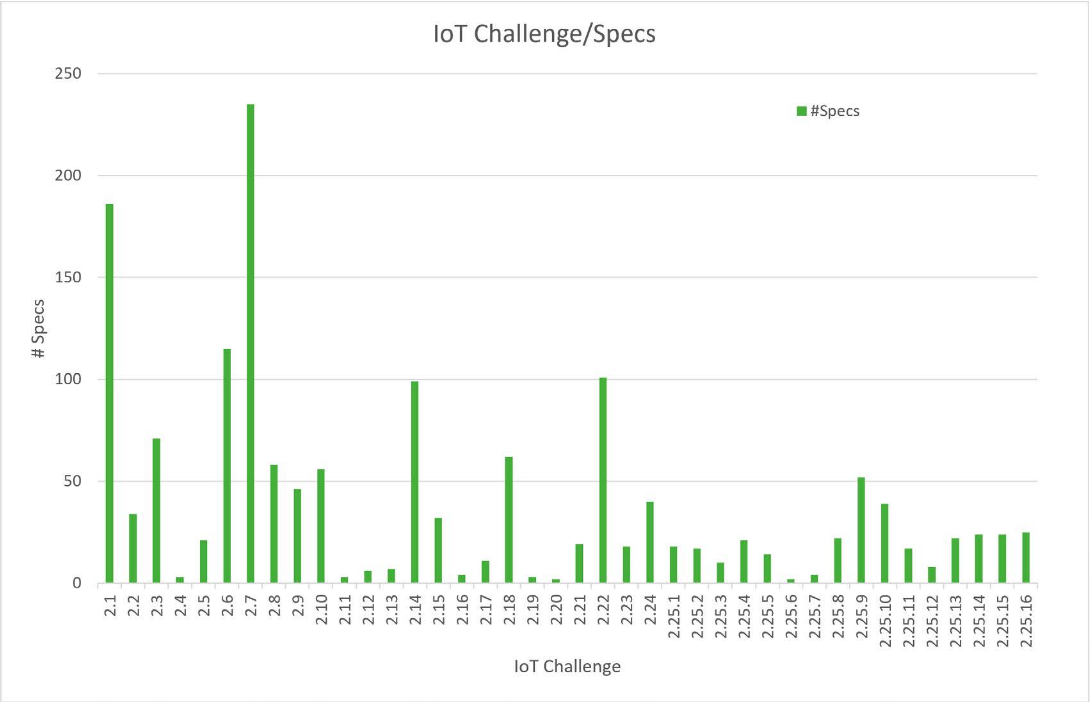

Figure 2: Number of specifications covering / working out an EUOS IoT identified challenge

From this analysis it can be concluded that:

- the following IoT challenges need more research before being standardised:
  - "2.15 User-level Service Management of IoT Network by Utilizing AI",
  - "2.16 IoT over ICN",
  - "2.20 Open Markets of Digital Services",
  - "2.25.4 Industrial Immersive Technologies Challenges -User interface (UI)",
  - "2.25.5 Industrial Immersive Technologies Challenges -Intelligent connectivity",
  - "2.25.6 Industrial Immersive Technologies Challenges -Blockchain and NFTs",
  - "2.25.7 Industrial Immersive Technologies Challenges - Edge IoT immersive platforms",
  - "2.25.9 Industrial Immersive Technologies Challenges - Integration of immersive technology",
  - "2.25.16 Industrial Immersive Technologies Challenges - Collaboration Across the Technology Spectrum".
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work (*Note that that the IoT challenges that need more research before being standardised are not listed below)*:
  - "2.11 IoT and Ethics",
  - "2.19 Ethics and Trustworthiness".
- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work (*Note that that the IoT challenges that need more research before being standardised are not listed below)*:
  - "2.12 IoT Governance and Regulation",
  - "2.13 Zero Touch Configuration",
  - "2.25.1 Industrial Immersive Technologies - Advanced HW and edge IoT devices",
  - "2.25.2 Industrial Immersive Technologies -New SW and CAD platforms",
  - "2.25.3 Industrial Immersive Technologies -Programming languages, libraries, and SW development kits (SDKs)",
  - "2.25.8 Industrial Immersive Technologies -High-quality, robust, reliable, and affordable immersive technologies",
  - "2.25.11 Industrial Immersive Technologies - Data Privacy and Security",
  - "2.25.12 Industrial Immersive Technologies -Scalability",
  - "2.25.14 Industrial Immersive Technologies -Ethical and Societal Implications",
  - "2.25.15 Industrial Immersive Technologies -Interdisciplinary Integration".

6. Conclusion

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

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

The EUOS "Landscape of Internet of Things (IoT) Standards V2" report has been used as a basis for the identification of the specifications and documents that are produced by different initiatives, such as SDOs, Industrial Consortia and Open Source Software (OSS) initiatives.

One of the goals of this document is to start a structured discussion within the EUOS (European Observatory) community and AIOTI community, to provide consolidated technical elements as well as guidance and recommendations.

In particular, Section 2 describes the research and standardisation key IoT challenges, Section 3 describes the identification and prioritisation of the EUOS identified IoT challenges in standardisation gaps, Section 4 describes the gap analysis work in SDOs and Section 5 describes the standardisation gaps analysis and recommendations, and includes the mapping of more than 800 SDOs specifications to the 40 IoT challenges identified by EUOS and presented in Section 2. Based on this analysis it can be concluded that:

- the following IoT challenges need more research before being standardised:
  - "2.15 User-level Service Management of IoT Network by Utilizing AI",
  - "2.16 IoT over ICN",
  - "2.20 Open Markets of Digital Services",
  - "2.25.4 Industrial Immersive Technologies Challenges -User interface (UI)",
  - "2.25.5 Industrial Immersive Technologies Challenges -Intelligent connectivity",
  - "2.25.6 Industrial Immersive Technologies Challenges -Blockchain and NFTs",
  - "2.25.7 Industrial Immersive Technologies Challenges - Edge IoT immersive platforms",
  - "2.25.9 Industrial Immersive Technologies Challenges - Integration of immersive technology",
  - "2.25.16 Industrial Immersive Technologies Challenges - Collaboration Across the Technology Spectrum"
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work (*Note that that the IoT challenge that need more research before being standardised are not listed below)*:
  - "2.11 IoT and Ethics",
  - "2.19 Ethics and Trustworthiness".
- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work (*Note that that the IoT challenge that need more research before being standardised are not listed below)*:
  - "2.12 IoT Governance and Regulation",
  - "2.13 Zero Touch Configuration",
  - "2.25.1 Industrial Immersive Technologies - Advanced HW and edge IoT devices",
  - "2.25.2 Industrial Immersive Technologies -New SW and CAD platforms",
  - "2.25.3 Industrial Immersive Technologies -Programming languages, libraries, and SW development kits (SDKs)",
  - "2.25.8 Industrial Immersive Technologies -High-quality, robust, reliable, and affordable immersive technologies",

- “2.25.11 Industrial Immersive Technologies - Data Privacy and Security”,
- “2.25.12 Industrial Immersive Technologies -Scalability”,
- “2.25.14 Industrial Immersive Technologies -Ethical and Societal Implications”,
- “2.25.15 Industrial Immersive Technologies -Interdisciplinary Integration”.

Annex I: Template used for IoT and/or edge computing challenge-research/standardisation requirement description, for EUOS StandICT.eu 2023 TWG IIoT and Edge Gap Analysis reports

Please fill in the fields

X. Title of IoT and/or edge computing research/standardisation challenge-requirement

<<Title>>

X.1 Type of challenge - requirement (IoT, Edge, IoT and Edge)

Provided the type of the challenge (IoT, Edge, IoT and Edge)

<< Please fill in here >>

X.2 mapping of the described challenge into the class/group/category of challenges

Please study the table with class/group/category of challenges shown in the Annex 1 of this template (Table 1)

<< Please fill in here >>

X.3 Description of IoT and/or edge computing challenge-research/standardisation requirement

Provide motivation of having this IoT and/or edge computing research/standardisation requirement

<< Please fill in here >>

Provide the description of the requirement<<>>

<< Please fill in here >>

Type of Requirement, see explanation and examples of functional and non-functional requirements, below) –

<< Please fill in here >>

These requirements can be split in:

- Functional requirements

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

- Non-functional requirements

Functional Requirement (Examples)

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

Non-Functional Requirement (Examples)

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

X.4 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.5 Application/Industry domain:

Define in which Application/Industry domain the challenge applies to (see explanation below):

<< Please fill in here ->>

Horizontal (cross-domain), Health, Mobility, Energy, Buildings, Agriculture, Manufacturing, Urban Society, etc.

Annex II: Tables including the AIOTI/EUOS identified IoT challenges covered/addressed by SDOs

Table 3: AIOTI/EUOS indentified IoT challenges covered/addressed by IEC

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	(Updated) IEC 61406 ED1 Identification Link - Part 1: General requirements	https://webstore.iec.ch/publication/67673	IEC 61406-1:2022 specifies minimum requirements for a globally unique identification of physical objects which also constitutes a link to its related digital information. This identification is designated hereinafter as "Identification Link" (IL), with the encoded data designated as IL string. The IL string has the data-format of a link (URL). The IL is machine-readable and is attached to the physical object in a 2D symbol or NFC tag. The requirements in this standard apply to physical objects: that are provided by the manufacturer as an individual unit, and that have already been given a unique identity by the manufacturer. This document does not specify any requirements on the content and the layout of nameplates/typeplates (e.g. spatial arrangement, content of the plain texts, approval symbols etc.).	S2.1, S2.14, S2.17
IEC	IEC 60869-1:2018	https://webstore.iec.ch/publication/60884	IEC 60869-1:2018 is available as (https://webstore.iec.ch/publication/64221)IEC 60869-1:2018 RLV, which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 60869-1:2018 applies to fibre optic passive power control devices. These have all of the following general features: they are passive in that they contain no optoelectronic or other transducing elements; they have two ports for the transmission of optical power and control of the transmitted power in a fixed or variable fashion; – the ports are non-connectorized optical fibre pigtails, connectorized optical fibres or receptacles. This document establishes generic requirements for the following passive optical devices:	S2.3

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			optical attenuator; optical fuse; optical power limiter. This document also provides generic information including terminology for the IEC 61753-05x series. Published IEC 61753-05x series documents are listed in Bibliography This fifth edition cancels and replaces the fourth edition published in 2012 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) the terms and definitions have been reviewed; b) the requirement concerning the IEC Quality Assessment System has been reviewed; c) the clause concerning quality assessment procedures has been deleted; d) Annex G, relating to technical information on variable optical attenuators, has been added. Keywords: fibre optic passive power control devices	
IEC	IEC 60875-1:2015	https://webstore.iec.ch/publication/22396	IEC 60875-1:2015 applies to non-wavelength-selective fibre optic branching devices, all exhibiting the following features: - they are passive, in that they contain no optoelectronic or other transducing elements; - they have three or more ports for the entry and/or exit of optical power, and share optical power among these ports in a predetermined fashion; - the ports are optical fibres, or optical fibre connectors. This standard establishes uniform requirements for the optical, mechanical and environmental properties. This sixth edition cancels and replaces the fifth edition published in 2010 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: - removal of terms and definitions for splitter, coupler, symmetric non-wavelength-selective branching device, asymmetric non-wavelength-selective branching device;	S2.3

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			- addition of terms and definitions for bidirectional non-wavelength-selective branching device and non-bidirectional non-wavelength-selective branching device, removal of assessment level. Keywords: non-wavelength-selective fibre optic branching devices, uniform requirements for the optical, mechanical and environmental properties	
IEC	IEC 61300-1:2022	https://webstore.iec.ch/publication/67663	The document IEC 61300-1:2022 contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. In particular, 61300-1:2022 provides general information and guidance for the basic test and measurement procedures defined in IEC 61300-2 (all parts) and IEC 61300-3 (all parts) for interconnecting devices, passive components, mechanical splices, fusion splice protectors, fibre management systems and protective housings. This document is used in combination with the relevant specification which defines the tests to be used, the required degree of severity for each of them, their sequence, if relevant, and the permissible performance limits. In the event of conflict between this document and the relevant specification, the latter takes precedence. This fifth edition cancels and replaces the fourth edition published in 2016. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: - addition of the information of measurement uncertainties in 4.2.1; - change of the requirements for attenuation variation in 4.2.2; - addition of the multimode launch conditions of other fibres than A1-OM2, A1-OM3, A1-OM4, A1-OM5 and A3e in 10.4; - addition of the multimode launch conditions of the planer waveguide in 10.6; - splitting Annex A for EF and Annex B for EAF; - correction of errors in the definitions of encircled flux and encircled angular flux.	S2.3, S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	(NEW) IEC 61406-2:2024 Identification link - Part 2: Types/ models, lots/batches, items and characteristics (Under development)	://www.iec.ch/dyn/www/f?p=103:38:510268376806243::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,112292	IEC 61406-2:2024 complements IEC 61406-1 by providing additional requirements for those cases where data elements are encoded within the Structured Identification Link string with standardized syntax and semantics. In addition, this document covers cases where the uniqueness relates to product types/models or lots/batches. The default assumption is that the Identification Link identifies unique objects such as unique serialized products, assets, persons or packages, unless otherwise identified.	S2.1, S2.14, S2.17
IEC	IEC 61753-1:2018	https://webstore.iec.ch/publication/67249	The document IEC 61753-1:2018 contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 61753-1:2018 provides guidance for the drafting of performance standards for all passive fibre optic products. This document defines the tests and severities which form the performance categories or general operating service environments and identifies those tests which are considered to be product specific. Test and severity details are given in Annex A. This second edition cancels and replaces the first edition published in 2007. It constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) definitions updated with new products: wall outlets, wall or pole mounted boxes, splices, ODF modules, street cabinets, hardened connectors and field mountable connectors; b) categories U and O are replaced by categories OP and OP+. No mandatory sequence in category OP+. Category OP+ contains the tests from category OP with the addition of only 4 other tests; c) addition of Category I (Industrial); d) temperature ranges added (with the HD suffix to the categories C, OP, OP+ and I) in case passive optical components are placed in a housing together with active electronics (HD stands for “heat dissipation”); e) the height of category A changed from 3 m to ground level (0 m); f) the lower level height of category G environment changed from ground level (0 m) to –1 m below ground level. Upper level remains at 3 m above ground level;	S2.3, S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			g) addition of performance tests, test severities and performance criteria for new products: Wall outlet, wall or pole mounted boxes, mechanical splices, fusion splice protectors, ODF modules, street cabinets, field mountable connectors and hardened optical connectors; h) test severity of "Mating durability" test for connectors in categories C, OP ,OP+ and I is reduced to 200 cycles for connectors with cylindrical ferrules and 50 cycles for connectors with rectangular ferrules; i) test severity of "Change of temperature" test for connectors and passive optical components in category I is reduced from 20 cycles to 12 cycles (harmonized with connectors and components from other categories); j) test severity of "Flexing of strain relief" test for connectors in categories C, OP and OP+ is reduced to 50 cycles; k) test severities of "Assembly and disassembly of fibre optic mechanical splices, fibre management systems and closures" test for all enclosures is reduced to 5 cycles; l) test severities of "Change of temperature" test for all protective housings in categories C, A, G and S is reduced from 20 cycles to 12 cycles (harmonized with connectors and components); m) test severities of "Resistance to solvents and contaminating fluids" test for closures in categories G and S changed – kerosene is removed, diesel oil exposure reduced to 1 h immersion and 24 h drying at room temperature; n) sealing performance criteria of sealed closures for categories G and A are reduced to 20 kPa overpressure. o) the change in attenuation criterion for connectors has changed from peak-to-peak into a +/- deviation from the original value of the transmitted power at the start of the test (harmonized with the change in attenuation criterion for components, splices and protective housings). Keywords: performance standards for all passive fibre optic products. The contents of the corrigendum of May 2019 have been included in this copy.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	IEC 61754-4:2022	https://webstore.iec.ch/publication/29284	The document IEC 61754-4:2022 contains the International Standard and its Red-line version, showing all changes of the technical content compared to the previous edition. IEC 61754-4:2021 specifies the standard interface dimensions for type SC family of connectors. This third edition cancels and replaces the second edition published in 2013 and constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: - the test method IEC 61300-3-22 for the compression force of the ferrule was added; - Annex A (informative) with cut out dimension requirements for testing the strength of mounted adaptors was added.	S2.3, S2.9, S2.21
IEC	IEC 61754-7-3:2019	https://webstore.iec.ch/publication/26692	IEC 61754-7-3: 2019 defines the standard interface dimensions for type MPO family of connectors with two rows of 16 fibres. Keywords: interface dimensions for type MPO connectors	S2.3, S2.21
IEC	IEC 61756-1:2019	https://webstore.iec.ch/publication/59508	IEC 61756-1:2019 covers general information on fibre management system interfaces. It includes the definitions and rules under which a fibre management system interface is created and it provides also criteria to identify the minimum bending radius for stored fibres. This document allows both single-mode and multimode fibre to be used. Liquid, gas or dust sealing requirements at the cable entry area or cable element ending are not covered in this document. This second edition cancels and replaces the first edition published in 2006. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: - addition of figures to show the interface between protective housing and fibre management system; - addition of definitions for protective housing, closure, wall box, street cabinets and optical distribution frame modules; - addition of table with dimensions of fusion splice protectors and mechanical splices; - addition of method to identify the minimum bending radius for stored fibres; - addition of clause for other factors relevant to fibre management systems;	S2.3

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			- addition of annex A for example of calculating the minimum bending radius of stored fibres in a fibre management system. Keywords: fibre management system interfaces, minimum bending radius for stored fibres	
IEC	IEC 62005-1:2001	https://webstore.iec.ch/publication/6280	IEC 62005-1:2001 is a guide for assessing the reliability of all types of fibre-optic interconnecting devices and passive optical components. It applies to passive devices for connection, branching, switching, minimization of reflection, control of power/attenuation, dispersion compensation, modulation and wavelength selection or filtering.	S2.3
IEC	IEC 62099:2001	https://webstore.iec.ch/publication/6459	IEC 62099:2001 applies to fibre optic wavelength switches, which are: - passive optical devices, without optical amplification or opto-electronic conversion - restricted to the routing of light rather than intentional power division - have two or more ports with optical fibres or connectors. The standard establishes switch requirements and quality assessment procedures.	S2.3
IEC	IEC 62541-10:2020	https://webstore.iec.ch/publication/61119	IEC 62541-10:2020 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-10:2020 defines the information model associated with Programs in the OPC Unified Architecture. This includes the description of the NodeClasses, standard Properties, Methods and Events and associated behaviour and information for Programs. The complete Address Space model including all NodeClasses and Attributes is specified in IEC 62541-3. The Services such as those used to invoke the Methods used to manage Programs are specified in IEC 62541 4. This third edition cancels and replaces the second edition published in 2015. This edition includes several clarifications and in addition the following significant technical changes with respect to the previous edition: a) Changed ProgramType to ProgramStateMachineType. This is in line with the NodeSet (and thus implementations). In ProgramDiagnosticDataType: changed the definition of lastInputArguments and lastOutputArguments and added two additional fields for the argument values.	S2.1, S2.18, S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
			Also changed StatusResult into Status-Code. Created new version of the type to ProgramDiagnostic2DataType. b) Changed Optional modelling rule to OptionalPlace-Holder for Program control Methods. Following the clarification in IEC 62541-3, this now allows subtypes (or instances) to add arguments.	
IEC	IEC 62541-100:2015	https://webstore.iec.ch/publication/21987	IEC 62541-100:2015 is an extension of the overall OPC Unified Architecture standard series and defines the information model associated with Devices. This part of IEC 62541 describes three models which build upon each other: - the (base) Device Model intended to provide a unified view of devices; - the Device Communication Model which adds Network and Connection information elements so that communication topologies can be created; - the Device Integration Host Model finally which adds additional elements and rules required for host systems to manage integration for a complete system. It allows reflecting the topology of the automation system with the devices as well as the connecting communication networks.	S2.1, S2.18, S2.22
IEC	IEC 62541-13:2020	https://webstore.iec.ch/publication/61131	IEC 62541-13:2020 contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-13:2020 is part of the overall OPC Unified Architecture specification series and defines the information model associated with Aggregates. This second edition cancels and replaces the first edition of IEC 62541-13, published in 2015. No technical changes but numerous clarifications. Also some corrections to the examples.	S2.1, S2.22
IEC	IEC 62541-14:2020	https://webstore.iec.ch/publication/61108	IEC 62541-14:2020 defines the OPC Unified Architecture (OPC UA) PubSub communication model. It defines an OPC UA publish subscribe pattern which complements the client server pattern defined by the Services in IEC 62541-4. IEC TR 62541-1 gives an overview of the two models and their distinct uses. PubSub allows the distribution of data and events from an OPC UA information source to interested observers inside a device network as well as in IT and analytics cloud systems.	S2.1, S2.2,S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
			This document consists of a) a general introduction of the PubSub concepts, b) a definition of the PubSub configuration parameters, c) mapping of PubSub concepts and configuration parameters to messages and transport protocols, and d) a PubSub configuration model. Not all OPC UA Applications will need to implement all defined message and transport protocol mappings. IEC 62541-7 defines the Profile that dictates which mappings need to be implemented in order to be compliant with a particular Profile.	
IEC	IEC 62541-3:2020	https://webstore.iec.ch/publication/61112	IEC 62541-3:2020 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-3:2020 defines the OPC Unified Architecture (OPC UA) AddressSpace and its Objects. This document is the OPC UA meta model on which OPC UA information models are based. This third edition cancels and replaces the second edition published in 2015. This edition includes the following significant technical changes with respect to the previous edition: a) Added new improved approach for exposing structure definitions. An Attribute on the DataType Node now simply contains a binary description. b) Added new flags for Variables to indicate atomicity when reading or writing. c) Added Roles and Permissions to allow configuration of a role-based authorization. d) Added new data types: "Union", "Decimal", "OptionSet", "DateString", "TimeString", "DurationString", NormalizedString", "DecimalString", and "AudioDataType". e) Added definition on how to use the ModellingRules OptionalPlaceHolder and MandatoryPlaceHolder for Methods. f) Added optional Properties "MaxCharacters" and "MaxByteStringLength" to Variable Nodes.	S2.1, S2.18, S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62541-4:2020	https://webstore.iec.ch/publication/61113	IEC 62541-4:2020 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-4:2020 defines the OPC Unified Architecture (OPC UA) Services. The Services defined are the collection of abstract Remote Procedure Calls (RPC) that are implemented by OPC UA Servers and called by OPC UA Clients. All interactions between OPC UA Clients and Servers occur via these Services. The defined Services are considered abstract because no particular RPC mechanism for implementation is defined in this document. IEC 62541-6 specifies one or more concrete mappings supported for implementation. For example, one mapping in IEC 62541-6 is to XML Web Services. In that case the Services described in this document appear as the Web service methods in the WSDL contract. Not all OPC UA Servers will need to implement all of the defined Services.	S2.1, S2.2, S2.18,S2.22
			IEC 62541-7 defines the Profiles that dictate which Services need to be implemented in order to be compliant with a particular Profile This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) Added ability to resend all data of monitored items in a Subscription using the ResendData Method. b) Added support for durable Subscriptions (lifetime of hours or days). c) Added Register2 and FindServersOnNetwork Services to support network-wide discovery using capability filters. d) Removed definition of software certificates. Will be defined in a future edition. e) Extended and partially revised the redundancy definition. Added sub-range definitions for ServiceLevel and added more terms for redundancy. f) Added a section on how to use Authorization Services to request user access tokens. g) Added JSON Web Tokens (JWTs) as a new user token. h) Added the concept of session-less service invocation. i) Added a generic structure that allows passing any number of attributes to the AddNodes Service. j) Added requirement to protect against user identity token attacks. k) Added new EncryptedSecret format for user identity tokens.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62541-5:2020	https://webstore.iec.ch/publication/61114	IEC 62541-5:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-5:2020 defines the Information Model of the OPC Unified Architecture. The Information Model describes standardized Nodes of a Server's AddressSpace. These Nodes are standardized types as well as standardized instances used for diagnostics or as entry points to server-specific Nodes. Thus, the Information Model defines the AddressSpace of an empty OPC UA Server. However, it is not expected that all Servers will provide all of these Nodes. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) Added Annex F on User Authentication. Describes the Role Information Model that also allows configuration of Roles. b) Added new data types: "Union", "Decimal", "OptionSet", "DateString", "TimeString", "DurationString", NormalizedString", "DecimalString", and "AudioDataType". c) Added Method to request a state change in a Server. d) Added Method to set Subscription to persistent mode. e) Added Method to request resending of data from a Subscription. f) Added concept allowing to temporarily create a file to write to or read from a server in C.4. g) Added new Variable type to support Selection Lists. h) Added optional properties to FiniteStateMachineType to expose currently available states and transitions. i) Added UrisVersion Property to ServerType. This version information can be used for session-less service invocation.	S2.1, S2.2, S2.18, S2.22
IEC	IEC 62541-6:2020	https://webstore.iec.ch/publication/61115	IEC 62541-6:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-6:2020 specifies the OPC Unified Architecture (OPC UA) mapping between the security model described in IEC TR 62541-2, the abstract service definitions specified in IEC 62541-4, the data structures defined in IEC 62541-5 and the physical network protocols that can be used to implement the OPC UA specification. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition:	S2.1,S2.2, S2.18,S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			Encodings: added JSON encoding for PubSub (non-reversible); added JSON encoding for Client/Server (reversible); added support for optional fields in structures; added support for Unions. Transport mappings: added WebSocket secure connection – WSS; added support for reverse connectivity; added support for session-less service invocation in HTTPS. Deprecated Transport (missing support on most platforms): SOAP/HTTP with WS-SecureConversation (all encodings). d) Added mapping for JSON Web Token. e) Added support for Unions to NodeSet Schema. f) Added batch operations to add/delete nodes to/from NodeSet Schema. g) Added support for multi-dimensional arrays outside of Variants. h) Added binary representation for Decimal data types. i) Added mapping for an OAuth2 Authorization Framework.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62541-7:2020	https://webstore.iec.ch/publication/61116	IEC 62541-7:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-7:2020 defines the OPC Unified Architecture (OPC UA) Profiles. The Profiles in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs. This could equally as well refer to test tools provided by another organization or a test lab provided by another organization. What is important is the concept of automated tool-based testing versus lab-based testing. The scope of this standard includes defining functionality that can only be tested in a lab and defining the grouping of functionality that is to be used when testing OPC UA products either in a lab or using automated tools.	S2.1, S2.2, S2.9,S2.18,S2.22
			The definition of actual TestCases is not within the scope of this document, but the general categories of TestCases are within the scope of this document. Most OPC UA applications will conform to several, but not all, of the Profiles. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) new functional Profiles: profiles for global discovery and global certificate management; profiles for global KeyCredential management and global access token management; facet for durable subscriptions; standard UA Client Profile; profiles for administration of user roles and permissions. b) new transport Profiles: HTTPS with JSON encoding; secure WebSockets (WSS) with binary or JSON encoding; • reverse connectivity.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			new security Profiles: transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy); securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15); securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP); user Token JWT (Jason Web Token). d) deprecated Security Profiles (due to broken algorithms): securityPolicy – Basic128Rsa15 (broken algorithm Sha1); securityPolicy – Basic256 (broken algorithm Sha1); transportSecurity – TLS 1.0 (broken algorithm RC4); transportSecurity – TLS 1.1 (broken algorithm RC4). deprecated Transport (missing support on most platforms): SOAP/HTTP with WS-SecureConversation (all encodings).	
IEC	IEC 62541-8:2020	https://webstore.iec.ch/publication/61117	IEC 62541-8:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-8:2020 is part of the overall OPC Unified Architecture (OPC UA) standard series and defines the information model associated with Data Access (DA). It particularly includes additional VariableTypes and complementary descriptions of the NodeClasses and Attributes needed for Data Access, additional Properties, and other information and behaviour. The complete address space model, including all NodeClasses and Attributes is specified in IEC 62541-3. The services to detect and access data are specified in IEC 62541-4. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) added new VariableTypes for AnalogItems; b) added an Annex that specifies a recommended mapping of OPC UA Dataccess to OPC COM DataAccess; c) changed the ambiguous description of "Bad_NotConnected"; d) updated description for EUInformation to refer to latest revision of UNCEFACT units.	S2.1,; S2.2, S2.9,S2.18,S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62541-9:2020	https://webstore.iec.ch/publication/61118	IEC 62541-9:2020 contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62541-9:2020 specifies the representation of Alarms and Conditions in the OPC Unified Architecture. Included is the Information Model representation of Alarms and Conditions in the OPC UA address space. Other aspects of alarm systems such as alarm philosophy, life cycle, alarm response times, alarm types and many other details are captured in documents such as IEC 62682 and ISA 18.2. The Alarms and Conditions Information Model in this specification is designed in accordance with IEC 62682 and ISA 18.2. This third edition cancels and replaces the second edition published in 2015. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) added optional engineering units to the definition of RateOfChange alarms; b) to fulfill the IEC 62682 model, the following elements have been added: - AlarmConditionType States: Suppression, Silence, OutOfService, Latched; - AlarmConditionType Properties: OnDelay, OffDelay, FirstInGroup, ReAlarmTime; - New alarm types: DiscrepencyAlarm, DeviationAlarm, InstrumentDiagnosticAlarm, SystemDiagnosticAlarm. c) added Annex that specifies how the concepts of this OPC UA part maps to IEC 62682 and ISA 18.2; d) added new ConditionClasses: Safety, HighlyManaged, Statistical, Testing, Training; e) added CertificateExpiration AlarmType; f) added Alarm Metrics model.	S2.1,S2.2, S2.9, S2.18 S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62714-1:2018	https://webstore.iec.ch/publication/32339	IEC 62714-1:2018 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. IEC 62714-1:2018 is a solution for data exchange focusing on the domain of automation engineering. The data exchange format defined in the IEC 62714 series (Automation Markup Language, AML) is an XML schema based data format and has been developed in order to support the data exchange in a heterogeneous engineering tools landscape. The goal of AML is to interconnect engineering tools in their different disciplines, e.g. mechanical plant engineering, electrical design, process engineering, process control engineering, HMI development, PLC programming, robot programming, etc. This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) use of CAEX 3.0 according to IEC 62424:2016 b) improved modelling of references to documents outside of the scope of the present standard, c) modelling of references between CAEX attributes and items in external documents, d) revised role libraries, e) modified Port concept, f) modelling of multilingual expressions, g) modelling of structured attribute lists or array, h) a new AML container format, i) a new standard AML attribute library	S2.1,S2.18
	IEC 62714-2:2015	https://webstore.iec.ch/publication/22030	IEC 62714-2:2015 specifies normative as well as informative AML role class libraries for the modelling of engineering information for the exchange between engineering tools in the plant automation area by means of AML. Moreover, it presents additional user defined libraries as an example. Its provisions apply to the export/import applications of related tools.	S2.1, S2.18
IEC	IEC 62714-3:2017	https://webstore.iec.ch/publication/34158	IEC 62714-3:2017 specifies the integration of geometry and kinematics information for the exchange between engineering tools in the plant automation area by means of AML.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62714-4:2020	https://webstore.iec.ch/publication/28979	IEC 62714-4:2020 specifies the integration of logic information as part of an AML model for the data exchange in a heterogenous engineering tool landscape of production systems. This document specifies three types of logic information: sequencing, behaviour, and interlocking information. This document deals with the six following sequencing and behaviour logic models (covering the different phases of the engineering process of production systems) and how they are integrated in AML: Gantt chart, activity-on-node network, timing diagram, Sequential Function Chart (SFC), Function Block Diagram (FBD), and mathematical expression. This document specifies how to model Gantt chart, activity-on-node network, and timing diagram and how they are stored in Intermediate Modelling Layer (IML). This document specifies how interlocking information is modelled (as interlocking source and target groups) in AML. The interlocking logic model is stored in Function Block Diagram (FBD). This document specifies the AML logic XML schema that stores the logic models by using IEC 61131-10. This document specifies how to reference PLC programs stored in PLCopen XML documents. This document does not define details of the data exchange procedure or implementation requirements for the import/export tools. The contents of the corrigendum of November 2020 have been included in this copy.	S2.1, S2.18
IEC	IEC 62714-5:2022	https://webstore.iec.ch/publication/65493	IEC 62714-5:2022 Engineering processes of technical systems and their embedded automation systems are executed with increasing efficiency and quality. Especially since the project duration tends to increase as the complexity of the engineered system increases. To solve this problem, the engineering process is more often being executed by exploiting software based engineering tools exchanging engineering information and artefacts along the engineering process related tool chain.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	(Updated) IEC 63365 ED1 Digital Nameplate – Digital Product Marking	https://webstore.iec.ch/en/publication/67436	IEC 63365:2022 Industrial process measurement, control and automation - Digital nameplate IEC 63365:2022 applies to products used in the process measurement, control and automation industry. It establishes a concept and requirements for the digital nameplate and provides alternative electronically readable solutions (e.g. 2D codes, RFID or firmware) to current conventional plain text marking on the nameplate or packaging of products. The digital nameplate information is contained in the electronically readable medium affixed to the product, the packaging or accompanying documents. The digital nameplate information is available offline without Internet connection. After electronic reading, all digital nameplate information is displayed in a human readable text format. The digital nameplate also includes the Identification Link String according to IEC 61406-1 which provides additional online information for the product. This document does not specify the contents of the conventional nameplate, which are subject to regional or national regulations and standards.	S2.1, S2.17
IEC	IEC TR 62541-1:2020	https://webstore.iec.ch/publication/61109	IEC TR 62541-1:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-1:2020 presents the concepts and overview of the OPC Unified Architecture (OPC UA). Reading this document is helpful to understand the remaining parts of this multi-part document set. Each of the other parts of IEC 62451 is briefly explained along with a suggested reading order.	S2.1, S2.18
IEC		https://www.iec.ch/dyn/www/f?p=103:38:731054763917753::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109017	Under development	
IEC	IEC 61987-1:2006	https://webstore.iec.ch/publication/6225	IEC 61987-1:2006 defines a generic structure in which product features of industrial-process measurement and control equipment with analogue or digital output should be arranged, in order to facilitate the understanding of product descriptions when they are transferred from one party to another. It applies to the production of catalogues of process measuring equipment supplied by the manufacturer of the product and helps the user to formulate his requirements.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61987-10:2009	https://webstore.iec.ch/publication/6227	IEC 61987-10:2009 provides a method of standardizing the descriptions of process control devices, instrumentation and auxiliary equipment as well as their operating environments and operating requirements (for example, measuring point specification data). The aims of this standard are: - to define a common language for customers and suppliers through the publication of Lists of Properties (LOPs), - to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations, - to reduce transaction costs. The standard describes industrial-process device types and devices using structured lists of properties and makes the associated properties available in a component data dictionary. This bilingual version, published in 2010-11, corresponds to the English version. The French version of this standard has not been voted upon. This publication is to be read in conjunction with http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/37363">IEC 61987-1:2006	
IEC	IEC 61987-11:2016	https://webstore.iec.ch/publication/32275	IEC 61987-11:2016 provides: - a characterisation of industrial process measuring equipment (device type dictionary) for integration in the Common Data Dictionary (CDD), and - generic structures for operating lists of properties (OLOP) and device lists of properties (DLOP) of measuring equipment in conformance with IEC 61987-10. This second edition cancels and replaces the first edition published in 2012. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: a) The classification in Table A.1 has been amended to reflect the changes in the classification scheme of process measuring equipment in the CDD due to the development of IEC 61987-14, IEC 61987-15 and IEC 61987-16. b) Annex A has become "informative".	S2.1
IEC	IEC 61987-12:2016	https://webstore.iec.ch/publication/24401	IEC 61987-12:2016 provides an operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for a flow measuring equipment and device lists of properties (DLOP) for the description of a number of flow measuring equipment types.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61987-13:2016	https://webstore.iec.ch/publication/24400	IEC 61987-13:2016 provides an operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for a pressure measuring equipment, and device lists of properties (DLOP) for a range of pressure measuring equipment types describing them.	S2.1
IEC	IEC 61987-14:2016	https://webstore.iec.ch/publication/24637	IEC 61987-14:2016 provides an operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for temperature measuring equipment and device lists of properties (DLOP) for the description of a range of contact and non-contact temperature measuring equipment types.	S2.1
IEC	IEC 61987-15:2016	https://webstore.iec.ch/publication/26177	IEC 61987-15:2016 provides operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for level measuring equipment, and device lists of properties (DLOPs) for the description of a range of level measuring equipment types.	S2.1
IEC	IEC 61987-16:2016	https://webstore.iec.ch/publication/34265	IEC 61987-16:2016 provides an - operating list of properties (OLOP) for the description of the operating parameters and the collection of requirements for a density measuring equipment, and - device lists of properties (DLOP) for a range of density measuring equipment types describing them. The structures of the OLOP and the DLOP correspond with the general structures defined in IEC 61987-11 and agree with the fundamentals for the construction of LOPs defined in IEC 61987-10.	
IEC	IEC 61987-32 ED1	https://www.iec.ch/ords/f?p=103:38:401030832849310::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,102293	Under development	
IEC	IEC 61987-41 ED1	https://www.iec.ch/ords/f?p=103:38:401030832849310::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,107355	Under development	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61987-92:2018	https://webstore.iec.ch/publication/33096	IEC 61987-92:2018 provides the lists of properties (LOPs) describing aspects of equipment for industrial-process automation that is subject to IEC 61987 standard series. This standard series proposes a method for standardization which will help both suppliers and users of measuring equipment to optimize workflows both within their own companies and in their exchanges with other companies. IEC 61987-92 contains additional aspects that are common to all devices, for example, "Packaging and transportation", "Calibration and test results" and "Device documents supplied". The structures of the LOPs correspond to the general structures defined in IEC 61987-11 and agree with the fundamentals for the construction of LOPs defined in IEC 61987-10. Libraries of properties and of blocks used in the aspect LOPs are listed in Annex B and Annex C.	S2.1
IEC	IEC 62443-2-1:2010	https://webstore.iec.ch/publication/7030	IEC 62443-2-1:2010 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization. This bilingual version (2012-04) corresponds to the monolingual English version, published in 2010-11.	S2.6, S2.10
IEC	IEC 62443-4-2:2019	https://webstore.iec.ch/publication/34421	IEC 62443-4-2:2019 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C (component). As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs): a) identification and authentication control (IAC), b) use control (UC), c) system integrity (SI), d) data confidentiality (DC), e) restricted data flow (RDF), f) timely response to events (TRE), and g) resource availability (RA). These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope. Show less	S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	IEC 62832-1:2020	https://webstore.iec.ch/publication/65858	IEC 62832-1:2020 defines the general principles of the Digital Factory framework (DF framework), which is a set of model elements (DF reference model) and rules for modelling production systems. This DF framework defines: a) model of production system assets; b) a model of relationships between different production system assets; c) the flow of information about production system assets. d) The DF framework does not cover representation of building construction, input resources (such as raw production material, assembly parts), consumables, work pieces in process, nor end products.. e) It applies to the three types of production processes (continuous control, batch control, and discrete control) in any industrial sector (for example aeronautic industries, automotive, chemicals, wood).	S2.1
IEC	IEC 62832-2:2020	https://webstore.iec.ch/publication/60214	IEC 62832-2:2020 specifies detailed requirements for model elements of the Digital Factory framework. It defines the nature of the information provided by the model elements, but not the format of this information.	S2.1
IEC	IEC 62832-3:2020	https://webstore.iec.ch/publication/60277	IEC 62832-3:2020 specifies rules of the Digital Factory framework for managing information of a production system throughout its life cycle. It also defines how the information will be added, deleted or changed in the Digital Factory by the various activities during the life cycle of the production system.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62872-2:2022	https://webstore.iec.ch/publication/63419	IEC 62872-2:2022 presents an IoT application framework for industrial facility demand response energy management (FDREM) for the smart grid, enabling efficient information exchange between industrial facilities using IoT related communication technologies. This document specifies: - an overview of the price-based demand response program that serves as basic knowledge backbone of the IoT application framework; - a IoT-based energy management framework which describes involved functional components, as well as their relationships; - detailed information exchange flows that are indispensable between functional components; - existing IoT protocols that need to be identified for each protocol layer to support this kind of information exchange; - communication requirements that guarantee reliable data exchange services for the application framework.	S2.1, S2.8, S2.24
IEC	(Updated) IEC 63278-1 ED1 Asset Administration Shell for industrial applications – Part 1: Asset Administration Shell structure	https://webstore.iec.ch/publication/65628	IEC 63278-1:2023 defines the structure of a standardized digital representation of an asset, called Asset Administration Shell (AAS). The Asset Administration Shell gives uniform access to information and services. The purpose of the Asset Administration Shell is to enable two or more software applications to exchange information and to mutually use the information that has been exchanged in a trusted and secure way. This document focuses on Asset Administration Shells representing assets of manufacturing enterprises including products produced by those enterprises and the full hierarchy of industrial equipment. It defines the related structures, information, and services. The Asset Administration Shell applies to: any type of industrial process (discrete manufacturing, continuous process, batch process, hybrid production); any industrial sector applying industrial-process measurement, control and automation;	S2.1, S2.17, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	(NEW) IEC 63278-2 ED1 Asset Administration Shell for Industrial Applications – Part 2: Information meta model (Under development)	https://www.iec.ch/dyn/www/f?p=103:38:502560904033881::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109017	This document focuses on the Asset Administration Shell for Industrial Applications – Part 2: Information meta model. This document is under development.	S2.1, S2.17, S2.18
IEC	IEC 63278-3 ED1	https://www.iec.ch/dyn/www/f?p=103:38:731054763917753::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,109075	IEC 63278-3 ED1: Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells (Under development)	S2.1, S2.17, S2.18
IEC	(NEW) IEC 63278-4 ED1 Asset administration shell for industrial applications - Part 4: Use cases and modelling examples (Under development)	https://www.iec.ch/dyn/www/f?p=103:38:508054836884348::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,116472	This document focuses on the Asset Administration Shell for Industrial Applications – Part 4: Use cases and modelling examples. This document is under development.	S2.1, S2.17, S2.18
IEC	(NEW) IEC 63278-5 ED1 Asset Administration Shell for industrial applications – Part 5: Interfaces (Under development)	https://www.iec.ch/dyn/www/f?p=103:38:508054836884348::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,121674	This document focuses on the Asset Administration Shell for Industrial Applications – Part 5: Interfaces. This document is under development.	S2.1, S2.17, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	(Updated) IEC 63339 ED1 Unified reference model for smart manufacturing (2024-10)	https://www.iec.ch/dyn/www/f?p=103:38:731054763917753::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,104329	IEC 63339:2024 ED1 (EN) specifies the unified reference model for smart manufacturing (URMSM) using a terminology and structure, and establishes criteria for creating reference models, as specializations, that support smart manufacturing. The terminology and structure comprise a set of common modelling elements, their associations, and conformance criteria. These common modelling elements address aspects and perspectives of products and production and their lifecycle considerations. The URMSM enables an approach for creating multiple models based upon a reference model that is sufficient for understanding significant relationships among entities involved in smart manufacturing (SM) and for the development of standards and other specifications.	S2.1, S2.18
IEC	(Updated) IEC 63376 ED1 INDUSTRIAL FACILITY ENERGY MANAGEMENT SYSTEM (FEMS) – Functions and Information Flows (2024-02)	https://webstore.iec.ch/publication/67721	IEC 63376:2023 specifies the functions and the information flows of industrial Facility Energy Management System (FEMS). Generic functions are defined for the FEMS, to enable upgrading traditional Energy Management System (EMS) from visualization of the status of energy consumption to automation of energy management defining a closer relation with other management and control systems. A generic method to classify the FEMS functions will be explained. The information exchange between the FEMS and other systems such as Manufacturing Operations Management (MOM), Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) will be outlined.	S2.1, S2.24
IEC	IEC TS 62443-1-1:2009	https://webstore.iec.ch/publication/7029	IEC/TS 62443-1-1:2009(E) is a technical specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.	S2.1, S2.6
IEC	IEC TS 62872-1:2019	https://webstore.iec.ch/publication/62884	IEC 62872-1:2019(E) defines the interface, in terms of information flow, between industrial facilities and the "smart grid". It identifies, profiles and extends where required, the standards needed to allow the exchange of the information needed to support the planning, management and control of electric energy flow between the industrial facility and the smart grid. The scope of this document specifically excludes the protocols needed for the direct control of energy resources within a facility where the control and ultimate liability for such control is delegated by the industrial facility to the external entity (e.g. distributed energy resource (DER) control by the electrical grid operator).	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	(NEW) IEC 63203-801-1	https://www.iec.ch/dyn/www/f?p=103:38:615499235431339::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20537,23,103719	This part of IEC 63203-801 specifies the ultra-low power physical layer (PHY) Smart BAN. As the use of wearables and connected body sensor devices grows rapidly in the Internet of Things (IoT), Wireless Body Area Networks (BAN) facilitate the sharing of data in smart environments such as smart homes, smart life etc. In specific areas of digital healthcare, wireless connectivity between the edge computing device or hub coordinator and the sensing nodes requires a standardized communication interface and protocols. The present document describes the Physical Layer (PHY) specifications: - packet formats; - modulation; - forward error correction	S2.1, S2.7
IEC	(Updated) IEC 63203-801-2	https://www.iec.ch/dyn/www/f?p=103:38:615499235431339::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20537,23,103720	This part of IEC 63203-801 specifies low complexity Medium Access Control (MAC) for SmartBAN. As the use of wearables and connected body sensor devices grows rapidly in the Internet of Things (IoT), Wireless Body Area Networks (BAN) facilitate the sharing of data in smart environments such as smart homes, smart life etc. In specific areas of digital healthcare, wireless connectivity between the edge computing device or hub coordinator and the sensing nodes requires a standardized communication interface and protocols. The present document describes the MAC specifications: - Channel Structure, - MAC Frame Formats, - MAC functions.	S2.1, S2.7
IEC		https://www.iec.ch/basecamp/internet-things-wireless-sensor-networks	Wireless sensor networks (WSN) are generating increasing interest from industry and research. This is driven by the availability of inexpensive, low-powered miniature components such as processors, radios and sensors which are sometimes integrated on a single chip. The idea of the Internet of Things (IoT) developed in parallel to WSNs. While IoT doesn't assume a specific communication technology, wireless communication technologies will play a major role in the roll-out of IoT. WSNs will drive many applications and many industries. This white paper discusses the use and evolution of WSNs in the wider context of IoT. It provides a review of WSN applications, infrastructures technologies, applications as well as standards that apply to WSN designs. The white paper was prepared by the IEC Market Strategy Board (MSB) wireless sensor networks project team in cooperation with the US National Institute of Standards and Technology (NIST).	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	(Updated) IEC 61987-31 ED1	https://webstore.iec.ch/en/publication/63343	IEC 61987-31:2022 ED1: Industrial-process measurement and control - Data structures and elements in process equipment catalogues - Part 31: List of Properties (LOPs) of infrastructure devices for electronic data exchange – Generic structures IEC 61987-31:2022 provides a characterization for the integration of infrastructure devices in the Common Data Dictionary (CDD); generic structures in conformance with IEC 61987-10 for Operating Lists of Properties (OLOPs) and Device Lists of Properties (DLOPs) of infrastructure devices. The generic structures for the OLOP and DLOP contain the most important blocks for infrastructure devices. Blocks pertaining to a specific equipment type will be described in the corresponding part of the IEC 61987 series. Similarly, equipment properties are not part of this part of IEC 61987. For instance, the OLOP and DLOP for I/O-modules are to be found in IEC 61987-32.	S2.1, S2.18
IEC		https://www.iec.ch/basecamp/iec-role-iot	This brochure provides a detailed overview of IEC work that directly impacts the Internet of Things. It explains why standardization is needed for the M2M world of Connected Services. The important role of sensors and MEMS. How nanotechnology will impact IoT. Big Data and the cloud and why data privacy and security willincrease in importance and how cyber security work can help. How the IoT applies in energy and the Smart Grid, smart buildings and homes, lighting as well as Smart Cities. How IEC work contributes to smart manufacturing and Industry 4.0. and why IoT will become more important in healthcare, personal safety, mobility and even for universal energy access, for example through LVDC.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC		https://www.iec.ch/basecamp/iot-2020-smart-and-secure-iot-platform	The internet of things (IoT) is an infrastructure of interconnected objects, people or systems that processes and reacts to physical and virtual information. IoT collectively uses today's internet backbone to connect things using sensors and other technologies. Through data collection and analysis it achieves a multitude of outcomes that generally aim to improve user experience or the performance of devices and systems. How data is collected and implemented will determine how transformational IoT can become. Security grows exponentially in importance as devices that were once isolated become interconnected and more and more information is collected. As with most disruptive technologies solutions are developed by a wide range of providers promoting their proprietary approaches which can also impact interconnectivity. Bringing the ambitious visions expressed by IoT to reality will require significant efforts in standardization. This white paper aims to provide an overview of today's IoT, including its limitations and deficiencies in the area of security, interoperability and scalability. It contains use cases that point to requirements for smart and secure IoT platforms. It also discusses next generation platform-level technologies and provides important recommendations to IoT stakeholders and for IoT standardization work. The white paper was prepared by the IEC Market Strategy Board (MSB) IoT 2020 project team with major contributions from SAP and the Fraunhofer Institute for Applied and Integrated Security AISEC.	S2.7
IEC	IEC 62443-3-2:2020	https://webstore.iec.ch/publication/30727	IEC 62443-3-2:2020 establishes requirements for: · defining a system under consideration (SUC) for an industrial automation and control system (IACS); · partitioning the SUC into zones and conduits; · assessing risk for each zone and conduit; · establishing the target security level (SL-T) for each zone and conduit; and · documenting the security requirements.	S2.1, S2.6
IEC	IEC 62443-2-4:2015	https://webstore.iec.ch/publication/22810	IEC 62443-2-4:2015 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. The contents of the corrigendum of August 2015 have been included in this copy.	S2.1, S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 62443-3-2:2020	https://webstore.iec.ch/publication/30727	IEC 62443-3-2:2020 establishes requirements for: a) defining a system under consideration (SUC) for an industrial automation and control system (IACS); b) partitioning the SUC into zones and conduits; c) assessing risk for each zone and conduit; d) establishing the target security level (SL-T) for each zone and conduit; and e) documenting the security requirements.	S2.1, S2.6
IEC	IEC 62443-3-3:2013	https://webstore.iec.ch/publication/7033	IEC 62443-3-3:2013 provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset. The contents of the corrigendum of April 2014 have been included in this copy.	S2.1, S2.6
IEC	IEC 62443-4-2:2019	https://webstore.iec.ch/publication/34421	Preview Abstract IEC 62443-4-2:2019 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component). As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs): a) identification and authentication control (IAC), b) use control (UC), c) system integrity (SI), d) data confidentiality (DC), e) restricted data flow (RDF), f) timely response to events (TRE), and g) resource availability (RA). These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.	S2.1, S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC TR 62443-2-3:2015	https://webstore.iec.ch/publication/22811	IEC TR 62443-2-3:2015(E) describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. This Technical Report recommends a defined format for the distribution of information about security patches from asset owners to IACS product suppliers, a definition of some of the activities associated with the development of the patch information by IACS product suppliers and deployment and installation of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however, it may also be applicable for non-security related patches or updates.	S2.1, S2.6
IEC	IEC TR 62443-3-1:2009	https://webstore.iec.ch/publication/7031	IEC/TR 62443-3-1:2009(E) provides a current assessment of various cybersecurity tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cybersecurity technology products and/or countermeasures.	S2.1, S2.6, S2.10
IEC	IEC TR 62541-2:2020	https://webstore.iec.ch/publication/61110	IEC TR 62541-2:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-2:2020 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and Profiles that are specified normatively in other parts of the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.	S2.1, S2.6, (S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	EC 63237-1 ED1	https://www.iec.ch/dyn/www/f?p=103:7:602873313141987::::FSP_ORG_ID,FSP_LANG_ID:1275,25	This part of IEC 63237 provides a method of standardizing the descriptions of household electrical appliances. The aims of this standard are: a) to define a common language for customers and suppliers through the publication of classes, represented by properties and their attributes; b) enable electronic data exchange by machines (including information technology systems, see M2M communication); c) to optimize workflows between customers and suppliers as well as in processes such as engineering, development and purchasing within their own organizations; d) to offer also a dictionary to legislators and; e) to reduce transaction costs. The standard describes household electrical appliances using properties and makes the associated properties available in the IEC Common Data Dictionary (IEC CDD). Furthermore, this document provides rules, methods and the generic data structure for product specific classification standards and on how to produce a reference dictionary based on IEC 61360 Series. This in turn creates a descriptive basis of company internal and external descriptions of household electrical appliances based on structured classes and lists of properties.	S2.1, S2.18
IEC	(NEW) IEC Cloud-watch D3.6 Cloud-watch D3.6 Security and Interop-er ability Standards Status Report	https://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Security-and-Interoperability-Standards-Status-Report.pdf	This document provides a monitoring of the standards landscape, identifying necessary extensions and profiles, and identifying relevant standards groups for future engagement of the EU projects. Through this deliverable Cloud WATCH2 is able to: Leverage input provided by finalized and on-going FP7 and H2020 projects to prepare and maintain a list of standards used by the different consortia. The list describes the level of adoption of each standard and the most common implementations. Identify contributions to existing and developing standards from the FP7 and H2020 projects. Provide evidence to the standardization community of identified gaps by analysing input from the above mentioned FP7 and H2020 projects.	S2.6, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	(NEW) IEC 61406-2:2024 Identification link - Part 2: Types/models, lots/batches, items and characteristics	https://webstore.iec.ch/publication/77973		S2.1, S2.7
IEC	IEC TR 63283-1:2022	https://webstore.iec.ch/publication/66314	IEC TR 63283-1:2022(E) is to compile a comprehensive collection of base terminology with compatible terms that can become relevant within the scope of Smart Manufacturing. Most of these terms refer to existing definitions in the domain of industrial-process measurement, control and automation and its various subdomains. When multiple similar definitions exist for the exact same term in different standards, this document contains only the preferred definition in the context of Smart Manufacturing. Whenever the existing definitions are not compatible with other terms in this document or when the definition does not fit into the broader scope of Smart Manufacturing, new or modified definitions are given.	S2.1
IEC	(NEW) IEC TR 63283-2:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 2: Use cases	https://webstore.iec.ch/publication/66315	IEC TR 63283-2:2022(EN) has the goal of analyzing the impact of "Smart Manufacturing" on the daily operation of an industrial facility. It focusses on the perspective of automation and control of the production system, but also on the supporting processes of ordering, supply chain management, design, engineering and commissioning, operational technology, life cycle management, and resource management. These recommendations are accomplished on the basis of several carefully selected use cases that are familiar to manufacturing industry. Therefore, each use case is described, followed by an analysis of the possible influence of "Smart Manufacturing" and the assessment of the impact on existing and future standardization.	S2.1, S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IEC	(NEW) IEC TR 63283-3:2022 Industrial-process measurement, control and automation - Smart manufacturing - Part 3: Challenges for cybersecurity	https://webstore.iec.ch/publication/66316	IEC TR 63283-3:2022(E) identifies challenges which apply to the engineering of a smart manufacturing facility related to cybersecurity.	S2.1, S2.6, S2.9
IEC	(NEW) IEC TR 63283-5:2024 Industrial-process measurement, control and automation – Smart manufacturing – Part 5: Market and innovation trends analysis.	https://webstore.iec.ch/en/publication/71399	IEC TR 63283-5:2024 describes the market and innovation trend analysis affecting smart manufacturing (SM). The market and innovation trends will influence the evolution of smart manufacturing and it will be important to have good insights on these trends. Specific aspects of the market trends are the evolution of the business cases that is assumed to highlight new supplier chain models, new revenue streams, new customer services, and/or new customer segments. The document will address the following topics: Market watch: Identify the important, likely, and/or disruptive market trends (e.g. mass customization) from an end-to-end perspective, which impact smart manufacturing topics/aspects. This includes the end-user, producers, supply chain, regulators, etc. Business model watch: Identify the new business model trends from an end-to-end perspective, which impact smart manufacturing. Technological watch: Identify the important, likely, and/or disruptive innovations (AI chipsets, 6G, quantum computing, etc.) describing the impacted smart manufacturing topics/aspects; this topic will focus on those technologies that are still under development but is assumed to influence (or is assumed to be influenced by) smart manufacturing. There are many more new trends which are used in SM. In this document, only some frequently discussed trends are presented. Some technologies are considered to have priority according to their maturity. This work will focus on how they can be used in SM.	S2.14

Table 4: AIOTI/EUOS indentified IoT challenges covered/addressed by ETSI

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(Updated) ETSI TR 102 638 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Release 2	https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/02.01.01_60/tr_102638v020101p.pdf	The present document identifies ITS services, supporting ITS applications functional and system needs, as well as related use cases which are intended to be the baseline for the development of the set of ITS Release 2 and beyond standards. The identified ITS services and use cases do not constitute an exhaustive list and new ones could be included in a new version of the present document.	S2.3, S2.7, S2.14
ETSI	(NEW) ETSI TS 102 731 V2.0.0 ITS; Security; Security Services and Architecture	https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/02.00.00_60/ts_102731v020000p.pdf	The document will specify mechanisms and protocols for secure and privacy-preserving communication in vehicular environments, including vehicle-to-vehicle and vehicle-to infrastructure communication. It will provide credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. It will incorporate mechanisms such as addressing schemes building on pseudonymization concepts, the protocols for address update, and for exchanging, updating, and invalidating credentials to counterfeit attacks on security and reliability of communication. Further methods to prevent malicious tracking of identity and location will be provided.	S2.6, S2.9
ETSI	(NEW) ETSI TS 102 894-2 V2.2.1 ITS; Users and applications requirements; Part 2: Applications and facilities layer common data dictionary	https://www.etsi.org/deliver/etsi_ts/102800_102899/10289402/02.02.01_60/ts_10289402v020201p.pdf	Definition and specifications on the common data container at the applications and facilities layer.	S2.1, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) ETSI TS 103 301 V2.1.1 ITS; Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services	http://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01.03.01_60/ts_103301v010301p.pdf	The present document provides specifications of infrastructure related ITS services to support communication between infrastructure ITS equipment and traffic participants using ITS equipment (e.g. vehicles, pedestrians). It defines services in the Facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity. It has been published for both Release 1 (V1.3.1) and Release 2 (V2.1.1) of the ETSI C-ITS standards.	S2.3, S2.7, S2.14
ETSI	(NEW) ETSI TS 103 325 V1.2.1 Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN	https://www.etsi.org/deliver/etsi_ts/103300_103399/103325/01.02.01_60/ts_103325v010201p.pdf	This standard specifies the medium access control and routing for Smart Body Area Networks (Smart BANs). It defines an ultra low power medium access control protocol for on-body communications between a hub and sensor nodes. It also contains provision made for relaying of data through a relay node to the hub.	S2.5
ETSI	ETSI TS 103 596-2 V1.1.1 (2021-05): Test Specification for CoAP; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359602/01.01.01_60/ts_10359602v010101p.pdf	The document provides an introduction and guide for developers and users investigating in security testing of the COAP communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. The structure of the present document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for COAP. Concrete practical hints and samples and configuration notes are provided where feasible.	S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			The latter two clauses focus on the security mechanisms and implementation notes mentioned in the COAP protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI	
ETSI	ETSI TS 103 597-2 V1.1.1 (2021-04): Test Specification for MQTT; Part 2: Security Tests	https://www.etsi.org/deliver/etsi_ts/103500_103599/10359702/01.01.01_60/ts_10359702v010101p.pdf	The document provides an introduction and guide for developers and users investigating in security testing of the MQTT communication protocol. It will be a reference base for both client side test campaigns and server side test campaigns addressing the security issues. The structure of the document consists of four main clauses: the first two clauses address the security test objectives, techniques and methods to be considered for MQTT. Concrete practical hints and samples and configuration notes are provided where feasible. The latter two clauses focus on the security mechanisms and implementation notes mentioned in the MQTT protocol standard and security vulnerabilities known from relevant vulnerability databases. Concrete test purposes have been described using the Test Description Language (TDL) standardized by ETSI.	S2.9
ETSI	ETSI TR 103 537 V1.1.1 (2019-09): Plugtests preparation on Semantic Interoperability	https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf	As part of its activities towards platforms interoperability, the document aims at preparing a Plugtests event on Semantic Interoperability. For this Plugtests event, the interoperability will be based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing, with the objective to demonstrate a more practical/industrial use. The document intends to identify the testing requirements from the semantic interoperability standards, especially those collected in ETSI TR 103 535 and ETSI TR 103 536	S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI	ETSI TR 103 778 V1.1.1 (2021-12):	https://www.etsi.org/deliver/etsi_tr/103700_103799/103778/01.01.01_60/tr_103778v010101p.pdf	The scope of this document is to a) identify, select and describe use cases where the IoT data and services require usability specifications; b) analyse the impact of these use cases for both machines and humans.	S2.14
ETSI	(NEW) ETSI TS 103 780 V1.1.1 SmartM2M; SAREF: oneM2M usage guidelines	https://www.etsi.org/deliver/etsi_ts/103700_103799/103780/01.01.01_60/ts_103780v010101p.pdf	The objective of this standard is to provide guidelines for the usage of SAREF over oneM2M (also including the SDT interoperability) for vertical industry sectors.	S2.1, S2.18
ETSI	(NEW) ETSI TS 103 849 V1.1.1 Smart M2M; Smart Escalators IoT System	https://www.etsi.org/deliver/etsi_ts/103800_103899/103849/01.01.01_60/ts_103849v010101p.pdf	The scope of this standard is the specification of the IoT system for Smart Escalators. It includes: the identification of the relevant roles; the information models in the Smart Lift system, including signals, alarms and commands; the mapping to the communication system (oneM2M); It is a twin specification of ETSI TS 103.735 "Smart Lift IoT System" and is expected to share most of the technical content with it in light of the similarities among lifts and escalators information systems. it is also expected to be linked with the ontology in TS 103410-11 "SAREF for Lifts".	S2.1, S2.18
ETSI	ETSI GS MEC 033 V3.1.1 (2022-12): Multi-access Edge Computing (MEC); IoT API	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/033/03.01.01_60/gs_MEC033v030101p.pdf	The present document defines the IoT API to assist the deployment and usage of devices that require additional support in a MEC environment, e.g. due to security constraints, limited power, compute and communication capabilities, such as IoT and MTC devices. The API enables the device provisioning and configuration of the associated components and applications requiring connection to these devices. The present document describes the information flows and the required information. It also specifies the RESTful binding with the data model.	S2.2 S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI/ oneM2M	ETSI TR 118 551 V2.0.0 (2020-11): oneM2M API guide	http://www.etsi.org/deliver/etsi_tr/118500_118599/118551/02.00.00_60/tr_118551v020000p.pdf	The guide will list the CRUDN messages for managing some of the main resources defined in TS-0001. It aims at providing the description and associated flow in basic examples. It is foreseesn to use HTTP binding and JSON serialization as example. Other binding and serialization could be considered later, or in a companion document. It also aims to use this list as a common sets of APIs and extend them to include other APIs (such as 3GPP interworking) so developers will have an option to write applications that can run across different platforms and specific implementations.	S2.2
ETSI	ETSI TR 103 675 V1.1.1 (2020-12): AI for IoT: A Proof of Concept	http://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf	The present document is addressing the development of a Proof of Concept based on three Use Cases analysed and selected in the associated ETSI TR 103 674. ETSI TR 103 674 addresses the issues related to the introduction of AI into IoT systems and, as first priority, into the oneM2M architecture. ETSI TR 103 674 has identified and described several Use Cases of which three are used for the development of the Proof of Concept described in the present document.	S2.15
ETSI	ETSI TR 103 674 V1.1.1 (2021-02): Artificial Intelligence and the oneM2M architecture	http://www.etsi.org/deliver/etsi_tr/103600_103699/103674/01.01.01_60/tr_103674v010101p.pdf	In order to maximize the benefits of integrating Artificial Intelligence and Machine Learning (ML), oneM2M has to, on the one hand, support the data-centric approach of AI/ML and its huge requirements in terms of resources available in the cloud domain as well as at the edge of the IoT network. On the other hand, AI is also an opportunity for oneM2M to provide open solutions to applications and services developers together with maintaining and enlarging its core asset of support to interoperability. The present document analyses the implications of AI on IoT systems and, as first priority, the oneM2M architecture.	S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI	ETSI SR 003 680 V1.1.1 (2020-03): Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach	http://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr_003680v010101p.pdf	The present document focuses on questions related to privacy, security, platforms interoperability and semantic interoperability that are addressed from different angles and not just from a simple technical perspective. Tables present "Frequently Asked Questions" with the intent to illustrate major questions in IoT, and their solutions in an easily digestible form. The present document offers some strategic, operational and technical guidelines, which intend to fix the issues addressed in it.	S2.18
ETSI	ETSI TR 103 533 V1.1.1 (2019-08): Security; Standards Landscape and best practices	http://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr_103533v010101p.pdf	The present document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT. And it provides an overview of the existing Security Standards Landscape with the focus on usage in the IoT domains, collect best practices from national and European IoT initiatives/projects, and provide guidance for understanding Compliance to IoT Cyber Security Package. This work is expected to be developed in close collaboration with the European Commission Internet of Things unit E4 and Cybersecurity unit H1, AIOTI WG3+WG4, ETSI TC CYBER, ENISA, ECSO and related PPPs.	S2.6
ETSI	ETSI TR 103 535 V1.1.1 (2019-10): Guidelines for using semantic interoperability in the industry	http://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf	The main objective of the present document is to push semantic interoperability in IoT forward in raising awareness about its importance in industry in order to unlock the potential economic value of IoT. A major focus is on the development of guidelines on how to use semantic interoperability in the industry.	S2.6 S2.1 S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TR 103 536 V1.1.2 (2019-12): Strategic/technical approach on how to achieve interoperability/ interworking of existing standardized IoT Platforms	http://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf	The present document is addressing the issues related to the interoperability and interworking of IoT platforms, in particular standardized IoT platforms, and how the way they are handled can foster their adoption by the IoT community.	S2.1
ETSI	ETSI TR 103 591 V1.1.1 (2019-10): Privacy study report; Standards Landscape and best practices	http://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf	The present document elaborates on how to ensure effective protection of individuals' privacy in the IoT environment. It acknowledges the challenges for privacy and data protection and stresses the necessity for a human centred approach.	S2.12
ETSI/ oneM2M	ETSI TR 118 518 V2.5.1 (2020-07): Industrial Domain Enablement	www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.05.01_60/tr_118518v020501p.pdf	Industrial domain is expectd to be able to improve efficiency and flexibility by utilizing ICT technology: collecting data from devices in multiple factories, analyzing them, and applying the analysis results to decisions. So, it is desirable to utilize oneM2M standardized technology in the industrial domain. To better understand the special requirements to support the operations of the industrial environment, it is desirable to conduct studies on various functionalities that are keen to support this purpose so as to identify necessary technical works to enhance the future oneM2M specifications. This work item is intended to study such functionalities and the results of that study will be presented in a Technical Report.	S2.3
ETSI	ETSI TR 103 438 V1.1.1 (2019-02): User centric approach in Digital Ecosystem	http://www.etsi.org/deliver/etsi_tr/103400_103499/103438/01.01.01_60/tr_103438v010101p.pdf	The goal of this TR is to consider Digital Ecosystem through user's point of view under the following two directions: - identification of user's needs such as QoS, security, usability, flexibility, Service Level Objectives (SLO) - study impact of technical implementations related to user's requirements/concerns	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TS 103 701 V1.1.1 (2021-08): Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf	The present document specifies a conformance assessment methodology for consumer IoT devices, their relation to associated services and corresponding relevant processes. It intends to support suppliers or implementers of consumer IoT products in first-party assessment (self-assessment), user organizations in second party assessment, independent testing organizations in third party assessment and certification and conformance declaration scheme owners in operating harmonized schemes.	S2.21
ETSI / oneM2M	ETSI TR 103 716 V1.1.1 (2021-04): oneM2M Discovery and Query solution(s) simulation and performance evaluation	http://www.etsi.org/deliver/etsi_tr/103700_103799/103716/01.01.01_60/tr_103716v010101p.pdf	This work will develop a simulation with the goal to provide a proof of concept and a performance evaluation to support the selection and development of the discovery and query solution to be contributed to oneM2M. An extract of the simulation results will be used to support the discussion and the proposal with oneM2M.	S2.23
ETSI	ETSI TR 103 621 V1.2.1 (2022-09): Guide to Cyber Security for Consumer Internet of Things	http://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf	The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.	S2.6
ETSI	ETSI TR 103 582 V1.1.1 (2019-07): Study of use cases and communications involving IoT devices in provision of emergency situations	http://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf	The purpose of the present document is to consider communications involving IoT devices in all types of emergency situations, such as emergency calling, mission critical communications, Public Warning System communications and a new domain identified as automated emergency response, and to prepare the potential standardization requirements enabling a safe operation of these communications.	S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI / oneM2M	ETSI TR 118 567 V4.0.0 (2021-11): oneM2M: Study on Management Object migration to SDT	http://www.etsi.org/deliver/etsi_tr/118500_118599/118567/04.00.00_60/tr_118567v040000p.pdf	The present document studies the completion of SDT (Smart Device Template) using <flexContainer> resource specializations and the possible migration of the existing device management model using Management Object (<mgmtObj>). The present document is initiated in the context of the Management Object Migration.	S2.22
ETSI / oneM2M	ETSI TS 118 122 V3.0.2 (2021-01): oneM2M; Field Device Configuration	http://www.etsi.org/deliver/etsi_ts/118100_118199/118122/02.03.01_60/ts_118122v020301p.pdf	The present document specifies the architectural options, resources and procedures needed to pre-provision and maintain devices in the Field Domain (e.g. ADN, ASN/MN) in order to establish M2M Service Layer operation between the device's AE and/or CSE and a Registrar and/Hosting CSE. The resources and procedures includes information about the Registrar CSE and/or Hosting CSE needed by the AE or CSE to begin M2M Service Layer operation.	S2.22
ETSI	ETSI TS 103 779 V1.1.1 (2022-05): Requirements and Guidelines for cross-domain data usability of IoT devices	http://www.etsi.org/deliver/etsi_ts/103700_103799/103779/01.01.01_60/ts_103779v010101p.pdf	The recommendations captured in the present document address the full machine learning pipeline. For maximum benefit the entire system should apply these recommendations, but each individual component or actor in the system can implement the relevant guidelines to provide a better outcome for the usability of the data generated from sensors and machine learning based solutions. The intended audience of the present document are IoT sensor module developers, IoT platform and service providers, machine learning model developers, application developers and IoT consumers.	S2.15 S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	http://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf	The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. Moreover, the present document addresses security considerations specific to constrained devices. The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. Table B.1 provides a schema for the reader to give information about the implementation of the provisions.	S2.6, S2.10
			Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document. The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.	
ETSI	ETSI TS 103 646 V1.1.1	https://www.etsi.org/deliver/etsi_ts/103600_103699/103646/01.01.01_60/ts_103646v010101p.pdf	The present document provides a test specification based on selected security requirements as known from IEC 6244-4-2. The chosen requirements have been collected by defining a dedicated IoT profile. The resulting IoT profile represents a generic minimum security level for IoT devices. Advanced requirements for higher security demands have been excluded. The present document serves as reference for a test campaign addressing the foundational security requirements of the IoT-Profile. The standardized notation TDL-TO has been applied for the definition of test purposes as it supports a unified presentation and semantics.	S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI DTS 103 942	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66187	Assemble security related functional modules within an IoT architecture, that support Security by Design and trustworthiness in order to retrieve relevant security testing methods and specific detailed test purposes using TDL-TO for generic IoT architectures applicable in multiple industrial domains.	S2.9
ETSI	(Updated) ETSI TR 103 946 Methods for Testing and Specification (MTS); Security validation of IoT architecture application and conformity Case Study Experiences	https://www.etsi.org/deliver/etsi_tr/103900_103999/103946/01.01.01_60/tr_103946v010101p.pdf	The goal of the present document is to compile case study experiences related to the security validation and assurance for the integration and conformity of IoT applications with an existing IoT architecture in order to have a common understanding in MTS and related committees and to support trustworthiness. Industrial experiences may cover but are not restricted to the following domains: smart home, smart grid, unmanned air systems, automated driving.	S2.9
ETSI	ETSI EG 202 798 ITS; Testing; Framework for conformance and interoperability testing	http://www.etsi.org/deliver/etsi_eg/202700_202799/202798/01.01.01_60/eg_202798v010101p.pdf	This document specifies the global framework for conformance and interoperability testing in ITS.	S2.9
ETSI	ETSI EN 300 175-1 Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview	http://www.etsi.org/deliver/etsi_en/300100_300199/30017501/02.09.01_60/en_30017501v020901p.pdf	This standard gives an introduction and overview of the complete Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI). It contains an abstract of the other parts of the DECT standard together with a general description of: the objectives of the standard; the DECT Common Interface; the protocol architecture of DECT. The standard also provides an extensive vocabulary; in particular it contains the common definitions of all the technical terms used in different parts of the standard. The standard includes New Generation DECT, a further development of the DECT standard introducing wideband speech, improved data services, new slot types and other technical enhancements. The standard includes DECT Evolution.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This is the first part of a multi-part standard with Part 1: Overview; Part 2: Physical Layer (PHL); Part 3: Medium Access Control (MAC) layer; Part 4: Data Link Control (DLC) layer; Part 5: Network (NWK) layer; Part 6: Identities and addressing; Part 7: Security features; Part 8: Speech and audio coding and transmission.	
ETSI	ETSI EN 302 065-1 Short Range Devices (SRD) using Ultra Wide Band technology (UWB); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Requirements for Generic UWB applications	http://www.etsi.org/deliver/etsi_en/302000_302099/30206501/02.01.01_60/en_30206501v020101p.pdf	This standard applies to transceivers, transmitters and receivers utilizing Ultra WideBand (UWB) technologies and used for short range applications. It applies to impulse, modified impulse and RF carrier based UWB communication technologies. The standard applies to fixed (indoor only), mobile or portable applications, e.g.: stand-alone radio equipment with or without its own control provisions; plug-in radio devices intended for use with, or within, a variety of host systems, e.g. personal computers, hand-held terminals, etc.; plug-in radio devices intended for use within combined equipment, e.g. cable modems, set-top boxes, access points, etc.; combined equipment or a combination of a plug-in radio device and a specific type of host equipment. It is the first part of a multi-part standard, with Part 1: Requirements for Generic UWB applications; Part 2: Requirements for UWB location tracking; Part 3: Requirements for UWB devices for ground based vehicular applications; Part 4: Material Sensing devices using UWB technology below 10,6 GHz; Part 5: Devices using UWB technology onboard aircraft.	S2.5, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI EN 302 636-1 ITS; Vehicular Communications; GeoNetworking; Part 1: Requirements	http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf	This document is the first part of a multi-part standard. It specifies the general, functional and performance requirements that apply to the GeoNetworking protocols. It is applicable to ITS stations implementing ETSI ITS for both single hop and multi-hop communications.	S2.3, S2.7
ETSI	ETSI EN 302 637-2 ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service	http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.01_60/en_30263702v010401p.pdf	Cooperative awareness within road traffic means that road users and roadside infrastructure are informed about each other's position, dynamics and attributes. Road users are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians and roadside infrastructure equipment including road signs, traffic lights or barriers and gates. The awareness of each other is the basis for several road safety and traffic efficiency applications with many use cases as described in ETSI TR 102 638. It is achieved by regular exchange of information among vehicles (V2V, in general all kind of road users) and between vehicles and road side infrastructure (V2I and I2V) based on wireless networks, called V2X network and as such is part of Intelligent Transport Systems (ITS). The information to be exchanged for cooperative awareness is packed up in the periodically transmitted Cooperative Awareness Message (CAM). The construction, management and processing of CAMs is done by the Cooperative Awareness basic service (CA basic service), which is part of the facilities layer within the ITS communication architecture.	S2.3, S2.7, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI EN 302 637-3 ITS; Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service	http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.03.01_60/en_30263703v010301p.pdf	The DEN basic service is an application support facility provided by the ITS facilities layer. It constructs, manages and processes the Decentralized Environmental Notification Message (DENM). The construction of a DENM is triggered by an ITS-S application. A DENM contains information related to a road hazard or an abnormal traffic conditions, such as its type and its position. Typically for an ITS application, a DENM is disseminated to ITS-S that are located in a geographic area through communications among ITS stations. At the receiving side, the DEN basic service of an receiving ITS-S processes the received DENM and provides the DENM content to an ITS-S application.	S2.3, S2.7, S2.14
ETSI	ETSI EN 302 663 ITS; ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.01_60/en_302663v010301p.pdf	The present document specifies the European profile of the physical and medium access control sub-layer of 5 GHz intelligent transport systems (ITS) using IEEE 802.11 as the base standard. One of the additionally selected functionalities being an essential part of the present document is "communication outside the context of a BSS" as developed by IEEE 802.11. Communication outside the context of a BSS enables exchange of data frames between stations that are not members of a BSS. This type of communication allows for immediate exchange of data frames, avoiding the latency associated with the establishment of a BSS.	S2.3, S2.7, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(Updated) ETSI EN 302 665 ITS; Communications Architecture	http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf	Definition of ITS Communications Architecture for Europe including the following views: Scenario description; Functional View and Information View; OSI reference model view including Application View, Security View, Network&Transport View, Interface View, Management view; Engineering view to support Implementation Guidelines for Interoperability; Enterprise/Organizational/Operational view.	S2.3, S2.7, S2.14
ETSI	ETSI EN 303 613 ITS; LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band	http://www.etsi.org/deliver/etsi_en/303600_303699/303613/01.01.01_60/en_303613v010101p.pdf	This document specifies the access layer for the LTE-V2X technology.	S2.3, S2.7, S2.14
ETSI	ETSI GR CIM 011 Context Information Management (CIM); NGSI-LD Testing Framework: Test Purposes Description Language (TPDL)	https://www.etsi.org/deliver/etsi_gr/CIM/001_099/011/01.01.01_60/gr_CIM011v010101p.pdf	The present document is a choice of Test Purposes Description Language (TPDL), with the intention to capture all of the information required by the Test Template and should be parseable using software.	S2.1, S2.9
ETSI	ETSI GR IP6 001 IPv6 Deployment in the Enterprise	https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_IP6001v010101p.pdf	The present document outlines the motivation for the deployment of IPv6 in enterprises, the objectives, the benefits, the risks, the challenges, the technology guidelines, the different choices that arise when designing IPv6-only or dual-stack enterprise network, step-by-step process, the addressing plan, and the milestones.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI GR IP6 008 IPv6-based Internet of Things Deployment of IPv6-based Internet of Things	https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_IP6008v010101p.pdf	The present document outlines the motivation for IPv6 in IoT, the technical challenges to address IoT on constrained devices and networks, the impact on the IPv6 technology and protocols, the technology guidelines, the step by step process, the benefits, the risks, as applicable to IoT domains including: M2M, Energy, Industrial, Mining, Oil and gas, Smart city, Transportation (including EVs), etc. IPv6-based IoT in this context refers to the connectivity network layers needed to support the communication between things. It is understood that a complete IoT system may use of an IoT architecture including but not necessarily an abstraction layer part of an IoT platform. The description of such IoT platform is out of the scope of the present document.	S2.7
ETSI	ETSI GS CIM 016 Context Information Management (CIM); NGSI-LD Testing Framework: Test Template	https://www.etsi.org/deliver/etsi_gs/CIM/001_099/016/01.01.01_60/gs_CIM016v010101p.pdf	The Testing Framework (document format) specifies a testing framework defining a methodology for the development of the test strategies, test systems and resulting test specifications. The present document identifies the implementation under test (scope of the testing), the format for the test specification, the test architecture, the points of control and observation, the naming conventions (e.g. for test case ID and test case grouping ID), etc. It also provides the Implementation Conformance Statement which is basically a checklist for a client-owner so they know what parts of the specification will be tested and if any is optional. The ICS will be published as a separate GS.	S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI	ETSI GS LTN 002 Low Throughput Networks (LTN) - Functional Architecture	https://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN002v010101p.pdf	The present document aims to: describe the characteristics of the architecture of a Low Throughput Network illustrate the applicability of LTN in industrial communication highlight the specificity of LTN deployment	S2.5, S2.14
ETSI	ETSI GS LTN 003 Low Throughput Networks (LTN) - Protocols and Interfaces	https://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN003v010101p.pdf	The document aims to define the protocols and interfaces of LTN systems. It goes along with the document GS LTN 002 on LTN functional architecture.	S2.5
ETSI	ETSI GS NGP 005 Next Generation Protocol Requirements	https://www.etsi.org/deliver/etsi_gs/NGP/001_099/005/01.01.01_60/gs_NGP005v010101p.pdf	The scope of the Standard is to specify the minimum set of key requirements for the Next Generation Protocols (NGP), Industry Specific Group (ISG). The present document addresses requirements in the following areas: Business Case and Techno-Economics Migration General Technical Requirements Addressing Security Mobility Multi-Access Support (including FMC) Context Awareness Performance (including Content Enablement) Network Virtualisation IoT Support Energy Efficiency e-Commerce MEC Mission Critical Services Drones and Autonomous Vehicles and Connected Vehicles Ultra Reliable Low Latency Communications	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI TS 103 264 V3.2.1 SAREF: the Smart Applications REFerence ontology and oneM2M Mapping	https://www.etsi.org/deliver/etsi_ts/103200_103299/103264/03.02.01_60/ts_103264v030201p.pdf	The Smart Applications REFerence ontology (SAREF) is intended to enable interoperability between solutions from different providers and among various activity sectors in the Internet of Things (IoT), thus contributing to the development of the global digital market.	S2.1, S2.18
ETSI	ETSI SR 003 680 SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach	http://www.etsi.org/deliver/etsi_sr/003600_003699/003680/01.01.01_60/sr_003680v010101p.pdf	Providing guidelines for Security, Privacy and Interoperability in IoT System Definition based on the analysis of representative use cases.	S2.6, S2.10
ETSI	ETSI SR 003 809 eHEALTH; The role of ICT to enable Health crisis management and recovery; Responding to the 2019 SARS-CoV-2 Pandemic	https://www.etsi.org/deliver/etsi_sr/003800_003899/003809/01.01.02_60/sr_003809v010102p.pdf	This report contains a detailed review of actions to be taken by ETSI, in partnership with other SDOs and industrial development groups, in driving ICT standards to support societal responses to health crisis. It considers the role played by ICT in response to the SARS-CoV-19 pandemic and identifies where there were successes, where there were failures, and where ICT and particularly standards in ICT, may play a role in future mitigations.	S2.14
ETSI	(NEW) GS MEC 033 V3.1.1	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/033/03.01.01_60/gs_MEC033v030101p.pdf	The present document defines the IoT API to assist the deployment and usage of devices that require additional support in a MEC environment, e.g. due to security constraints, limited power, compute and communication capabilities, such as IoT and MTC devices. The API enables the device provisioning and configuration of the associated components and applications requiring connection to these devices. The present document describes the information flows and the required information. It also specifies the RESTful binding with the data model.	S2.2, S2.5

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI/ oneM2M	(NEW) TR 118 551 V2.0.0	http://www.etsi.org/deliver/etsi_tr/118500_118599/118551/02.00.00_60/tr_118551v020000p.pdf	The guide will list the CRUDN messages for managing some of the main resources defined in TS-0001. It aims at providing the description and associated flow in basic examples. It is foreseesn to use HTTP binding and JSON serialization as example. Other binding and serialization could be considered later, or in a companion document. It also aims to use this list as a common sets of APIs and extend them to include other APIs (such as 3GPP interworking) so developers will have an option to write applications that can run across different platforms and specific implementations.	S2.1
ETSI	(NEW) TR 103 675	http://www.etsi.org/deliver/etsi_tr/103600_103699/103675/01.01.01_60/tr_103675v010101p.pdf	The present document is addressing the development of a Proof of Concept based on three Use Cases analysed and selected in the associated ETSI TR 103 674. ETSI TR 103 674 addresses the issues related to the introduction of AI into IoT systems and, as first priority, into the oneM2M architecture. ETSI TR 103 674 has identified and described several Use Cases of which three are used for the development of the Proof of Concept described in the present document.	S2.14, S2.15
ETSI/ oneM2M	(NEW) TR 118 518 V2.5.1	www.etsi.org/deliver/etsi_tr/118500_118599/118518/02.05.01_60/tr_118518v020501p.pdf	Industrial domain is expectd to be able to improve efficiency and flexibility by utilizing ICT technology: collecting data from devices in multiple factories, analyzing them, and applying the analysis results to decisions. So, it is desirable to utilize oneM2M standardized technology in the industrial domain. To better understand the special requirements to support the operations of the industrial environment, it is desirable to conduct studies on various functionalities that are keen to support this purpose so as to identify necessary technical works to enhance the future oneM2M specifications. This work item is intended to study such functionalities and the results of that study will be presented in a Technical Report.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TS 103 701 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103400_103499/103438/01.01.01_60/tr_103438v010101p.pdf	The goal of this TR is to consider Digital Ecosystem through user's point of view under the following two directions: - identification of user's needs such as QoS, security, usability, flexibility, Service Level Objectives (SLO) - study impact of technical implementations related to user's requirements/concerns	S2.14
ETSI/ oneM2M	(NEW) TR 103 716 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103700_103799/103716/01.01.01_60/tr_103716v010101p.pdf	This work will develop a simulation with the goal to provide a proof of concept and a performance evaluation to support the selection and development of the discovery and query solution to be contributed to oneM2M. An extract of the simulation results will be used to support the discussion and the proposal with oneM2M.	S2.23
ETSI	(NEW) TR 103 621 V1.2.1	http://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf	The present document serves as guidance to help manufacturers and other stakeholders in meeting the cyber security provisions defined for Consumer IoT devices in ETSI EN 303 645 and ETSI TS 103 645.	S2.6, S2.10
ETSI/ oneM2M	(NEW) TR 118 567 V4.0.0	http://www.etsi.org/deliver/etsi_tr/118500_118599/118567/04.00.00_60/tr_118567v040000p.pdf	The present document studies the completion of SDT (Smart Device Template) using <flexContainer> resource specializations and the possible migration of the existing device management model using Management Object (<mgmtObj>). The present document is initiated in the context of the Management Object Migration.	S2.1, S2.18, S2.22
ETSI/ oneM2M	(NEW) TS 118 122 V4.5.1	https://www.etsi.org/deliver/etsi_ts/118100_118199/118122/04.05.01_60/ts_118122v040501p.pdf	The present document specifies the architectural options, resources and procedures needed to pre-provision and maintain devices in the Field Domain (e.g. ADN, ASN/MN) in order to establish M2M Service Layer operation between the device's AE and/or CSE and a Registrar and/Hosting CSE. The resources and procedures includes information about the Registrar CSE and/or Hosting CSE needed by the AE or CSE to begin M2M Service Layer operation.	S2.5

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TS 103 846 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103800_103899/103846/01.01.01_60/ts_103846v010101p.pdf	With reference to the findings and analysis in DTR/ SmartM2M-103844 (D1) and the standardized functionalities and requirements in DTS/ SmartM2M-103845 (D2) -Definition of Digital Twins communication functionalities and properties, -Guidelines for the adoption of Digital Twins -Standardization of Digital Twins communication.	S2.15
ETSI	(NEW) GS NIN 006 V1.1.1	http://www.etsi.org/deliver/etsi_gs/NIN/001_099/006/01.01.01_60/gs_NIN006v010101p.pdf	The present work item intends to provide updates to the GS NGP 001 V1.3.1.	
ETSI	(NEW) EN 303 760 V1.1.0	http://www.etsi.org/deliver/etsi_en/303700_303799/303760/01.01.00_20/en_303760v010100a.pdf	The relevance of the semantic work to assure semantic interoperability has driven the development of ontology specifications according to the SAREF methodology. IoT is currently experiencing a period of evolution and adoption in the different sectors, as a consequence the SAREF specifications are deemed to evolve quickly with the evolution of IoT solutions. Therefore the SAREF Technical Specification suite is expected to evolve dynamically to timely accommodate new needs and contributions coming from all the interested stakeholders (from the same or from different domains). This requires the adoption of an effective SAREF methodology with the ability to point to the latest technical specifications. This EN will specify the guidelines for the application of SAREF methodology in order to: - apply SAREF - extend SAREF - evolve SAREF The document will make extensive use of references to the SAREF Technical Specification suite and to the SAREF Portal.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) GS CIM 029 V1.1.1	http://www.etsi.org/deliver/etsi_gs/CIM/001_099/029/01.01.01_60/gs_CIM029v010101p.pdf	The relevance of the semantic work to assure semantic interoperability has driven the development of ontology specifications according to the SAREF methodology. IoT is currently experiencing a period of evolution and adoption in the different sectors, as a consequence the SAREF specifications are deemed to evolve quickly with the evolution of IoT solutions. Therefore the SAREF Technical Specification suite is expected to evolve dynamically to timely accommodate new needs and contributions coming from all the interested stakeholders (from the same or from different domains). This requires the adoption of an effective SAREF methodology with the ability to point to the latest technical specifications. This EN will specify the guidelines for the application of SAREF methodology in order to: - apply SAREF - extend SAREF - evolve SAREF The document will make extensive use of references to the SAREF Technical Specification suite and to the SAREF Portal.	S2.1, S2.18
ETSI	(NEW) GS CIM 027 V1.1.1	http://www.etsi.org/deliver/etsi_gs/CIM/001_099/027/01.01.01_60/gs_CIM-027v010101p.pdf	includes test purpose description language extracted from ETSI GS CIM 016	S2.1, S2.18
ETSI	(NEW) TS 103 828 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103800_103899/103828/01.01.01_60/ts_103828v010101p.pdf	This deliverable will fill the priority gaps identified related to SAREF in DTR/SmartM2M-103827 and will include guidelines about how to use SAREF in the context of Urban Digital Twins and with Digital Twins	
ETSI	(NEW) TS 103 845 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103800_103899/103845/01.01.01_60/ts_103845v010101p.pdf	This deliverable will fill the priority gaps identified related to SAREF in DTR/SmartM2M-103827 and will include guidelines about how to use SAREF in the context of Urban Digital Twins and with Digital Twins	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TS 103 927 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103900_103999/103927/01.01.01_60/ts_103927v010101p.pdf	The present document defines security provisions for Smart Voice-Controlled Devices extending from the provisions for consumer IoT devices defined in ETSI EN 303 645 [1]. In terms of security concerns, Smart Voice-Controlled Device has a different focus than other generic IoT devices (e.g., distributed sensors, smart appliances, etc.). For example, Smart Voice-Controlled Devices mainly interact with users through voice assistants that can understand users' voice commands and assist users to control other devices in the IoT network. This feature actually expands the attack surface of Smart Voice-Controlled Devices. In addition, Smart Voice-Controlled Devices usually collect the user's voice and train a model uniquely suitable for the current user to provide personalized service. Therefore, Smart Voice-Controlled Devices-related privacy protection issues are particularly prominent. This vertical will focus on addressing the unique security issues of Smart Voice-Controlled Devices. NOTE 1: Smart Voice-Controlled Devices in the context of this standard refers specifically to Smart Voice-Controlled Devices used in consumer environments, not those used in industrial environments. Smart Voice-Controlled Devices for industrial purpose is not in the scope of this document.	S2.3, S2.6, S2.10, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TR 103 936 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103900_103999/103936/01.01.01_60/tr_103936v010101p.pdf	The use of IoT devices by users to abuse and coerce vulnerable users is a matter that ETSI cannot ignore. The number, and format, of devices, their penetration, and their core functionality, all make them attractive to both the vulnerable user and their abuser. The intent of this work item is to identify design practices that guide the development of measures that allow some degree of mitigation in both the devices themselves and in the services that the devices support. Thread #1: Coercive control resistant design	S2.14, S2.17
			The role of coercive control resistant design is addressed in device and service design. It is expected that this will examine and guide the designer on the roles of user identification, location and access control, in order to limit, where possible, the ability of the abusive or coercive party to use the device whilst not limiting the access to the device functionality by the intended user. Thread #2: Trauma informed design Trauma informed design requires acceptance that devices are actively targeted as threat-agents of coercion. This element of the work is expected to address feature extensions in IoT devices and services to allow the at risk user to seek help without interference from the coercive party. The work should also identify where future standards are required to further strengthen the protection of the vulnerable user.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TS 103 815 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103800_103899/103815/01.01.01_60/ts_103815v010101p.pdf	This document specifies requirements and guidelines for cyber security, credential related security, electromechanical security and mechanical security (e.g. refering to existing CEN standards) of consumer residential connected smart door locking devices. This document builds on EN 303 645 for cyber security requirements, adding additional provisions specific to smart door locking devices. This document builds on other standards for credential related security, electromechanical security and mechanical security. The document includes both product security performance requirements and test methodology. The intent is to provide an appropriate level of assurance.	S2.6, S2.9
ETSI	(NEW) TR 103 844 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103800_103899/103844/01.01.01_60/tr_103844v010101p.pdf	With reference to Digital Twins: -Analysis the major characteristics and architectures -Identification major functionalities, -selection of the candidate communication functionalities for standardization -Collection, identification and Definition of uses cases for IoT and in particular industrial IoT -Identification of potential requirements	S2.14, S2.15
ETSI	(NEW) TS 103 410-12 V1.1.1	http://www.etsi.org/deliver/etsi_ts/103400_103499/10341012/01.01.01_60/ts_10341012v010101p.pdf	Specify an extension to SAREF to include the semantic model for the Smart Grid domain. This extension will be based on the set of use cases and data models identified in the corresponding requirements TR.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ETSI	(NEW) TR 103 827 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103800_103899/103827/01.01.01_60/tr_103827v010101p.pdf	The present document defines security provisions for Smart Voice-Controlled Devices extending from the provisions for consumer IoT devices defined in ETSI EN 303 645 [1]. In terms of security concerns, Smart Voice-Controlled Device has a different focus than other generic IoT devices (e.g., distributed sensors, smart appliances, etc.). For example, Smart Voice-Controlled Devices mainly interact with users through voice assistants that can understand users' voice commands and assist users to control other devices in the IoT network. This feature actually expands the attack surface of Smart Voice-Controlled Devices. In addition, Smart Voice-Controlled Devices usually collect the user's voice and train a model uniquely suitable for the current user to provide personalized service. Therefore, Smart Voice-Controlled Devices-related privacy protection issues are particularly prominent. This vertical will focus on addressing the unique security issues of Smart Voice-Controlled Devices. NOTE 1: Smart Voice-Controlled Devices in the context of this standard refers specifically to Smart Voice-Controlled Devices used in consumer environments, not those used in industrial environments. Smart Voice-Controlled Devices for industrial purpose is not in the scope of this document.	S2.3, S2.6, S2.10, S2.14
ETSI	(NEW) TR 103 781 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103700_103799/103781/01.01.01_60/tr_103781v010101p.pdf	to report on the modularization and factorization potential of the TC SmartM2M suite using reference ontology patterns. The present document lists identified modelling discrepancies in SAREF extensions, along with proposals to homogenise the modelling. As a result, the present document describes a set of core ontology patterns and how they can be used as a basis for future normative work in TC SmartM2M	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	(NEW) TR 103 839 V1.1.1	http://www.etsi.org/deliver/etsi_tr/103800_103899/103839/01.01.01_60/tr_103839v010101p.pdf	Identification of relevant deployment scenarios. The description of these scenarios include detailed information of the IoT solution topology, characteristics of both IoT devices and applications in terms of number of entities, traffic profiles, targeted performances, etc. The deliverable will also include the procedures to define additional evaluation scenarios.	S2.7, S2.14
ETSI	(NEW) ETSI TS 104 134 V1.1.1 (2025-09)	https://www.etsi.org/deliver/etsi_ts/104100_104199/104134/01.01.01_60/ts_104134v010101p.pdf	Simplified Method for including Uncertainty and Sensitivity Aspects in Calculations of the Avoided Environmental Impact of Information and Communication Technology Solutions: The present document concerns a methodology for including uncertainty and sensitivity aspects for avoided environmental impact calculations. The objective of the present document is to provide a standardized method to assess in a simplified manner the uncertainty of calculations for avoided environmental impact resulting from the introduction of Information and Communication Technology (ICT) Solutions. Moreover, the sensitivity of individual elements and the contribution to the total uncertainty is outlined. A method is defined based on existing standards, e.g. Recommendation ITU-T L.1480 [i.8] and recognized methods which allow for communication of the results to the public and consumers. The uncertainty and sensitivity calculation procedures are standardized for the method to be developed to make visible the relation between the degree of simplification and the ability to draw conclusions.	S2.24

Table 5: AIOTI/EUOS indentified IoT challenges covered/addressed by 3GPP

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
3GPP	3GPP TR 36.763 V17.0.0	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3747	The objectives for this document are, based on the outcomes of the Release-17 NR NTN WI [7] and Release-16 TR 38.821 [8], to study a set of necessary features/adaptations enabling the operation of the IoT NTN for 3GPP Release 17 with a priority on satellite access. The first objective of this Study is to identify scenarios applicable to NB-IoT/eMTC [RAN1, RAN2]. The second objective is, for the above identified scenarios, to study and recommend necessary changes to support NB-IoT and eMTC over satellite, reusing as much as possible the conclusions of the studies performed for NR NTN in TR38.821.	S2.7
3GPP	3GPP TR 36.802 V13.0.0	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3033	This document summarizes the studies of radio requirements for BS and UE radio transmission and reception as part of the work item on Narrowband Internet of Things (NB-IoT). The objective is to specify a radio access for cellular internet of things, based to a great extent on a non-backward-compatible variant of E-UTRA, that addresses improved indoor coverage, support for massive number of low throughput devices, low delay sensitivity, ultra low device cost, low device power consumption and (optimised) network architecture.	S2.7
3GPP	3GPP TR 38.825 V16.0.0 (2019-03)	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3492	This section focuses on PDCP duplication and higher layer multi-connectivity aspects such as assessment of gains of duplication with more than two copies, potential enhancements to achieve resource efficient PDCP duplication and captures RAN aspects of higher layer multi-connectivity solutions.	S2.7
3GPP	(NEW) 3GPP TR 22.840 V19.0.0 Study on Ambient power-enabled Internet of Things (Release 19)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.840/22840-j00.zip	The present document describes use cases, traffic scenarios, device constraints of Ambient Internet of Things and identify new potential service requirements as well as new KPIs. An Ambient Internet of Things (Ambient IoT) device is an IoT device, being either battery-less or with limited energy storage capability (i.e., using a capacitor) and the energy is provided through the harvesting of radio waves, light, motion, heat, or any other suitable power source.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TR 22.865 V19.2.0 Study on satellite access Phase 3; (Release 19)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.865/22865-j20.zip	The present document describes use cases and aspects related to enhancements of the 5G system over satellite, including: Store and Forward (S&F) Satellite operation for delay-tolerant communication service UE-Satellite-UE communication GNSS independent operation Positioning enhancements for satellite access	
3GPP	(NEW) 3GPP TR 22.867 V18.2.0 Study on 5G Smart Energy and Infrastructure (Release 18)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.867/22867-i20.zip	The present document is to address study use cases, potential new service requirements for 5G system to support Smart Grid including the following topics: Smart Grid services, e.g. IEC standards, and their communications requirements including capacity, latency, availability, end-to-end QoS, resilience/ redundancy and security. Deployment requirements when considering constraints e.g. service lifetime, coverage (ubiquity), electromagnetic applicability (e.g. penetration, ability to operate in high EM environments,) etc. Additional requirements due to operational manageability – e.g. the ability to configure and monitor the real (achieved & up to date) availability of virtual network topologies New Smart Grid use cases and potential service function requirements: e.g. on-demand power supply, distributed power supply system, distribution automation, higher accuracy power load measurement and control, meter automation, etc. Communication KPI and service requirements for enabling microgrids, DER and specifically distributed generation (DG) that require 5G wireless communication (e.g. wind and solar energy generation, including scenarios at or near residential / consumer premises, etc.)	S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TR 23.776 V17.0.0 Study on architecture enhancements for 3GPP support of advanced Vehicle-to-Everything (V2X) services; Phase 2; (Release 17)	https://www.3gpp.org/ftp/Specs/archive/23_series/23.776/23776-h00.zip	The objective of this Technical Report is to investigate 5G System enhancements based on what has been specified in Rel-16, for enhanced support of V2X operation for pedestrian UEs (i.e. UEs for Vulnerable Road Users), e.g. V2X communication with power efficiency, according to vehicular services requirements defined in TS 22.185 and TS 22.186.	S2.7, S2.22
3GPP	(NEW) 3GPP TR 28.841 V18.0.1 Study on management aspects of Internet of Things (IoT) Non-Terrestrial Networks (NTN) enhancements (Release 18)	https://www.3gpp.org/ftp/Specs/archive/28_series/28.841/28841-i01.zip	The present document studies on management aspects of IoT NTN enhancements. It investigates specific IoT NTN related parameters which should be considered by O&M, investigates NRM enhancement, performance measurement and related new KPIs of IoT NTN. It studies the key issues associated with service and network management of IoT NTN enhancements (whether as NG-RAN or E-UTRAN) and potential solutions, and provides recommendations for the further normative work.	S2.22
3GPP	(NEW) 3GPP TS 23.542 V18.4.0 Application layer support for Personal IoT Network;	https://www.3gpp.org/DynaReport/23542.htm	The present document specifies the application enabler layer architecture, procedures and information flows necessary for enabling PIN applications over 3GPP networks. The specification includes the capabilities (e.g. PIN management, discovery of elements, capabilities and services related to PIN) at the application enablement layer that fulfil the deployment and operational requirements of PIN applications over 3GPP networks. The PIN enabler capabilities applies to 5GS.	S2.7, S2.22
3GPP	(NEW) 3GPP TS 23.433 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL);	https://www.3gpp.org/ftp/Specs/archive/23_series/23.433/23433-j30.zip	With increasing demand of applications consumption over mobile networks, more and more application content is transmitted over the mobile networks. Vertical applications have diverse requirements for the application content distribution and delivery. To ease the various data delivery demands for vertical applications, a data delivery enabler is specified in this document.	S2.1, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TS 23.434 V19.3.0 Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows; (release 19)	https://www.3gpp.org/ftp/Specs/archive/23_series/23.434/23434-j30.zip	This document specifies a functional architecture for service enabler architecture layer (SEAL) over 3GPP networks to support vertical applications (e.g. V2X applications). This functional architecture will include common application plane and signalling plane entities. A set of common services (e.g. group management, configuration management, location management) specified in this document can be shared across vertical applications. The SEAL functional architecture takes into consideration the common capabilities to support mission critical and other vertical applications.	S2.7, S2.22
3GPP	(NEW) 3GPP TR 26.928 V2.0.0 (2020-03)	https://www.3gpp.org/ftp/Specs/archive/26_series/26.928/26928-200.zip	Rel-16 is the first 3GPP release that explicitly addresses XR, in the Technical Report (TR) 26.928 'Extended Reality (XR) in 5G', which had the charter of defining a roadmap for future work in 3GPP WGs, mentioning several areas suited for standardization. It also listed a set of potential XR use cases, and provided a survey of 3D, XR visual and audio formats.	S2.25.9, S2.25.10
3GPP	(NEW) 3GPP TR 22.842 V17.2.0 (2019-12)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.842/22842-h20.zip	The objective of this TR is to study the use cases and to derive potential service requirements to provide users with interactive services, including: New use cases and new requirements for Interactive Services. Part of this TR are XR and Cloud gaming use cases. Gap Analyses between requirements and existing eMBB service requirements / existing ProSe requirements After the use cases have been identified, service requirements and KPIs will be studied including QoS, operator control, charging, etc.	S2.25.9, 2.25.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TR 38.838 V17.0.0 (2021-12)	https://www.3gpp.org/ftp/specs/archive/38_series/38.838/38838-h00.zip	The TR 38.838 "Study on XR enhancements for NR" introduced some new features to improve the capacity of the cellular system to cover more users using XR services and to considerably reduce the energy consumption of such services. Additional enhancements can be listed as follows: enhancements in data speeds, reduced latency, and ultra-reliability. These encompass Multiple In Multiple Out (MIMO) for 5G New Radio (NR), Improved Uplink Coverage, Enhanced Sidelink Communications, Positioning Enhancement, UE Power Saving, Ultra-Reliable Low Latency Communications (URLLC)/ IIoT Enhancements, Integrated Access and Backhaul (IAB), and Non-Terrestrial Networks (NTN). Support to Metaverse and Reduced Capability (RedCap) devices were also introduced for applications like those running in wearables (e.g., smartwatches, wearable medical devices, augmented reality (AR)/VR goggles, industrial wireless sensors, and video surveillance). ML coverage was expanded to provide descriptions of principles for RAN intelligence enabled by ML.	S2.24, S2.25.5, S2.25.8, S2.25.9, S2.25.13, S2.25.16
3GPP	(NEW) 3GPP TR 22.847 V18.2.0 (2022-03)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.847/22847-i20.zip	This document provides stage 1 use cases and potential 5G requirements on supporting tactile and multi-modal communication services. In the context of the present document, the aspects addressed include: Study new scenarios and identify use cases and potential requirements for immersive real time experience involving tactile and multi-modal interactions, including: Network assistance for coordinated transmission of multiple modal representations associated with the same session, aspects of charging, security and privacy, and KPIs (including network reliability and availability). Gap analysis with existing requirements and functionalities on supporting tactile and multi-modal communication services.	S2.6, S2.25.8, S2.25.9, S2.25.11, S2.25.13, S2.25.16

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TS 22.261 V18.18.0 (2025-06)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-ii0.zip	This document describes the service and operational requirements for a 5G system, including a UE, NG-RAN, and 5G Core network. In particular, in the context of metaverse, it introduced support for new services like tactile internet and for applications aiming at delivering immersive experiences to users.	S2.25.8. S2.25.9, S2.25.10, S2.25.13, S2.25.16
3GPP	(NEW) 3GPP TR 22.856 V19.2.0 (2023-12)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.856/22856-j20.zip	This document investigates specific use cases and service requirements for 5GS support of enhanced XR-based services, (as XR-based services are an essential part of "Metaverse" services considered in this study,) as well as potentially other functionality, to offer shared and interactive user experience of local content and services, accessed either by users in the proximity or remotely. In particular, this TR addresses directly the Metaverse services, i.e.: "Study on localized mobile Metaverse services".	S2.25.4, S2.25.5, S2.25.8. S2.25.9, S2.25.10, S2.25.12
3GPP	(NEW) 3GPP TS 22.261 V19.11.0 (2025-06)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-jb0.zip	This document describes the service and operational requirements for a 5G system, including a UE, NG-RAN, and 5G Core network. In particular focuses, on the need to support different kinds of UEs (e.g. for the Internet of Things (IoT)), services, and technologies is driving the technology revolution to a high-performance and highly efficient 3GPP system. The drivers include IoT, Virtual Reality (VR), industrial control, ubiquitous on-demand coverage, as well as the opportunity to meet customized market needs. These drivers require enhancements to the devices, services, Includeing Metaverse services, and technologies well established by 3GPP.	S2.7, S2.25.1, S2.25.2, S2.25.4, S2.25.5, S2.25.8. S2.25.9, S2.25.10, S2.25.11, S2.25.13, S2.25.16
3GPP	(NEW) 3GPP TS 22.156 V19.1.0 (2024-03)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.156/22156-j10.zip	The present document provides Stage 1 normative service and performance requirements for diverse service enablers to enhance XR-based services. In particular, this TR addresses directly the Metaverse services, i.e.: " Mobile Metaverse services ".	S2.25.1, S2.25.2, S2.25.3, S2.25.4, S2.25.5, S2.25.8. S2.25.9, S2.25.10, S2.25.11, S2.25.12, S2.25.13, S2.25.15, S2.25.16

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
3GPP	(NEW) 3GPP TS 22.261 V20.3.0 (2025-06)	https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-k30.zip	This document describes the service and operational requirements for a 5G system, including a UE, NG-RAN, and 5G Core network. In particular, focuses on the need to support different kinds of UEs (e.g. for the Internet of Things (IoT)), services, and technologies is driving the technology revolution to a high-performance and highly efficient 3GPP system. The drivers include IoT, Virtual Reality (VR), industrial control, ubiquitous on-demand coverage, as well as the opportunity to meet customized market needs. These drivers require enhancements to the devices, services, and technologies well established by 3GPP. Note that Release 20 is the release that will first work on 6G specifications, a set of technical reports (TRs) are planned to be provided, mainly based on defining 6G use cases and requirements of the to-be defined 6G architecture. AI/ML are expected to be natively integrated in all 6G specifications, marking 6G as the first generation of data-driven mobile networks.	S2.7, S2.15, S2.25.1, S2.25.2, S2.25.4, S2.25.5, S2.25.8. S2.25.9, S2.25.10, S2.25.11, S2.25.13, S2.25.16

Table 6: AIOTI/EUOS indentified IoT challenges covered/addressed by ISO/IEC JTC1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ISO/ IEC JTC1	ISO/IEC 30177 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104960	This document specifies the detailed description on interworking components in underwater network management system (U-NMS). It provides the intra-working of U-NMS components, interworking between U-NMS's terrestrial domain components and U-NMS's surface domain components, interworking between U-NMS's surface domain components and U-NMS's underwater domain components, and interworking in U-NMS's underwater domain components.	S2.7
ISO/ IEC JTC1	ISO/IEC 30180 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,106630	This document specifies the functional requirements about the following items to figure out the status of self-quarantine through IoT data interfaces working over a set of hand-held devices, wristbands, and a management system: - Functional requirements for self-quarantine app and optional wristband at a self-quarantine place; - Functional requirements for self-quarantine management app and system at the management side; and - Functional requirements for the protection of the self-quarantine status and the privacy information.	S2.7
ISO/ IEC JTC1	ISO/IEC 30178 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104965	This document defines common formats, value, and coding for Internet of things (IoT).	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30181 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::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.	S2.17, S2.18
ISO/ IEC JTC1	ISO/IEC 30183 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,108553	This document provides addressing interoperability guidelines between heterogeneous underwater acoustic sensor networks (UWASNs) based on underwater delay and disruption tolerant network (UDTN): - Architecture for heterogeneous UWASNs interworking; - U-DTN functions on heterogeneous UWASNs interworking; - Addressing interoperability guidelines between heterogeneous UWASNs.	S2.1 , S2.18
ISO/ IEC JTC1	ISO/IEC 30179 ED1	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,105254	This document specifies the Internet of Things system for ecological environment monitoring in the following: — System infrastructure and system entities of the IoT system for ecological environment monitoring for natural entities such as air, water, soil, living creatures; and — The general requirements of the IoT system for ecological environment monitoring.	S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 19637:2016	https://webstore.iec.ch/publication/59623	ISO/IEC 19637:2016 specifies: a) testing framework for conformance test for heterogeneous sensor networks; b) generic services between test manager (TMR) and test agent (TA) in the testing framework; and c) guidance for creating testing platform and enabling the test of different sensor network protocols.	S2.9
ISO/ IEC JTC1	ISO/IEC TR 22417:2017	https://webstore.iec.ch/publication/60605	This technical report identifies IoT scenarios and use cases based on real-world applications and requirements. The use cases provide a practical context for considerations on interoperability and standards based on user experience. They also clarify where existing standards can be applied and highlight where standardization work is needed.	S2.7
ISO/ IEC JTC1	ISO/IEC 30140-2:2017	https://webstore.iec.ch/publication/60610	This part of ISO/IEC 30140 provides an underwater acoustic sensor network (UWASN) conceptual model by identifying and defining three domains (application domain, network domain and UWASN domain). It also provides multiple reference architecture views consistent with the requirements defined in ISO/IEC 30140-1 (systems reference architecture, communication reference architecture and information reference architecture). For each view, related physical and functional entities are described.	S2.7
ISO/ IEC JTC1	(Updated) ISO/IEC 30140-3:2018	https://webstore.iec.ch/publication/60611	The 30140 series provides general requirements, reference architecture and high-level interface guidelines supporting interoperability among underwater acoustic sensor networks (UWASNs). Part 3 provides descriptions for the entities and interfaces of the UWASN reference architecture.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30140-4:2018	https://webstore.iec.ch/publication/60612	The ISO/IEC 30140 series provides general requirements, reference architecture and high-level interface guidelines supporting interoperability among underwater acoustic sensor networks (UWASNs). Part 4 provides information on interoperability requirements among entities within a UWASN and among various UWASNs.	S2.7
ISO/ IEC JTC1	ISO/IEC TR 30176:2021	https://webstore.iec.ch/publication/66420	This report identifies and collects use cases for the integration of the DLT/blockchain within IoT systems, applications, and/or services. The use cases presented in this document use the IoT use case template.	S2.10
ISO/ IEC JTC1	ISO/IEC 30142:2020	https://webstore.iec.ch/publication/62443	ISO/IEC 30142:2020 provides the overview and requirements of a network management system in underwater acoustic sensor network (UWASN) environment. It specifies the following: a) functions which support underwater network management system; b) entities required for underwater network management system; c) data about the communication between elements in underwater network management system; d) guidelines to model the underwater network management system; e) general and functional requirements of underwater network management system	S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(Updated) ISO/IEC TR 30167:2021	https://www.iso.org/standard/84977.html	ISO/IEC TR 30167:2021 describes the enabling and driving technologies of underwater communication such as acoustic communication, optical communication, Very Low Frequency (VLF)/Extremely, Low Frequency (ELF) communication, and Magnetic Fusion Communication (MFC). This document also highlights: a) technical overview of different communication technologies; b) characteristics of different communication technologies; c) trends of different communication technologies; d) applications of each communication technology; e) benefits and challenges of each communication technology.	S2.7
ISO/ IEC JTC1	ISO/IEC PWI JTC1-SC41-7	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::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.	S2.23, S2.24
ISO/ IEC JTC1	(Updated) ISO/IEC 27400	https://standardsdevelopment.bsigroup.com/projects/9021-06476#/section	This document provides the following: a) a conceptual model of cyber-physical systems (CPS) and its general features; b) security concerns, which serve as the basis for the discussion of security risks and security controls for the CPS based on the conceptual model, and several security frameworks to overcome those security concerns.	
ISO/ IEC JTC1	ISO/IEC 27400:2022	https://www.iso.org/standard/44373.html	This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.	S2.6, S2.8, S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(Updated) ISO/IEC 27404	https://www.iso27001security.com/html/27404.html	This document defines a universal cybersecurity labelling framework for the development and implementation of cybersecurity labelling programmes for consumer IoT products and includes guidance on the following topics: Risks and threats associated with consumer IoT products; Stakeholders, roles and responsibilities; Relevant standards and guidance documents; Conformity assessment options; Labelling issuance and maintenance requirements; and Mutual recognition considerations.	S2.6, S2.8, S2.9
ISO/ IEC JTC1	(Updated) ISO/IEC CD 27402.2	https://www.iso.org/standard/80136.html	This document will provide the minimum-security requirements for IoT Devices	S2.6, S2.8, S2.9, S2.21
ISO/ IEC JTC1	(Updated) ISO/IEC CD 27403.2	https://www.iso.org/standard/78702.html	This proposal provides guidelines to analyse security and privacy risks and identifies controls that need to be implemented in IoT domotis systems	S2.6, S2.8, S2.9
ISO/ IEC JTC1	(Updated) ISO/IEC DIS 24392	https://www.iso.org/standard/78703.html	This document presents specific characteristics of IIPs, including related security threats, context-specific security control objectives and security controls. This document covers specific security concerns in the industrial context and thus complements generic security standards and reference models. In particular, it includes secure data collection and transmission among industrial devices, data security of industrial cloud platform, and secure collaborations with various industry stakeholders. The audiences for this document are organizations who develop, operate, or use any components of IIPs, including third parties who provide services to the above stakeholders.	S2.6, S2.8, S2.9, S2.20

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(Updated) ISO/IEC DIS 27071	https://www.iso.org/standard/56572.html	This document provides a framework and recommendations for establishing trusted connections between devices and services based on hardware security modules, including recommendations for components such as: hardware security module, roots of trust, identity, authentication and key establishment, remote attestation, data integrity and authenticity. This document is applicable to establishing trusted connections between devices and services based on hardware security modules. This document does not address privacy concerns.	S2.6, S2.8, S2.9
ISO/ IEC JTC1	(Updated) ISO/IEC TS 30168	https://www.iec.ch/ords/f?p=103:38:706375228480080::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,20,104067	This document specifies a generic application programming interface (API) for the integration of secure elements within Industrial IoT (IIoT) devices. It considers needs from industrial usage scenarios and applications. This document also provides guidance for implementation, testing, and conformity validation.	S2.8, S2.9, S2.21
ISO/ IEC JTC1	ISO/IEC TR 30174:2021	https://webstore.iec.ch/publication/66419	ISO/IEC TR 30174:2021(E) describes: a) key features of the socialized IoT systems, e.g. sensing the external physical world, resolving the uncertainties of targets, satisfying users' demand and providing quality service, etc.; b) socialized attributes, i.e. socialized network, socialized collaboration, and socialized services, which are derived from the key features; and c) guidelines on how to use or apply the socialized attributes in the design and development of IoT systems.	S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC PWI JTC1-SC41-8	https://www.iec.ch/ords/f?p=103:38:204774363295796::::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.	S2.1, S2.12
ISO/ IEC JTC1	(Updated) ISO/IEC PWI JTC1-SC41-6	https://www.iec.ch/dyn/www/f?p=103:38:204774363295796::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104897	The scope of this document is to: a) define a conceptual model for the building of use cases; b) specify a use case template ontology, i.e. vocabulary as well as conventions for describing and representing use case contents; c) provide guidance on building use case templates and on extending a use case ontology to cover the targeted standard; d) provide examples of use case templates and use cases; and e) specify an implementation scheme that will allow use cases to be stored and shared in a repository.	S2.24
ISO/ IEC JTC1	ISO/IEC 21823-4:2022	https://webstore.iec.ch/publication/65649	ISO/IEC 21823-4:2022 specifies the IoT interoperability from a syntactic point of view. In ISO/ IEC 21823-1: Framework [2], five facets are described for IoT interoperability, i.e. transport, semantic, syntactic, behavioural and policy. In this document, the following specifications for IoT interoperability from syntactic viewpoint are included: a) a principle of how to achieve syntactic interoperability among IoT systems which include IoT devices; b) requirements on information related to IoT devices for syntactic interoperability; and c) a framework for processes on developing information exchange rules related to IoT devices from the syntactic viewpoint.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 29182-1:2013	https://webstore.iec.ch/publication/11411	ISO/IEC 29182-1:2013 provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks.	S2.7
ISO/ IEC JTC1	ISO/IEC 29182-2:2013	https://webstore.iec.ch/publication/11412	ISO/IEC 29182-2:2013 is intended to facilitate the development of International Standards in sensor networks. It presents terms and definitions for selected concepts relevant to the field of sensor networks. It establishes a general description of concepts in this field and identifies the relationships among those concepts. It may also be used as guidance for development of other parts of ISO/IEC 29182 and any other sensor network related standard.	S2.7
ISO/ IEC JTC1	ISO/IEC 29182-3:2014	https://webstore.iec.ch/publication/11413	ISO/IEC 29182-3:2014 provides Sensor Network Reference Architecture (SNRA) views. The architecture views include business, operational, systems, and technical perspectives, and these views are presented in functional, logical, and/or physical views where applicable. ISO/IEC 29182-3:2014 focuses on high-level architecture views which can be further developed by system developers and implementers for specific applications and services.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 29182-4:2013	https://webstore.iec.ch/publication/11414	The purpose of the ISO/IEC 29182 series is to a) - provide guidance to facilitate the design and development of sensor networks, b) improve interoperability of sensor networks, and c) make sensor network components plug-and-play, so that it becomes fairly easy to add/remove sensor nodes to/ from an existing sensor network. ISO/IEC 29182-4 presents models for the entities that enable sensor network applications and services according to the Sensor Network Reference Architecture (SNRA).	S2.7
ISO/ IEC JTC1	ISO/IEC 29182-5:2013	https://webstore.iec.ch/publication/11415	ISO/IEC 29182-5:2013 provides the definitions and requirements of sensor network (SN) interfaces of the entities in the Sensor Network Reference Architecture and covers the following aspects: - interfaces between functional layers to provide service access for the modules in the upper layer to exchange messages with modules in the lower layer; - interfaces between entities introduced in the Sensor Network Reference Architecture enabling sensor network services and applications.	S2.7
ISO/ IEC JTC1	ISO/IEC 29182-5:2013	https://webstore.iec.ch/publication/11416	ISO/IEC 29182-6:2014, describes and provides - a compilation of sensor network applications for which International Standardized Profiles (ISPs) are needed, - guidelines for the structured description of sensor network applications, and - examples for structured sensor network applications. It does not cover ISPs for which drafting rules are described in ISO/IEC TR 10000. Due to the generic character of ISO/IEC 29182, fully developed ISPs will not be included in this International Standard.	S2.7

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 29182-7:2015	https://webstore.iec.ch/publication/21827	ISO/IEC 29182-7:2015 provides a general overview and guidelines for achieving interoperability between sensor network services and related entities in a heterogeneous sensor network.	S2.7
ISO/ IEC JTC1	ISO/IEC 30101:2014	https://webstore.iec.ch/publication/11540	ISO/IEC 30101:2014 is for sensor networks in order to support smart grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications, and associated environmental challenges. This International Standard characterizes the requirements for sensor networks to support the aforementioned applications and challenges. Data from sensors in smart grid systems is collected, transmitted, published, and acted upon to ensure efficient coordination of the various systems and subsystems. The intelligence derived through the sensor networks supports synchronization, monitoring and responding, command and control, data/information processing, security, information routing, and human-grid display/graphical interfaces. This International standard specifies: - interfaces between the sensor networks and other networks for smart grid system applications, - sensor network architecture to support smart grid systems, - interface between sensor networks with smart grid systems, and - sensor network based emerging applications and services to support smart grid systems.	S2.1, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30128:201	https://webstore.iec.ch/publication/11545	ISO/IEC 30128:2014 specifies the interfaces between the application layers of service providers and sensor network gateways, which is Protocol A in interface 3, defined in ISO/IEC 29182-5. This International Standard covers: - description of generic sensor network applications' operational requirements, - description of sensor network capabilities, and - mandatory and optional interfaces between the application layers of service providers and sensor network gateways.	S.2.7, S2.22
ISO/ IEC JTC1	ISO/IEC TR 22560:2017	https://webstore.iec.ch/publication/60608	This Technical Report describes the concepts, issues, objectives, and requirements for the design of an active air-flow control (AFC) system for commercial aircraft based on a dense deployment of wired and wireless sensor and actuator networks. It focuses on the architecture design, module definition, statement of objectives, scalability analysis, system-level simulation, as well as networking and implementation issues using standardized interfaces and service-oriented middleware architectures.	S2.7
ISO/ IEC JTC1	ISO/IEC 21823-1:2019	https://webstore.iec.ch/publication/60604	ISO/IEC 21823-1:2019(E) provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This document enables IoT systems to be built in such a way that the entities of the IoT system are able to exchange information and mutually use the information in an efficient way. This document enables peer-to-peer interoperability between separate IoT systems. This document provides a common understanding of interoperability as it applies to IoT systems and the various entities within them.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(Updated) ISO/IEC 20924:2021	https://webstore.iec.ch/publication/68737	ISO/IEC 20924:2021 RLV contains both the official IEC International Standard and its Redline version. The Redline version is available in English only and provides you with a quick and easy way to compare all the changes between the official IEC Standard and its previous edition. ISO/ IEC 20924:2021 (E) provides a definition of Internet of Things along with a set of terms and definitions. This document is a terminology foundation for the Internet of Things.	
ISO/ IEC JTC1	ISO/IEC 30147:2021	https://webstore.iec.ch/publication/62644	ISO/IEC 30147:2021(E) 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.	S2.6, S2.8, S2.9, S2.10, S2.11, S2.13, S2.19
ISO/ IEC JTC1	ISO/IEC 30144:2020	https://webstore.iec.ch/publication/62503	ISO/IEC 30144:2020 (E) specifies intelligent wireless sensor network (iWSN) from the perspectives of iWSN's system infrastructure and communications internal and external to the infrastructure, and technical requirements for iWSN to realize smart electrical power substations.	S2.7, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30143:2020	https://webstore.iec.ch/publication/62405	ISO/IEC 30143:2020 provides the guidelines for designing and developing new applications in the underwater environment such as fish farming, environment monitoring, harbour security, etc. This document also: a) provides the components required for developing the application; b) provides instructions for modelling the application with examples; c) helps the user to understand the communication between the elements in the application for modelling the communication between elements; d) guides the user with the design process of underwater applications.	S2.7
ISO/ IEC JTC1	ISO/IEC 30140-1:2018	https://webstore.iec.ch/publication/60609	ISO/IEC 30140-1:2018(E) This part of ISO/IEC 30140 provides a general overview of underwater acoustic sensor networks (UWASN). It describes their main characteristics in terms of the effects of propagation variability and analyses the main differences with respect to terrestrial networks. It further identifies the specificities of UWASN and derives some specific and general requirements for these networks.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 21823-3:2021	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: a) requirements of the core ontologies for semantic interoperability; b) 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; c) cross-domain specification and formalization of ontologies to provide harmonized utilization of existing ontologies; d) 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 e) use cases and service scenarios that exhibit necessities and requirements of semantic interoperability.	S2.1, S2.18
ISO/ IEC JTC1	ISO/IEC 21823-2:2020	https://webstore.iec.ch/publication/61085	ISO/IEC 21823-2:2020 (E) specifies a framework and requirements for transport interoperability, in order to enable the construction of IoT systems with information exchange, peer-to-peer connectivity and seamless communication both between different IoT systems and also among entities within an IoT system. This document specifies: transport interoperability interfaces and requirements between IoT systems; transport interoperability interfaces and requirements within an IoT system.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC TR 30166:2020	https://webstore.iec.ch/publication/64321	ISO/IEC TR 30166:2020 (E) describes the following: a) general Industrial IoT (IIoT) systems and landscapes which outline characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure and a listing of standardizing organisations, consortia and open-source communities with work on all aspects on IIoT; b) considerations for the future standardization perspective of IIoT including risk analysis, new technologies and identified collaboration.	
ISO/ IEC JTC1	ISO/IEC 30165:2021	https://webstore.iec.ch/publication/63972	ISO/IEC 30165:2021 specifies the framework of a real-time IoT (RT-IoT) system, including: a) RT-IoT system conceptual model based on domain-based IoT reference model defined in ISO/IEC 30141; b) impacts of time-parameter in terms of four viewpoints (time, communication, control and computation).	S2.3, S2.5
ISO/ IEC JTC1	ISO/IEC TR 30164:2020	https://webstore.iec.ch/publication/62522	ISO/IEC TR 30164:2020 describes the common concepts, terminologies, characteristics, use cases and technologies (including data management, coordination, processing, network functionality, heterogeneous computing, security, hardware/ software 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.	S2.4

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30163:2021	https://webstore.iec.ch/publication/63491	ISO/IEC 30163:2021 specifies the system requirements of an Internet of Things (IoT)/ Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including: a) System infrastructure that describes functional components; b) System and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.; c) Performance requirements and performance specifications of each functional component; d) Interface definition of the integrated platform system. This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.	S2.7
ISO/ IEC JTC1	ISO/IEC 30162:2022	https://webstore.iec.ch/publication/63489	ISO/IEC 30162:2022 specifies network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of: a) data transmission protocols interaction; b) distributed data interoperability & management; c) connectivity framework; d) connectivity transport; e) connectivity network; f) best practices and guidance to use in IIoT area.	S2.1, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30161:2020	https://webstore.iec.ch/publication/63404	ISO/IEC 30161-1:2020(E) specifies requirements for an Internet of Things (IoT) data exchange platform for various services in the technology areas of: a) the middleware components of communication networks allowing the co-existence of IoT services with legacy services; b) the end-points performance across the communication networks among the IoT and legacy services; c) the IoT specific functions and functionalities allowing the efficient deployment of IoT services; d) the IoT service communication networks' framework and infrastructure; and e) the IoT service implementation guideline for the IoT data exchange platform.	S2.1, S2.7
ISO/ IEC JTC1	ISO/IEC 30149 ED1	https://www.iec.ch/dyn/www/f?p=103:38:6519395980104::::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.	S2.6, S2.8, S2.9, S2.10 S2.11, S2.13 S2.19
ISO/ IEC JTC1	ISO/IEC TR 30148:2019	https://webstore.iec.ch/publication/63562	ISO/IEC TR 30148:2019 (E) describes: a) the structure of wireless gas meter networks, and b) the application protocol of wireless gas meter networks.	S2.7
ISO/ IEC JTC1	ISO/IEC 30141:2018	https://webstore.iec.ch/publication/60606	This document provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT Conceptual Model, deriving a high level system based reference with subsequent dissection of that model into five architecture views from different perspectives.	
ISO	(NEW) ISO ISO/CD 24227 ISO/CD 24227	www.iso.org/standard/78134.html	Validation protocol for walking speed as extracted from various sensor systems that measure human body motion for the healthcare sector	S2.5, S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO	(NEW) ISO ISO 31700-1:2023	https://www.iso.org/standard/84977.html	Consumer protection — Privacy by design for consumer goods and services Part 1: High-level requirements	S2.6
ISO	(NEW) ISO ISO/IEEE 11073 (2014)	https://www.iso.org/standard/77338.html	Health informatics — Device interoperability Part 10101: Point-of-care medical device communication — Nomenclature	S2.5, S2.7, S2.22
ISO	(NEW) ISO ISO/PAS 19450:2015	https://www.iso.org/standard/84612.html?browse=tc	Automation systems and integration — Object-Process Methodology	S2.22
ISO/IEC	(NEW) IEC 80001-1:2021	https://www.iso.org/standard/72026.html	IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software	S2.5, S2.14, S2.6
ISO	(NEW- ISO 27269:2025	https://www.iso.org/standard/84639.html	Health informatics — International patient summary	
ISO	(NEW) ISO/ DPAS 24305	https://www.iso.org/standard/78390.html	Health informatics — Guidelines for implementation of HL7 FHIR based on ISO 13940:2015, ISO 13606-1:2019 and ISO 13606-3:2019 This document provides guidance on how four complementary international standards can be used in combination by developers of health ICT systems and infrastructures.	S2.5, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO	(NEW) ISO 27799 :2016(en)	https://www.iso.org/obp/ui/es/#iso:std:iso:27799:ed-2:v1:en	This International Standard provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.	S2.6
ISO/IEC	(NEW) ISO/ IEC 15408-1:2022	https://www.iso.org/standard/72891.html	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security Part 1: Introduction and general model	S2.6, S2.9, S2.10
ISO/IEC	(NEW) ISO/IEC 18045:2022	https://www.iso.org/standard/72889.html	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation	S2.6, S2.9, S2.10
ISO	(NEW) ISO 81001-1:2021	https://www.iso.org/standard/71538.html	Health software and health IT systems safety, effectiveness and security Part 1: Principles and concepts	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO	(NEW) SO/TS 81001-2-1:2025	https://www.iso.org/standard/82210.html	Health software and health IT systems safety, effectiveness and security Part 2-1: Coordination — Guidance and requirements for the use of assurance cases for safety and security This document establishes requirements and gives guidance on assurance case framework for healthcare delivery organizations (HDOs) and for health software and medical device manufacturers (MDMs) and can be used to support the communication and information transfer between all parties. An assurance case can be used to communicate information and knowledge about different risks to other roles.	S2.6
ISO	(NEW) ISO TC 215 ISO 81001 (part 3) (Abandoned)	https://genorma.com/en/standards/iso-pwi-81001-3-1	Health software and health IT systems safety, effectiveness and security — Part 3-1: Healthcare Delivery Organization guidance	
ISO	(NEW) ISO TC 215 ISO 81001 (part 4) Will replace IEC 80001-1:2021	https://www.iso.org/standard/94014.html	ISO/CD 81001-4-1 Health software and health IT systems safety, effectiveness and security Part 4-1: Application of risk management in the implementation and clinical use phases	S2.14, S2.6
ISO	(NEW) IEC 81001-5-1:2021	https://www.iso.org/standard/76097.html	Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/IEC 18045:2022	https://www.iso.org/standard/72889.html	The target audience for this document is primarily evaluators applying the ISO/IEC 15408 series and certifiers confirming evaluator actions. Evaluation sponsors, developers, protection profile (PP), PP-Module, PP-Configuration, and security target (ST) authors, and other parties interested in IT security, can be a secondary audience. This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.	S2.6, S2.9, S2.10
ISO/ IEC JTC1	(NEW) ISO/ IEC 15408-1:2022	https://www.iso.org/standard/72891.html	The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software. This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This document provides an overview of all parts of the ISO/ IEC 15408 series. It describes the various parts of the ISO/ IEC 15408 series; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given. This document introduces: the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types; a description of the organization of security components throughout the model; the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations; general information about the evaluation methods given in ISO/IEC 18045; guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045; general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5; information in regard to the scope of evaluation schemes.	S2.6, S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 15408-2:2022	https://www.iso.org/standard/72892.html	Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP, PP-Module, functional package or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus. Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies. This document defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.	S2.6, S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 15408-3:2022	https://www.iso.org/standard/72906.html	Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PP-Configuration, or a Security Target (ST). These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs. This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).	S2.6, S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 15408-4:2022	https://www.iso.org/standard/72913.html	This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities. This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest. In particular, this document describes a framework that can be used for deriving evaluation activities from work units of ISO/IEC 18045 and grouping them into evaluation methods (EMs). Evaluation activities or evaluation methods can be included in protection profiles (PPs) and any documents supporting them. Where a PP, PP-Configuration, PP-Module, package, or Security Target (ST) identifies that specific evaluation methods/evaluation activities are to be used, then the evaluators are required by ISO/ IEC 18045 to follow and report the relevant evaluation methods/evaluation activities when assigning evaluator verdicts.	S2.6, S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			As noted in ISO/IEC 15408-1, in some cases an evaluation authority can decide not to approve the use of particular evaluation methods/evaluation activities: in such a case, the evaluation authority can decide not to carry out evaluations following an ST that requires those evaluation methods/evaluation activities. This document also allows for evaluation activities to be defined for extended SARs, in which case derivation of the evaluation activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/ IEC 15408-3 for SARs (such as when defining rationales for evaluation activities), then, in the case of an extended SAR, the reference applies instead to the equivalent action elements and work units defined for that extended SAR. For clarity, this document specifies how to define evaluation methods and evaluation activities but does not itself specify instances of evaluation methods or evaluation activities.	
ISO/ IEC JTC1	(NEW) ISO/ IEC 15408-5:2022	https://www.iso.org/standard/72917.html	This document provides pre-defined packages of security requirements. Such security requirements can be useful for stakeholders as they strive for conformity between evaluations. Packages of security requirements can also help reduce the effort in developing Protection Profiles (PPs) and Security Targets (STs).	S2.6, S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC TR 40141	https://www.iec.ch/dyn/www/f?p=103:38:16526658145347::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,126453	This document provides: - Guidance on using the ISO/ IEC 30141 - IoT Reference Architecture Edition 2; - Background on the changing context IoT systems are being developed in, an overview of the different sections of the IoT Reference Architecture; - Some rationales on why to use the IoT Reference Architecture and information about how to use it to architect an IoT system; and - An explanation of construction patterns.	S2.7
ISO/ IEC JTC1	(NEW) ISO/IEC 20924:2024	https://webstore.iec.ch/en/publication/70408	ISO/IEC 20924:2024 is available as ISO/IEC 20924:2024 RLV which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. ISO/IEC 20924:2024 provides a definition of Internet of Things and digital twin along with a set of terms and definitions. This document is a terminology foundation for the Internet of Things and digital twin. This third edition cancels and replaces the second edition published in 2021. This edition constitutes a technical revision. This edition includes the following technical changes with respect to the previous edition: a) addition of new terms which are used in other ISO/IEC IoT related standards; b) update of some definitions to align with current usage in IoT standards; c) extension of digital twin related vocabularies with title and scope changes	S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 30161-2:2023	https://webstore.iec.ch/en/publication/68295	SO/IEC 30161-2:2023 specifies the following items for the transport interoperability between nodal points in the IoT data exchange platform (IoT DEP): requirements, functional blocks, operation mechanism.	S2.7
ISO	(NEW) ISO 5231:2022	https://www.intertekinform.com/en-gb/standards/itu-t-y-suppl-76-09-2023--1344020_saig_itu_itu_3342182/	This document specifies an extensible communication system concept and defines rules for adding new functionalities to cover specific use cases.	S2.7, S2.14
ISO/ IEC JTC1	(NEW) ISO/ IEC TS 30168:2024	https://webstore.iec.ch/en/publication/66553	ISO/IEC TS 30168:2024 specifies a generic programming interface for the integration of secure elements within Industrial IoT devices. This includes requirements from industrial usage scenarios and applications. This document also provides guidance for implementation and testing.	S2.14, S2.9, S2.10
ISO/ IEC JTC1	(NEW) ISO/ IEC AWI 21823-5 Internet of Things (IoT) - Behavioral and policy interoperability	https://www.iso.org/standard/90177.html	This document focuses on Interoperability for IoT systems and in particular on Behavioural and policy interoperability.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-1:2020	https://www.iso.org/standard/73581.html	Information technology — Media context and control Part 1: Architecture: Specifies the architecture of MPEG-V (media context and control) and its three types of associated use cases: information adaptation from virtual world to real world; information adaptation from real world to virtual world; information exchange between virtual worlds. MPEG-V (Media context and control) provides an architecture and specifies associated information representations to enable the interoperability between virtual worlds, e.g., digital content providers of a virtual world, (serious) gaming, simulation, and with the real world, e.g., sensors, actuators, vision and rendering, robotics. MPEG-V is applicable in various business models/ domains for which audiovisual contents can be associated with sensorial effects that need to be rendered on appropriate actuators and/or benefit from well-defined interaction with an associated virtual world.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-2:2018	https://www.iso.org/standard/73580.html	Information technology - Media context and control, Part 2: Control information. Specifies syntax and semantics of the tools required to provide interoperability in controlling devices (actuators and sensors) in real as well as virtual worlds: Control Information Description Language (CIDL) as an XML schema-based language which enables one to describe a basic structure of control information; Device Capability Description Vocabulary (DCDV), an XML representation for describing capabilities of actuators such as lamps, fans, vibrators, motion chairs, scent generators, etc.; Sensor Capability Description Vocabulary (SCDV), interfaces for describing capabilities of sensors such as a light sensor, a temperature sensor, a velocity sensor, a global position sensor, an intelligent camera sensor, etc.; Sensory Effect Preference Vocabulary (SEPV), interfaces for describing preferences of individual user on specific sensorial effects such as light, wind, scent, vibration, etc.; Sensor Adaptation Preference Vocabulary (SAPV), interfaces for describing preferences on a sensor of an individual user on each type of sensed information.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-3:2019	https://www.iso.org/standard/71076.html	Information technology - Media context and control. Part 3: Sensory information. Specifies syntax and semantics of the tools describing sensory information to enrich audio-visual contents: Sensory Effect Description Language (SEDL) as an XML schema-based language which enables one to describe a basic structure of sensory information; Sensory Effect Vocabulary (SEV), an XML representation for describing sensorial effects such as light, wind, fog, vibration, etc. that trigger human senses.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-4:2018	https://www.iso.org/standard/73579.html	Information technology - Media context and control. Part 4: Virtual world object characteristics. Specifies syntax and semantics of the tools used to characterize a virtual world object related metadata: Virtual World Object Characteristics (VWOC) as an XML Schema-based language which enables one to describe a basic structure of avatars and virtual world objects in virtual environments.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-5:2019	https://www.iso.org/standard/73438.html	Information technology - Media context and control, Part 5: Data formats for interaction devices. Specifies syntax and semantics of the data formats for interaction devices by providing a standardized format for interfacing actuators and sensors by defining XML schema-based language named Interaction Information Description Language (IIDL). IIDL provides a basic structure with common information for communication with various actuators and sensors in consistency. Device Command Vocabulary (DCV) is defined to provide a standardized format for commanding individual actuator, and Sensed Information Vocabulary (SIV) is defined to provide a standardized format for holding information from individual sensors either to get environmental information from real world or to influence virtual world objects using the acquired information based on IIDL.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-6:2019	https://www.iso.org/standard/73439.html	Information technology - Media context and control, Part 6: Common types and tools. Provides definitions of data types and tools, which are used in other parts of the ISO/IEC 23005 series but are not specific to a single part.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	(NEW) ISO/ IEC 23005-7:2019	https://www.iso.org/standard/75529.html	Information technology - Media context and control. Part 7: Conformance and reference SW. Specifies the conformance and reference SW implementing the normative clauses of all parts of the ISO/IEC 23005 series. The information provided is applicable for determining the reference SW modules available for the parts of the ISO/IEC 23005 series, understanding the functionality of the available reference SW modules, and utilizing the available reference SW modules.	S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10
ISO/ IEC JTC1	(NEW) ISO/ IEC TR 23844:2023	https://www.iso.org/standard/77144.html	Information technology for learning, education, and training — Immersive content and technology: Specifies potential directions for using immersive technologies in learning, education, and training (LET) and provides suggestions on what can be standardized for this purpose. For the purposes of this document, immersive technologies include augmented reality (AR), virtual reality (VR), mixed reality or merged reality (MR). The document does not apply to technologies such as metaverse, digital twin and extended reality (XR).	S2.25.9, S2.25.13, S2.25.14
ISO/ IEC JTC1	(NEW) ISO/ IEC DIS 24931-1	https://www.iso.org/standard/88529.html	Information Technology — Metaverse Part 1 - Concepts, definitions and terminology: This document provides an overview of the Metaverse, defines terms and terminology used for the Metaverse and defines concepts for the Metaverse.	S2.25.9, S2.25.13, S2.25.14
ISO/ IEC JTC1	(NEW) ISO/ IEC CD TR 25468	https://www.iso.org/en/contents/data/standard/09/04/90497.html	Information technology — Learning, education, and training — Metaverse services for LET: This document focuses on earning, education, and training for Metaverse. Currently under development.	S2.25.9, S2.25.13, S2.25.14

Table 7: AIOTI/EUOS indentified IoT challenges covered/addressed by CEN/CENELEC

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 13757-3:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:61820&cs=1699FDB9F0D54F7BB01D7266589ED286A	This draft European Standard specifies application protocols for communication systems for meters and remote reading of meters. This draft European Standard specifies application protocols, especially the M-Bus application protocol. This draft European Standard is intended to be used with the lower layer specifications determined in EN 13757-2, EN 13757-4, EN 13757-5, EN 13757-6 and prEN 13757-7.	S2.1
CEN	EN 13757-4:2019	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:60262&cs=156CDF6A723103E3251766A06586779B6	This European Standard specifies the requirements of parameters for the physical and the link layer for systems using radio to read remote meters. The primary focus is to use the Short Range Device (SRD) unlicensed telemetry bands. The standard encompasses systems for walk-by, drive-by and fixed installations. As a broad definition, this European Standard can be applied to various application layers.	S2.1
CEN	EN 13757-6:2015	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41515&cs=14E87496D5D72D87C65ABEBFFCB3BD0AB	This European Standard specifies the physical layer parameters of a local meter readout system (Local Bus) for the communication with and the readout of a single meter or a small cluster of meters via a single battery powered readout device (master) which can be connected temporarily or stationary for the communication directly to a meter (i.e. local readout) or via a fixed wiring or a small bus (i.e. remote readout). For generic descriptions concerning communication systems for meters and remote reading of meters, refer to EN 13757-1.	S2.1
CEN	EN 13757-7:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:61822&cs=107399C785EC0B2EDACF60D74955A90D5	This draft European Standard specifies Transport and Security Services for communication systems for meters and remote reading of meters. This draft European Standard specifies secure communication capabilities by design and supports the building of a secure system architecture. This draft European standard is applicable to the protection of consumer data to ensure privacy. This draft European Standard is intended to be used with the lower layer specifications determined in EN 13757-2, EN 13757-3, EN 13757-4, EN 13757-5 and EN 13757-6.	S2.1, S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 1434-3:2015	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41516&cs=157EF44C329D0ADE1DB97DF0406BAA443	This European Standard specifies the general requirements and applies to heat meters. Heat meters are instruments intended for measuring the energy which in a heat-exchange circuit is absorbed (cooling) or given up (heating) by a liquid called the heat-conveying liquid. The meter indicates heat in legal units. Part 3 specifies the data exchange between a meter and a readout device (POINT / POINT communication). For these applications using the optical readout head, the EN 62056-21 protocol is recommended. For direct or remote local readout of a single or a few meters via a battery driven readout device, the physical layer of EN 13757-6 (local bus) is recommended. For bigger networks with up to 250 meters, a master unit with AC mains supply according to EN 13757-2 is necessary to control the M-Bus. For these applications the physical and link layer of EN 13757-2 and the application layer of EN 13757-3 is required. For wireless meter communications, EN 13757-4 describes several alternatives of walk/drive-by readout via a mobile station or by using stationary receivers or a network. Both unidirectionally and bidirectionally transmitting meters are supported by this standard.	S2.1, S2.18
CEN	EN 16836-2:2016	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41099&cs=181323929D1945B365914E7CE01F502AD	This European Standard specifies the medium access control/physical layer MAC/PHY and networking layer of a communication protocol for the exchange of data from metering devices to other devices within a mesh network. The referenced documents in this European Standard contain specifications, interface descriptions, object descriptions, protocols and algorithms pertaining to this protocol standard, the device objects, device profile, the application framework, the network layer, and security services. They are referenced in their entirety for reasons of backwards compatibility and interoperability with products in the field currently using this technology.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16836-3:2016	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41100&cs=1C46CE950442B0C43F9EDDAC4585ACF19	This European Standard specifies the application layer of a communication protocol for the exchange of data from metering devices to other devices within a mesh network. This European Standard makes reference to a number of documents whereby core requirements are specified. This referencing is in compliance with the Bridge Consortium and additionally the Memorandum of Understanding between the ZigBee Alliance and CEN/CENELEC. The EN 16836 series represents a feature subset of a larger standard and as such not all of the features specified in the referenced documents are specified in this standard, due to some features being outside the scope of CEN/TC 294. Where this is the case the out of scope feature has either been omitted or specified as excluded.	S2.1, S2.24
CEN	CEN/TR 17167:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:61828&cs=1338F0A4C7239D0EC0470C6E1605E2BCF	This Technical Report contains additional information to the requirements determined in EN 13757-2, EN 13757-3 and EN 13757-7, in particular examples for the implementation, Datagram examples secured by security mechanism of part 7 and additional non-normative requirements beyond meter communication itself.	S2.1, S2.6
CEN	EN ISO 14814:2006	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:21173&cs=184DD778D0F4ED9BEEC2F72C92F3FFFB1	ISO 14814:2006 establishes a common framework to achieve unambiguous identification in ITS/RTTT (Intelligent Transport Systems/Road Transport and Traffic Telematics) AVI/AEI (Automatic Vehicle Identification/Automatic Equipment Identification) applications. This scheme and Reference Architecture Model is designed to be an “enabling” structure to allow interoperability between different commercial systems, and not prescriptive in determining any one system. It is not frequency- nor air interface protocol-specific, provides maximum interoperability, has a high population capability, and provides the possibility of upwards migration to more capable systems. ISO 14814:2006 provides a reference structure which enables an unambiguous identification and also identifies the data construct as an ITS/RTTT message. The construct also identifies which ITS/RTTT data structure is contained in the message.	S2.1, S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	prEN 13757-8	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73097,25&cs=19B94878D7D6F98142DFDE0433CC7D3C1	This document describes the functionalities and specifies the requirements of an Adaptation Layer to be applied when transporting M-Bus upper layers using a wireless communication protocol other than Wireless M-Bus. These alternative radio technologies developed outside CEN/TC 294 could be based on Internet Protocol or not and operate either in licensed or unlicensed frequency bands.	S2.1
CENELEC	CENELEC EN 50090 (ISO 14543)	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110::::FSP_PROJECT,FSP_ORG_ID:55668,1258281&cs=14BD408738BD97FB5CF4581F27FF76877	System Architecture, Communications/Networking, Data and Information Management - KNX is an open standard (see EN 50090, ISO/IEC 14543) for commercial and domestic building automation. KNX evolved from three earlier standards: the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB or Instabus). On this network, the devices form distributed applications and tight interaction is possible. This is implemented via interworking models with standardized datapoint types and objects, modelling logical device channels.	
CEN	CEN/ TC 294 (Communication systems for meters and remote reading of meters)	https://standards.iteh.ai/catalog/tc/cen/a0640f96-2f0c-4456-af8e-20887cd8b203/cen-tc-294-wg-6	Produce and maintain standards for meter data exchange protocols, for use over short range wireless networks with meshing functionality. Note: Work will be based on existing ZigBee specifications.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16157-1:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:62523&cs=15997C7B-B19A97A296D8A7719196409AD	This document specifies and defines components required to support the exchange and shared use of data and information in the field of traffic and travel. The components include the framework and context for the modelling approach, data content, data structure and relationships. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator-initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. This part of EN 16157 specifies the DATEX II framework of all parts of this European Standard, the context of use and the modelling approach taken and used throughout this European Standard. This approach is described using formal methods and provides the mandatory reference framework for all other parts	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identi-fied IoT challeng-es
	Title	URL	Abstract	Labels & Sections
CEN	EN 16157-2:2019	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:60747&cs=1C3A140087AD1FDE865115EA876607C93	This European Standard series (EN 16157) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard series is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This European Standard series establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this European Standard series may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content: - road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment, - operator initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. This part of the EN 16157 series specifies the informational structures, relationships, roles, attributes and associated data types, for the implementation of the location referencing systems used in association with the different publications defined in the Datex II framework. It also defines a DATEX II publication for exchanging predefined locations. This is part of the DATEX II platform independent data model	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16157-3:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:60748&cs=13B159A7784936BDC97A42AFA8C21211A	This document specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - operator-initiated actions, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and instructions relating to use of the road network. This document specifies the informational structures, relationships, roles, attributes and associated data types required for publishing situation traffic and travel information within the DATEX II framework. This is specified as a DATEX II Situation Publication sub-model which is part of the DATEX II platform independent model, but this part excludes those elements that relate to: - location information which are specified in FprEN 16157 2; - common information elements, which are specified in EN 16157 7.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16157-4:2021	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::F-SP_PROJECT:68227&cs=19CD8A5DF-8D8A747A2648590BAC670053	This European Standard (EN 16157 series) specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. This European Standard is applicable to: - Traffic and travel information which is of relevance to road networks (non-urban and urban), - Public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - Traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This European Standard establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), Use of this European Standard may be applicable for use by other actors. This European Standard series covers, at least, the following types of informational content: - Road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment, - Operator initiated actions, - Road traffic measurement data, status data, and travel time data, - Travel information relevant to road users, including weather and environmental information, - Road traffic management information and instructions relating to use of the road network. This part of the CEN/TS 16157 series specifies the informational structures, relationships, roles, attributes and associated data types required for publishing variable message sign information within the Datex II framework.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This is specified in two publications, a DATEX II VMS Table Publication sub-model and a VMS Publication sub-model, which are part of the DATEX II platform independent model, but this part excludes those elements that relate to: - location information which are specified in EN 16157-2, - common information elements, which are specified in EN 16157-7, - situation information which are specified in EN 16157-3. The VMS Table Publication supports the occasional exchange of tables containing generally static reference information about deployed VMS which enable subsequent efficient references to be made to pre-defined static information relating to those VMS. The VMS Publication supports the exchange of the graphic and textual content of one or several VMS plus any status information on device configuration that aid the comprehension of the informational content. This content is potentially subject to rapid change. These publications are not intended to support the control or configuration of VMS equipment. Each is part of the DATEX II platform independent model.	
CEN	EN 16157-5:2020	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68225&cs=15C7361EFFD209FF289AF2AAE0FBC17A1	This document is the fifth part of the DATEX II European Standard which deals with the publication sub-models within the DATEX II model that support the exchange of measured and elaborated information. These publications are intended to support the exchange of informational content from the organization having the measured data and creating elaborated data to other organisations providing ITS services or onward information exchange. It also includes the exchange of static information about measurement sites. This is specified in three sub-models, a DATEX II Measurement Site Table Publication sub-model, a DATEX II Measured Data Publication sub-model and a DATEX II Elaborated Data Publication sub-model.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16157-7:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:62524&cs=14AD3FDA01670AAB7137D7857613CB12B	This document specifies and defines component facets required to support the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for data content, data structure and relationships, communications specification. This document is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban), - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service), - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This document establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs), Use of this document can be applicable for use by other actors. This document covers, at least, the following types of informational content: - road traffic event information - planned and unplanned occurrences both on the road network and in the surrounding environment, - information about operator initiated actions - including both advisory and mandatory measures, - road traffic measurement data, status data, and travel time data, - travel information relevant to road users, including weather and environmental information, - road traffic management information and information and advice relating to use of the road network. This part of EN 16157 specifies common informational structures, relationships, roles, attributes and associated data types required for publishing information within the DATEX II framework. This is specified as a DATEX II sub-model which is part of the DATEX II platform independent model, but this part only covers common elements that are used by more than one publication. It excludes those elements that relate to location information which are specified in FprEN 16157 2.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN ISO/TS 19468:2022	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:71962&cs=18889333092FF2E127C49B472E09BA2FB	This document defines and specifies component facets supporting the exchange and shared usage of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the data content, structure and relationships necessary and the communications specifications, in such a way that they are independent from any defined technical platform. This document establishes specifications for data exchange between any two instances of the following actors: — Traffic information centres (TICs); — Traffic control centres/ Traffic management centres (TCCs/ TMCs); — Service providers (SPs). This document can also be applied for use by other actors, e.g. car park operators. This document includes the following types of information: — use cases and associated requirements, and features relative to different exchange situations; — different functional exchange profiles; — abstract elements for protocols; — data model for exchange (informational structures, relationships, roles, attributes and associated data types required). In order to set up a new technical exchange framework, it is necessary to associate one functional exchange profile with a technical platform providing an interoperability domain where plug-and-play interoperability at a technical level can be expected. The definition of such interoperability domains is out of scope of this document but can be found in other International Standards or Technical Specifications (e.g. the ISO 14827 series). This document is restricted to data exchange. Definition of payload content models is out of the scope of this document.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN/TS 16157-10:2022	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::F-SP_PROJECT:71189&cs=17CE8E7FC-7390CF7CC48C34700D0A825D	The EN 16157 series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships. The EN 16157 series is applicable to: - traffic and travel information which is of relevance to road networks (non-urban and urban); - public transport information that is of direct relevance to the use of a road network (e.g. road link via train or ferry service); - traffic and travel information in the case of Cooperative intelligent transport systems (C-ITS). This series establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs); - Traffic Control Centres (TCCs); - Service Providers (SPs). Use of this series can be applicable for use by other actors. This series covers, at least, the following types of informational content: - road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment; - operator initiated actions; - road traffic measurement data, status data, and travel time data; - travel information relevant to road users, including weather and environmental information; - road traffic management information and instructions relating to use of the road network. This part of the CEN/TS 16157 series specifies details of infrastructure for vehicle energy supply. The provided data model is separated into two publications for static and dynamic information. The static information regarding the infrastructure is not subject to frequent changes, whereas the dynamic part offers the ability to provide highly up-to-date information. The static part covers all relevant information on vehicle energy infrastructure, e.g. sites, stations and refill points for electric vehicles as well as petrol, gasoline or gas-based refuelling for vehicles. In terms of dynamic information, the availability of the infrastructure, possible faults and a price indication are covered.	S2.1, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN/TS 16157-11	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:71777&cs=10465408B33310E1C137C3B2AABC7EE51	This document specifies a publication sub-model within the DATEX II model that supports the publication of electronic traffic regulations. This publication is intended to support the exchange of informational content from road traffic authorities issuing traffic regulation orders and organisations implementing these orders to other organisations providing ITS services or onward information exchange.	S2.1
CEN	CEN/TS 16157-12	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73025,25&cs=191FBA7A8FAE57738466F76A27106F67D	This document specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, data content, data structure and relationships.	S2.1
CEN	(Updated) CEN/TS 16157-6:2015	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:69724,25&cs=1451A03D2D2D1D87355F1559FEB7FA425	This new work item will revise and extend the sixth part of the DATEX II Technical Specifications which defines three DATEX II parking-related publications and a truck parking profile and that supports the exchange of static as well as dynamic information about parking facilities and areas, including intelligent truck parking as defined by the Directive 2010/40/EU priority action e as well as urban parking as specified in action a. The formerly used Level B extension will be replaced by a new namespace in the context of version 3.0 of DATEX II. The publications are intended to support the exchange of informational content from the organisation performing measurements and collecting/eliciting basic data to other organisations providing ITS services or onward information exchange. It is the ambition to harmonise existing information models from different sources such as EasyWay deployment guidelines and truck parking initiatives, and to liaise with the stakeholders involved, especially with the Alliance for Parking Data Standards and CEN/TC 278 working group 3.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
CEN	CEN/TS 16157-8	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68653&cs=18BC2B0B4960475D11D2ABEA1D8C23A2D	This document constitutes a Part of the CEN 16157 DATEX II series of standards and technical specifications. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for exchanges, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 8, this document, specifies additional data model structures that are applicable for traffic management applications in the urban environment. This Part addresses data concepts to support the exchange of Traffic Management Plans, rerouting, extensions of the existing DATEX II core model to better support application to the urban environment. It establishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document may be applicable for use by other actors.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identi-fied IoT challeng-es
	Title	URL	Abstract	Labels & Sections
CEN	CEN/TS 16157-9	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68652&cs=18B5180A209437120996363BB8237DDAC	This document constitutes a part of the CEN 16157 DATEX II series of standards and technical specifica-tions. This series specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and travel. The component facets include the framework and context for ex-changes, the modelling approach, the data content, the data structure and relationships and the communications specification. Part 9, this document, specifies additional data model struc-tures that are applicable for traffic signal management applications in the urban environment. This part specifies data concepts to support the exchange of traffic signal status messaging, intersection geometry definition and attribution in a consist-ent way with existing C-ITS standards and technical specifications. It estab-lishes specifications for data exchange between any two instances of the following actors: - Traffic Information Centres (TICs), - Traffic Control Centres (TCCs), - Service Providers (SPs). Use of this document may be applicable for use by other actors	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN/TS 16614-1:2020	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:66892&cs=1CAED5ABB1179CBAE5D7E61C865704C55	1.1 General NeTEx is dedicated to the exchange of scheduled data (network, timetable and fare information). It is based on Transmodel V6 (EN 12896 series) and SIRI (CEN/TS 15531-4/-5 and EN 15531-1/-2/-3) and supports the exchange of information of relevance for passenger information about public transport services and also for running Automated Vehicle Monitoring Systems (AVMS). NOTE Many NeTEx concepts are taken directly from Transmodel; the definitions and explanation of these concepts are extracted directly from the respective standard and reused in NeTEx, sometimes with adaptions in order to fit the NeTEx context. Although the data exchanges targeted by NeTEx are predominantly oriented towards provisioning passenger information systems and AVMS with data from transit scheduling systems, it is not restricted to this purpose and NeTEx can also provide an effective solution to many other use cases for transport data exchange. 1.2 Transport modes All mass public transport modes are taken into account by NeTEx, including train, bus, coach, metro, tramway, ferry, and their submodes. It is possible to describe airports and air journeys, but there has not been any specific consideration of any additional requirements that apply specifically to air transport. 1.3 Compatibility with existing standards and recommendations Concepts covered in NeTEx that relate in particular to long-distance train travel include; rail operators and related organizations; stations and related equipment; journey coupling and journey parts; train composition and facilities; planned passing times; timetable versions and validity conditions. In the case of long distance train the NeTEx takes into account the requirements formulated by the ERA (European Rail Agency) - TAP/TSI (Telematics Applications for Passenger/ Technical Specification for Interoperability, entered into force on 13 May 2011 as the Commission Regulation (EU) No 454/2011), based on UIC directives.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identi-fied IoT challeng-es
	Title	URL	Abstract	Labels & Sections
			As regards the other exchange proto-cols, a formal compatibility is ensured with TransXChange (UK), VDV 452 (Germany), NEPTUNE (France), UIC Leaflet, BISON (The Netherlands) and NOPTIS (Nordic Public Transport In-terface Standard). The data exchange is possible either through dedicat-ed web services, through data file exchanges, or using the SIRI exchange protocol as described in part 2 of the SIRI documentation.	
CENE-LEC	(Updated) CENELEC EN 50090-6-3:2023 Home and Building Electronic Systems (HBES)- Part 6-3 -3rd Party HBES IoT API API	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:74475,25&cs=1046EE8EC4361FAC-C3F6370EBB7B68089	The 3rd Party HBES IoT API consists of: Required restful access methods to read or write Endpoints, to set or retrieve Installation state data. Required Endpoints hosting concepts such as Functions and Datapoints comprising the Runtime communica-tion of an (HBES) Installation. Required methods to authorize from an IoT 3rd Party Client, additionally, such as the security methods to be used to access the API. Required access permission control types: for security reasons the actual access to Functions or Datapoints is gated by the IoT 3rd Party Server, this access will be granted as part of the authorization. Endpoints allowing to setup notifica-tions on changes of Installation state data, provided to subscribers that are clients to the Installation. For all Endpoints, their expected request/ response document formats, and their content. Moreover, their mandatory and optional parts.	S2.1, S2.2, S2.6, S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 13757-1	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:65216,6275&cs=1520E24EB7BA8E7321D0D175C7F1CF004	This document specifies data exchange and communications for meters in a generic way. This document establishes a protocol specification for the Application Layer for meters and establishes several protocols for meter communications which can be applied depending on the application being fulfilled. This document also specifies the overall structure of the Object Identification System (OBIS) and the mapping of all commonly used data items in metering equipment to their identification codes. NOTE Electricity meters are not covered by this document, as the standardization of remote readout of electricity meters is a task for CENELEC/IEC.	S2.1, S2.22
CEN	EN 13757-2	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61821,6275&cs=148E2A53815B1043A00AB94D1340B84A1	This draft European standard is applicable to the physical and link layer parameters of baseband communication over twisted pair (M Bus) for meter communication systems. It is especially applicable to thermal energy meters, heat cost allocators, water meters and gas meters. NOTE It is usable also for other meters (like electricity meters) and for sensors and actuators. For generic descriptions concerning communication systems for meters and remote reading of meters see EN 13757-1.	S2.1, S2.22
CEN	EN 13757-5	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:36150,6275&cs=1B9B9291A8674B58CF7FF96F8B88F5B85	This European Standard specifies the protocols to use when performing relaying in wireless meter readout networks. This European Standard is an extension to wireless meter readout specified in EN 13757-4. It supports the routing of modes P and Q, and simple single-hop repeating of modes S, T, C, F and N. The main use of this standard is to support simple retransmission as well as routed wireless networks for the readout of meters. NOTE Electricity meters are not covered by this standard, as the standardisation of remote readout of electricity meters is a task for IEC/CENELEC.	S2.1, S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 16836-1	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::F-SP_PROJECT,FSP_ORG_ID:41098,6275&cs=11019F-C07793E83E7C3B39E9E3A6DBF78	This European Standard gives the standardization framework of communication systems applicable to the exchange of data from metering devices to other devices within a mesh network. This European Standard specifies how to interpret prEN 16836-2:2015 and prEN 16836-3:2015 which give a list of references to the ZigBee documents. This series is applicable to communications systems that involve messages and networking between a meter or multiple meters and other devices in a mesh network, such as in home displays (IHDs) and communications hubs. This European Standard allows routing between devices and also allows channel agility to avoid contention with other networks of the same type, or indeed networks of other types operating in the same frequency bands. This European Standard is designed to support low power communications for devices such as gas and water meters which can make data from such devices available on the mesh network at any time through a proxy capability within a permanently powered device.	S2.1, S2.22
CEN	Updated) CEN prEN 14154-4:2023 Water meters — Part 4: Additional functionalities	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73396,25&cs=1DA0D-2906520CD899CB94F5BB61C72E7F	This document specifies definitions, requirements and testing of additional functionalities for water meters, without metrological impact, in combination with Additional Functionality Devices (AFD) and in response to EU/EFTA Mandate M/441 EN. These AFDs are considered as “ancillary devices” as defined in EN ISO 4064 1:2017 and EN ISO 4064 4:2014. This document does not cover the changing of metrological software within the meter or the upload/download of metrological software.	S2.9
CEN	(Updated)CEN ISO/TS 17425:2016	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:35914&cs=10C18F278124980B-9F4075E355AB45BC3	This document defines the In-Vehicle Signage service and application that delivers In-Vehicle Signage information to ITS stations (vehicle ITS stations or personal ITS stations devices) concerning road and traffic conditions, qualified by road authorities/operators, in a consistent way with road authority’s/operator’s requirements, in the manner that is coherent with the information that would be displayed on a road sign or variable message sign (VMS).	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	(Updated)CEN ISO/TS 17429:2017	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:35915&cs=1DF674B52BAF01613F1CDAABBB1D408E6	ISO/TS 17429:2017 specifies generic mechanisms enabling the exchange of information between ITS stations for applications related to Intelligent Transport Systems. It complies with the ITS station reference architecture (ISO 21217) and defines the following ITS station facilities layer functionalities: - Communication Profile Handler (CPH); - Content Subscription Handler (CSH); - Facilities Services Handler (FSH). These functionalities are used by ITS-S application processes (ITS-S-AP) to communicate with other ITS-S application processes and share information. These functionalities describe - how lower-layer communication services assigned to a given data flow are applied to the service data units at the various layers in the communication protocol stack (CPH, see 6.2.3), - how content from data dictionaries can be published and subscribed to by ITS-S application processes (CSH, see 6.2.5), - how well-known ITS station facilities layer and management services can be applied to application process data units (FSH, see 6.2.4), relieving (ITS-S) application processes from having to implement these services on their own, - how service access points (SAP) primitives specified in ISO 24102-3 are used, - service primitives for the exchange of information between ITS-S application processes and the ITS station facilities layer (FA-SAP), and - a set of communication requirements and objectives (profiles) using the methods defined in ISO/TS 17423 to select the level of performance (best effort or real-time, etc.), confidence and security (authentication, encryption, etc.) for information exchange between ITS stations, such as data provision, event notification, roadside configuration, map update.	S2.1, S2.3, S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identi-fied IoT challeng-es
	Title	URL	Abstract	Labels & Sections
CEN	(Updat-ed) CEN ISO/TS 19091:2019	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:64994&cs=155A0F218787309EC4D33F96797394306	This document defines the message, data structures, and data elements to support exchanges between the roadside equipment and vehicles to address applications to improve safety, mobility and environmental efficiency. In order to verify that the defined messages will satisfy these applications, a systems engineering process has been employed that traces use cases to requirements and requirements to messages and data concepts. This document consists of a single document that contains the base specification and a series of annexes. The base specification lists the derived information requirements (labelled informative) and references to other standards for message definitions where available. Annex A contains descriptions of the use cases addressed by this document. Annexes B and C contain traceability matrices that relate use cases to requirements and requirements to the message definitions (i.e. data frames and data elements). The next annexes list the base message requirements and application-oriented specific requirements (requirements traceability matrix) that map to the message and data concepts to be implemented. As such, an implementation consists of the base plus an additional group of extensions within this document. Details on information requirements, for other than SPaT, MAP, SSM, and SRM messages are provided in other International Standards. The focus of this document is to specify the details of the SPaT, MAP, SSM, and SRM supporting the use cases defined in this document. Adoption of these messages varies by region and their adoption can occur over a significant time period. This document covers the interface between roadside equipment and vehicles. Applications, their internal algorithms, and the logical distribution of application functionality over any specific system architecture are outside the scope of this document.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN ISO/TS 19321:2020	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68350&cs=1FE9288D0BD55B9A6A45F662E5E523F64	This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.	S2.1, S2.18
CEN	(Updated)CEN ISO/TS 19321:2020	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68350&cs=1FE9288D0BD55B9A6A45F662E5E523F65	This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	(Updated) prCEN ISO/ TS 19321 rev	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,F-SP_LANG_ID:73937,25&cs=108B-9C05FB54333B566ACFD5122C7E1F9	This document specifies the in-vehicle information (IVI) data structures that are required by different intelligent transport system (ITS) services for exchanging information between ITS Stations (ITS-S). A general, extensible data structure is specified, which is split into structures called containers to accommodate current-day information. Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazard warnings, location-based services, re-routing. The information in the containers is organized in sub-structures called data frames and data elements, which are described in terms of its content and its syntax. The data structures are specified as communications agnostic. This document does not provide the communication protocols. This document provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.	S2.1
CEN	EN 13757-2:2018/prA1	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,F-SP_LANG_ID:74544,25&cs=1761F-4D6E55C0F87848EB2822BAF9FAAF	This draft European standard is applicable to the physical and link layer parameters of baseband communication over twisted pair (M Bus) for meter communication systems. It is especially applicable to thermal energy meters, heat cost allocators, water meters and gas meters. NOTE It is usable also for other meters (like electricity meters) and for sensors and actuators. For generic descriptions concerning communication systems for meters and remote reading of meters see EN 13757-1.	S2.1, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CENELEC	(Updated) CEN EN 17927:2023 Security Evaluation Standard for IoT Platforms (SESIP).	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:74909,25&cs=157BB6AD851BD6F80A208E00FBBD6B8DD	This document describes a cybersecurity evaluation methodology, named SESIP, for components of connected ICT products. Security claims in SESIP are made based on the security services offered by those components. Components can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of components which apply to the foundational components of devices that are not application specific. The methodology describes the re-use of evaluation results	S2.6
CENELEC	CLC/prTS 50491-7	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:75291,25&cs=1AC4B90B75A5026B198062B2BBB1F96BE	This Technical Specification provides guidance to set-up and manage/ update a cybersecure HBES / BACS system This document provides: 1) Categories of HBES / BACS networks related to cybersecurity updates (managed and unmanaged networks) 2) Risk assessment guide for the above-mentioned categories (at device level for both managed and unmanaged networks, at system level for managed ones only) For manufacturers the document provides a classification scheme based on the security levels from existing standards (ETSI EN 303 645 , IEC 62443). For installers, system integrators and other administrators of HBES/BACS this document provides - a generic method for assessment of the security risk for each product in the perspective of the overall system. The result of the evaluation gives the minimum required security level on product level corresponding to the manufacturer classification above. - A guide to select products to comply with the required security level. - Best practice measures on the system security level. - A guide to enhance the maturity level of the cyber security management process.	S2.9, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN/ CENELEC	CWA 17431	https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa17431.pdf	This CWA addresses a broad set of Principles and Guidance to form a solid foundation for future practice with regard to SEP licensing for ICT standards such as mobile communication standards and other wireless communication standards. The CWA also includes information about licensing to those who are new to the implementation and use of standardised technology and the licensing of patents that cover those technologies.	S2.21
CENELEC	(Updated) CENELEC prEN IEC 63345 Energy Efficiency Systems - Simple External Consumer Display	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:74332,25&cs=10C4D76ADB0C4C7D5B9DA81FF8E547C2D	This Standard specifies a data model to abstract the metering world towards a simple external consumer display. The data model, as described by means of functional blocks contained in this IEC Standard, lays down the format of metering data accessible by a simple external consumer display. This data interface would be typically part of the meter communication functions and be accessed by a simple external consumer display via the H1 interface of the CEN/CLC/ETSI TR 50572 between the display and the meter communication functions.	S2.14, S.2.24
CENELEC	prEN IEC 63402	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:74575,25&cs=167DD57F4AA099C41201ADC1979E157B2	This Standard specifies General Requirements and Architecture of an application layer interface between the Customer Energy Manager (CEM) and Smart Devices (SD) operating within the smart grid premises-side system (i.e. home or building but not industrial premises).	S.2.24

Table 8: AIOTI/EUOS indentified IoT challenges covered/addressed by IEEE

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	IEEE 802.1AS-2020	https://standards.ieee.org/ieee/802.1AS/7121/	This standard defines a protocol and procedures for the transport of timing over bridged and virtual bridged local area networks. 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). The PDF of this standard is available at the IEEEGET program. The "IEEE Get Program" grants public access to view and download individual PDFs of select standards at no charge. Visit http://standards.ieee.org/about/get/index.html for details.	S2.3
IEEE	IEEE 802.11p	https://ieeexplore.ieee.org/document/5514475	Communications/Networking - DSRC is a U.S. Department of Transportation (DOT) project based on ISO's Communications Access for Land Mobiles (CALM) architecture for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars.	S2.3
IEEE	IEEE 1872.2-2021	https://standards.ieee.org/ieee/1872.2/7094/	This standard extends IEEE 1872-2015 Standard for Ontologies for Robotics and Automation to represent additional domain-specific concepts, definitions, and axioms commonly used in Autonomous Robotics (AuR). This standard is general and can be used in many ways - for example, to specify the domain knowledge needed to unambiguously describe the design patterns of AuR systems, to represent AuR system architectures in a unified way, or as a guideline to build autonomous systems consisting of robots operating in various environments.	S2.1, S2.18
IEEE	IEEE 754-2008	https://ieeexplore.ieee.org/document/4610935	This standard specifies formats and methods for floating-point arithmetic in computer systems: standard and extended functions with single, double, extended, and extendable precision, and recommends formats for data interchange. Exception conditions are defined and standard handling of these conditions is specified.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(Updated) IEEE - P1451.99	https://standards.ieee.org/ieee/1451.99/11634/	This standard defines an Internet of Things (IoT) TRusted Area Networking (TRAN) architecture, designated as IoT-TRAN, for harmonizing IEEE Std 1451 sensor networks, IoT and Industrial IoT (IIoT) systems. IoT-TRAN provides an interoperability framework, including communication and semantics, allowing data sharing and interoperability in a trusted environment in which security of messages, agreements between devices, life-cycle management, and ownership of devices are granted over a cloud-oriented, federated, and decentralized network of things. The standard is built on top of the eXtensible Messaging and Presence Protocol (XMPP). A set of technologies is identified, allowing different devices to interoperate regardless of underlying communication technology. Each such technology is built as a standardized extension to this open protocol. A gateway to IoT-TRAN is an infrastructural component identified as a binding providing technology-specific devices reachability and real-time transparent conversion with other devices using their respective IoT protocols. As part of the IEEE Std 1451 standard family, features like Transducer Electronic Data Sheet (TEDS) and IEEE Std 1451.0 Universally Unique Identification (UUID) are leveraged in this standard to enhance the support of interfacing with IoT and IIoT systems.	S2.7, S2.10
IEEE	(NEW) IEEE 2668-2022	https://standards.ieee.org/ieee/2668/7254/	The maturity index of Internet-of-things (IoT), referred to as IDex, is defined in this standard. The formats for 1) the IDex and 2) the IDex database and the IDex evaluation model database are specified. The general mechanism of the IDex evaluation is defined as pertinent to the applications and technical fields of the IoT objects to be evaluated. The IDex can be applied to IoT devices, networks, applications, algorithms, hardware, software, systems, and infrastructure. With slight modifications, the IDex can be extended to evaluate objects and infrastructure in various services, such as smart city services.	S2.1, S2.22
IEEE	(NEW) IEEE SA - IEEE 2735-2022	https://standards.ieee.org/ieee/2735/7392/	A framework for IoT application systems, a definition of a complex virtual instrumentation model, and agreement on a framework and interfaces to achieve interoperability of IoT applications, while specifying the communication methods, invocation parameters and return value formats of the interfaces, is given in this standard.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE 2735.1-2022	https://standards.ieee.org/ieee/2735.1/7393/	This standard designs and standardizes data input interfaces, computing service interfaces, interconnection service interfaces, Laboratory Information Management System (LIMS) service interfaces, functional design requirements, and constraints for Complex Virtual Instruments (CVI) in the field of household appliance testing based on IEEE Std 2735. The purpose is to process the data or metadata from different types of household appliance complex virtual instruments.	S2.1, S2.7, S2.22
IEEE	(NEW) IEEE/ ISO/IEC 42010-2022	https://standards.ieee.org/ieee/42010/6846/	This document specifies requirements for the structure and expression of an architecture description (AD) for various entities, including software, systems, enterprises, systems of systems, families of systems, products (goods or services), product lines, service lines, technologies and business domains. This document distinguishes the architecture of an entity of interest from an AD expressing that architecture. Architectures are not the subject of this document. This document specifies requirements for use of the architectural concepts and their relationships as captured in an AD. It does not specify requirements for any entity of interest or its environment. This document specifies requirements for an architecture description framework (ADF), an architecture description language (ADL), architecture viewpoints and model kinds in order to usefully support the development and use of an AD. This document specifies conformance to the requirements for an AD, ADF, ADL, architecture viewpoint and model kind. This document does not specify the processes, architecting methods, models, notations, techniques or tools by which an AD is created, utilized or managed. This document does not specify any format or media for recording an AD.	S2.17, S2.21

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE 1935-2023	https://standards.ieee.org/ieee/1935/7181/	With the innovation of mobile applications and the arrival of the fifth generation of telecommunication, edge computing has become a popular scheme due to its geo-graphical proximity to end users. The overall architecture has the advantage of lower latency and improved user experience. However, because of physical limitations, management and orchestration in the edge system is necessary to maintain operations, common functions, and application life-cycle. Accordingly, a standardized, orches-tration-wise design to simplify the process and offer better system performance and user experience was introduced by the IEEE P1935 working group. The framework, architecture, and procedures of the edge-fog system as well as its application lifecycle management are involved in this standard.	S2.7, S.2.22
IEEE	(NEW) IEEE 3219-2023	https://standards.ieee.org/ieee/3219/11163/	The surging needs for the Internet of Things (IoT) are dramatically shifting the network structure and challenging the traditional perimeter security paradigm. To establish secure and trustworthy interop-erability among billions of heterogeneous interconnected devices, there is a need for standards defining a common frame-work. In this standard, a blockchain-based Zero-Trust access control framework is defined. The framework provides a typical implementation model and deployment variations, addressing general security and trust in IoT applications with the inspiration of the emerging Zero-Trust paradigm and blockchain technology. The leverage of blockchain and Zero-Trust discussed could provide reliable interactions among people, things, and applications in the presence of failures and attacks, and improve an IoT system's overall information technology security posture.	S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE 1451.0-2024	https://standards.ieee.org/ieee/1451.0/11001/	The common functions, network services, transducer services, and Transducer Electronic Data Sheet (TEDS) formats for members of the IEEE 1451 family of standards to be interoperable in both network interface and transducer interface are provided. The common functions and characteristics that are to be performed by a network capable application processor (NCAP), which is a 1451 server, and all devices that implement the NCAP are defined. A set of network services that includes a set of commands and replies to access transducer data and TEDS data from the NCAP (1451 server) by the Internet of Things (IoT) applications (APPs) that are 1451 clients are also defined. Application programming interfaces (APIs) of network services are outlined to facilitate communications between the APPs (1451 clients) and NCAPs. Furthermore, the common functions and characteristics that are to be performed by a transducer interface module (TIM) and all devices that implement the TIM are discussed. A set of transducer services that includes a set of commands and replies to facilitate the setup and control of the TIM, as well as reading and writing the data used by the NCAP, are outlined. APIs of transducer services are also discussed to facilitate communications between the NCAPs and TIMs. Finally, the formats for a TEDS and methods to access the TEDS are specified, along with the common functions and characteristics that are to be performed by an APP and all devices that implement the APP. Additional Open Source content available here: https://opensource.ieee.org/1451/1451.0-schema/	S2.7
IEEE	(NEW) IEEE 1901c-2024	https://standards.ieee.org/ieee/1901c/10922/	Physical (PHY) and media access control (MAC) layers of an improved flexible channel wavelet (FCW) technology to be usable for communication on any media called extended flexible channel wavelet (FCW) PHY/MAC are specified in this amendment. New communication channels are defined in low-frequency bands to extend the communication range and increase the robustness of communication, and how the IEEE Std 1588 precision time protocol (PTP) works over wavelet networks is specified to enhance network functions.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE 1918.1-2024	https://standards.ieee.org/ieee/1918.1/6721/	This standard defines a framework for the Tactile Internet, including descriptions of various application scenarios, definitions and terminology, functions, and technical assumptions. This framework prominently also includes a reference model and architecture, which defines common architectural entities, interfaces between those entities, and the mapping of functions to those entities. The Tactile Internet encompasses mission critical applications (e.g., manufacturing, transportation, healthcare and mobility), as well as non-critical applications (e.g., edutainment and events).	S2.3, S2. 25.9, S2.25.15
IEEE	(NEW) IEEE/ UL 2933-2024	https://standards.ieee.org/ieee/2933/7592/	A framework with TIPPSS principles (trust, identity, privacy, protection, safety, and security) for Clinical Internet of Things (IoT) data and device interoperability is established in this standard. This includes wearable clinical IoT and interoperability with healthcare systems including electronic health records (EHR), electronic medical records (EMR), other Clinical IoT devices, in-hospital devices, and future devices and connected healthcare systems.	S2.10, S2.7
IEEE	(NEW) IEEE P2418.3	https://standards.ieee.org/ieee/2418.3/7714/	This standard provides a common framework for distributed ledger technology (DLT) usage, implementation, and interaction in agriculture. The framework maps DLT terms including transactions, smart contracts, tokens, assets and networks to terms in agriculture, and addresses technical aspects including scalability, security and privacy challenges with regard to DLT in agriculture. Concerns from different stakeholders and requirements in horizontal and vertical categories of agriculture are included in the framework.	S2.6, S2.10,

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE P2992	https://standards.ieee.org/ieee/2992/10614/	This standard defines recommended practices for designing smart agriculture data focusing on the data format, data tags, their naming rules, and data transfers to show the unified practices of data expression, exchange, and processing. This is indispensable for smart agriculture systems, such as data acquisition, data management, data service provisioning, and data processing for data security, as well as privacy from the perspective of agricultural machinery control, greenhouse management, and farming management. This recommended practice provides the co-existence and interoperability using common data structure and transfer between heterogeneous systems; namely, various systems of different manufacturers work together to achieve the farmers' requirement efficiently and effectively as for a smart agriculture system.	S2.1, S2.18
IEEE	(NEW) IEEE - P1451-99 Standard for Harmonization of Internet of Things (IoT) Devices and Systems (2024-05)	https://standards.ieee.org/ieee/1451.99/11634/	This standard utilizes the advanced capabilities of the XMPP protocol, such as providing globally authenticated identities, authorization, presence, life cycle management, interoperable communication, IoT discovery and provisioning. Descriptive meta-data about devices and operations will provide sufficient information for infrastructural components, services and end-users to dynamically adapt to a changing environment. Key components and needs of a successful Smart City infrastructure will be identified and addressed. This standard does not develop Application Programming Interfaces (APIs) for existing IoT or legacy protocols.	S2.1, S2.6, S2.18
IEEE	(NEW) IEEE 802.11a™	https://standards.ieee.org/ieee/802.11ax/7180/	Wi-Fi 6 is designed to get better efficiency using increased throughput in 2.4, 5 and 6 GHz bands. Modifications to both the IEEE 802.11 physical layer (PHY) and medium access control (MAC) sublayer for high-efficiency operation in frequency bands between 1 GHz and 7.125 GHz are defined in this amendment to IEEE Std 802.11-2020.	S2.7, S2.25.1, S.2.25.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE (NEW) P802.11be™	https://standards.ieee.org/ieee/802.11be/7516/	Wi-Fi 7 with 4x faster data rates (~40 Gbit/s) and twice the bandwidth (320 MHz channels vs. 160 MHz channels for Wi-Fi 6). It also supports more efficient and reliable use of the available and contiguous spectrum through multi-band/multi-channel aggregation and other means. The standard features numerous enhancements to MIMO protocols and many other advancements and refinements of existing Wi-Fi capabilities. The capabilities match the requirements for AR/VR and verses applications. IEEE 802.11-based Wi-Fi networks carry an extensive and growing amount of data, making it possible to leverage new AI/ML algorithms, such as federated learning, to improve Wi-Fi performance and user experiences. The IEEE 802.11 Extremely High Throughput Study Group has been established to explore new IEEE 802.11 features for bands between 1 and 7.125 GHz that would increase peak throughput to support these demanding applications.	S.2.3, S2.7, S2.25.1, S2.25.5, S2.25.10
6IEEE	(NEW) IEEE 2888.1-2023	https://standards.ieee.org/ieee/2888.1/7676/	IEEE Standard for Specification of Sensor Interface for Cyber and Physical Worlds: The vocabulary, data formats, and application programming interfaces (APIs) for acquiring information from sensors are defined in this standard, enabling communication between the cyber world and the physical world.	S2.1, S2.10, S2.25.1, S2.25.2, S2.25.3, S2.25.4, S2.25.9, S2.25.10
IEEE	(NEW) IEEE 2888.2-2023	https://standards.ieee.org/ieee/2888.2/10469/	IEEE Standard for Actuator Interface for Cyber and Physical Worlds: The vocabulary, data formats, and application programming interfaces (APIs) for controlling the actuators, which helps enable the definition of interfaces between the cyber world and the physical world, are defined in this standard.	S2.1, S2.18, S2.25.1, S2.25.2, S2.25.3, S2.25.4, S2.25.5, S2.25.9, S2.25.10
IEEE	(NEW) IEEE P2888.3	https://standards.ieee.org/ieee/2888.3/10470/	Standard on Orchestration of Digital Synchronization between Cyber and Physical Worlds: This standard defines the vocabulary, requirements, metrics, data formats and application program interfaces (APIs) for setting up parameters for and communicating with digital objects to provide sequences of synchronization and interaction with physical objects.	S2.6, S2.10, S2.25.1, S2.25.2, S2.25.4, S2.25.9, S2.25.10
IEEE	(NEW) IEEE 2888.4-2023	https://standards.ieee.org/ieee/2888.4/10471/	IEEE Standard for Architecture for Virtual Reality Disaster Response Training System with Six Degrees of Freedom (6 DoF). Defined in this standard is a reference architecture required for building a virtual reality (VR) training system for large space disaster response.	S2.7, S2.25.3, S2.25.5, S2.25.9, S2.25.10, S2.25.12

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE P2888.5	https://standards.ieee.org/ieee/2888.5/10787/	IEEE Draft Standard for Virtual Training System Evaluation Methods. This standard defines the evaluation methods and frameworks for virtual training systems. The evaluation framework consists of a plan, design, data, test, and analysis that can evaluate the virtual training systems' effectiveness, usability, and acceptability.	S2.14, S2.25.3, S2.25.5, S2.25.9, S2.25.10, S2.25.12
IEEE	(NEW) IEEE P2888.6	https://standards.ieee.org/ieee/2888.6/10788/	Standard for Holographic Visualization for Interfacing Cyber and Physical Worlds. This standard defines representations of holographic content to provide interfaces between Cyber and Physical Worlds for objects, which may exist either in Cyber or Physical Worlds. This includes following formats and scheme: Holographic printing file format, Holographic contents, etc.	S2.25.2, S2.25.3, S2.25.4, S2.25.10
IEEE	(NEW) IEEE 1589-2020	https://standards.ieee.org/ieee/1589/6073/	IEEE Standard for Augmented Reality Learning Experience Model. Defines two data models and their binding to XML and JSON for representing learning activities (also known as employee tasks and procedures) and the learning environment in which these tasks are performed (also known as the workplace). The interoperability specification and standard are presented in support of an open market where interchangeable component products provide alternatives to monolithic AR-assisted learning systems. Moreover, it facilitates the creation of experience repositories and online marketplaces for AR-enabled learning content.	S2.20, S2.25.9, S2.25.10, S2.25.14
IEEE	(NEW) IEEE P7016.1	https://standards.ieee.org/ieee/7016.1/11237/	Standard for Ethically Aligned Educational Metadata in Extended Reality (XR) & Metaverse. defines a high-level overview of a conceptual data schema for a metadata instance based on ethics concepts for a learning object utilized within XR systems and Metaverse applications. This standard does not aim to define whether procedures and operations as presented through the Metaverse are ethical or not. This standard does not involve evaluation of the ethical value of learning content objects. Use case examples of the conceptual data schema are defined. This standard also describes a high-level ethical design methodology of learning objects for XR and the Metaverse applications, using the IEEE Std 7000 applied ethical approach.	S2.10, S2.19, S.25.2, S2.25.3, S2.25.10, S2.25.14,

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE IC15-004-01	https://standards.ieee.org/wp-content/uploads/import/governance/iccom/3DBP-An_Introduction.pdf	3D Body Processing: This initiative was launched in the first quarter of 2016 with an initial focus on exploring technology standardization opportunities for hardware and software technologies across the "3D body processing" pipeline; i.e., from scanning of people and creating body model data to simulating, modeling, analytics, and visualization. A Virtual Fit use case and relevant 3DBP attributes are examined as an example of a 3D body processing use case. File formats, metadata, and communication protocols are discussed and initial guidance is proposed for evaluating and selecting among existing formats and protocols. While the white paper utilizes examples from an apparel/retail context, it is important to note that the direction taken by the 3DBP initiative is applicable to use cases in other industries such as health, wellness, fitness and athletics as well as complementary to adjacent technology ecosystems such as IOT, 5G, AI, fog, and cloud computing.	S2.10, S2.25.10, S2.25.15, S2.25.16
IEEE	(NEW) IEEE IC16-004-02	https://standards.ieee.org/wp-content/uploads/import/governance/iccom/IC16-004-02_Augmented_Reality_in_the_Oil_Gas_Electric_Industry.pdf	Augmented Reality in the Oil/Gas/Electric Industry: IEEE hosted a workshop in October 2015, exploring the application of augmented reality (AR) solutions in the oil and gas industry. Coupled with interest within the electric power industry, workshop participants expressed an interest in forming an ongoing interest group to facilitate collaboration in identifying requirements, standards needs and other issues, to help enable AR solutions, as well as potentially mixed and virtual reality solutions, that can benefit these industries. Existing augmented reality devices have not yet achieved a state of readiness for widespread application in the oil, gas, and electric industries. "Heads up Display" type devices are of particular interest, however a variety of issues need to be overcome including ruggedness, wireless connectivity, use case viability and human factors considerations. While each of the represented industries have some industry-specific interests, there are sufficient commonalities such that aggregating efforts is anticipated to provide a beneficial approach to achieving efficient solutions.	S2.25.10, S2.25.15, S2.25.16

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			Both hardware and software issues can be largely influenced by standards. Participants in this activity will identify existing standards, and standards in progress that are relevant and valuable to supporting AR in the electric/oil/gas industries, as well as identifying gaps where new standards efforts are recommended – analysis will include not only IEEE standards, but standards and specification available via other SDOs, alliances, etc. Use Cases will also be an area of work activity – development of a collection of use cases that are 1) of mutual interest across electric/oil/gas, 2) of segment specific interest. Prioritize use cases and identify applicable standards and gaps in existing standards.	
IEEE	(NEW) IEEE IC16-005-02	https://ieee-sa.imeetcentral.com/p/eAAAAAAAIPLYAAAAAEUAYuI	Consumer Healthcare Alliance: Consumer Healthcare Alliance (CHA) is a community of global industry and academic leaders dedicated to improve consumers'daily health life with innovations in healthcare electronics. As technology advanced in the past years, more and more healthcare electronics has been developed and shipped directly to consumers. Itis important that this trend be standardized, documented and systematically improved with cooperation among industry and academic leaders in the area.	S2.25.10, S2.25.15, S2.25.16
IEEE	(NEW) IEEE P2048	https://standards.ieee.org/ieee/2048/11169/	Standard for Metaverse: Terminology, Definitions, and Taxonomy. This is the most relevant of the projects (P) that started on the Metaverse in IEEE. IEEE P2048 has the charter to create a common understanding in the international ecosystem on categories and levels of what will be called Metaverse. The work started in 2023 and is supposed to be completed by 2026.	S2.25.10
IEEE	(NEW) IEEE 2048.101-2023	https://standards.ieee.org/ieee/2048.101/10390/	IEEE Standard for Augmented Reality on Mobile Devices--General Requirements for Software Framework, Components, and Integration: This standard specifies the general technical framework, components, integration, and main business processes of augmented reality systems applied to mobile devices, and defines its technical requirements, including functional requirements, performance requirements and the corresponding test methods. The target applications and services include but are not limited to the design, development, and management of augmented reality and mixed reality enabled applications or features of applications on mobile devices.	S2.7, S2.25.1, S2.25.8, S2.25.9, S2.25.10, S2.25.13

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE P2048.111	https://standards.ieee.org/ieee/2048.111/11598/	Standard for Technical Specification for Three-dimensional (3D) Reconstruction and Visual Localization for Large-Scale Scenes: This standard specifies a structure of a large-scale scene (indoor or outdoor scenes with an area of more than 300 m^2), oriented 3D reconstruction and visual localization system, the functional requirements, and basic performance requirements and test methods.	S2.7, S2.25.8, S2.25.9, S2.25.10, S2.25.13
IEEE	(NEW) IEEE P 2048.121	https://standards.ieee.org/ieee/2048.121/11599/	Standard for General Technical Requirements for Service-oriented Digital Human Based on Artificial Intelligence: This standard specifies a reference framework and requirements for the functionality and performance of service-oriented digital humans based on artificial intelligence (AI). This standard provides guidance for design, development, testing, application, and management of service-oriented digital human based on AI.	S2.15, S2.25.4, S2.25.5, S2.25.8, S2.25.9, S2.25.10
IEEE	(NEW) IEEE P2048.201	https://standards.ieee.org/ieee/2048.201/11600/	Standard for Security Specification of Blockchain-based Metaverse Accounts: This standard specifies the security requirements for consumer's personal accounts and public accounts of blockchain-based Metaverse technology, including general account requirements, basic security requirements, and service security requirements.	S.2.6, S.2.25.6, S2.25.11
IEEE	(NEW) IEEE P2048.202	https://standards.ieee.org/ieee/2048.202/11673/	Standard for Security Specifications of Blockchain-Based Metaverse Data: This standard specifies consumer's data security requirements in the blockchain-based metaverse, including data transmission, data storage, data migration, data sharing, data backup and recovery, and data destruction. Thereby, the standard helps to protect the integrity and authenticity of transactions as well as consumers' personal privacy information, such as identity information, and payment passwords. Furthermore, encryption technology specified in this standard can enable that consumer data is not illegally obtained or tampered with during transmission and storage.	S2.6, S.2.25.6, S2.25.11

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	(NEW) IEEE P2874	https://standards.ieee.org/ieee/2874/11717/	Standard for Spatial Web Protocol, Architecture and Governance. This standard describes a Hyperspace Transaction Protocol (HSTP) that enables interoperable, semantically compatible connections between connected hardware (e.g. autonomous drones, sensors, smart devices, robots) and software (e.g. services, platforms, applications, artificial intelligence systems). The Spatial Web Protocol, Architecture and Governance specification defines requirements for the interoperability and governance of cyber-physical systems at a global scale, including autonomous devices, applications, spatial content, and operations. The full specification is developed by the Spatial Web Foundation and the IEEE P2874 Spatial Web, Architecture and Governance Working Group. The system design includes: a shared and linkable knowledge domain architecture ("Architecture"); a common language with which to describe domain elements and their interrelationships – HSML; a method for querying and updating the states of those elements ("Protocol") – HSTP; the ability to allow access and control of that method ("Governance"), and a Universal Domain Graph. Collectively these elements are the Spatial Web Standards ("Standards").	S2.1, S2.7, S2.10, S2.25.1, S2.25.2, S2.25.3, S2.25.4. S2.25.5, S2.25.8, S2.25.10, S2.25.15, S2.25.16
IEEE	(NEW) IEEE 3079-2020	https://standards.ieee.org/ieee/3079/7283/	IEEE Standard for Head-Mounted Display (HMD)-Based Virtual Reality (VR) Sickness Reduction Technology: Defines the technical requirements that can reduce or control the VR sickness caused by the HMD-based VR content service. The VR content service mentioned in this document is considered HMD-based VR content service by default unless otherwise mentioned. The requirements cover the followings: Content design for VR sickness reduction - The framework for VR sickness assessment; The measurement and the network requirements related to motion-to-photon latency for VR sickness reduction.	S2.25.1, S2.25.2, S2.25.4, S2.25.8, S2.25.13, S2.25.15
IEEE	(NEW) IEEE P3141	https://standards.ieee.org/ieee/IEEE_SA_White_Paper/10667/	Standard for 3D Body Processing: This standard addresses the anthropometric and topo-physiological attributes that contribute to the quality of experience of 3D body processing, as well as identifying and analysing metrics and other useful information, as well as data relating to these attributes.	S2.10, S2.25.2, S2.25.3, S2.25.4, S2.25.10, S2.25.14, S2.25.15, S2.25.16

Table 9: AIOTI/EUOS indentified IoT challenges covered/addressed by ITU-T

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T L.1370 (11/2018)	https://handle.itu.int/11.1002/1000/13724	This recommendation sets out the services and data required for a sustainable and intelligent building to improve the quality of life of citizens, as well as the specification of its functional features and the technical requirements to be met by the device that provides these services and data.	S2.8 , S2.24
ITU-T	ITU-T G.9959	https://www.itu.int/rec/T-REC-G.9959-201501-I/en	Recommendation ITU-T G.9959 specifies the physical (PHY), medium access control (MAC), segmentation and reassembly (SAR), and logical link control (LLC) layers for short range narrow-band digital radiocommunication transceivers (TRXs). This Recommendation contains the non-radio (frequency) related aspects of the radiocommunication TRX. Sub 1 GHz TRXs claiming compliance with this specification shall also comply with Annex A of this Recommendation.	
ITU-T	ITU-T Q.4060 (10/2018)	https://handle.itu.int/11.1002/1000/13700	This recommendation describes the testing methodology of the heterogeneous network gateway, which is to be used for communication among IoT devices. The tests will include the following, but not limited to: a) checking the gateway to verify stress load (benchmarking); b) checking the gateway to determine the possibility for the transmission of various types and sizes of frames and (or) packages; c) verifying joint conversions from different protocols and multiple interfaces; d) checking the gateway operation settings (CPU, RAM, etc.); and e) checking the network parameters (delay, data loss, etc.).	S2.9
ITU-T	ITU-T Y.4117 (10/2017)	https://handle.itu.int/11.1002/1000/13386	The scope of this recommendation includes: a) description of characteristics of WD and WDS; b) specific requirements of the IoT for support of WD and WDS; c) specific capabilities of the IoT for support of WD and WDS; d) Information concerning use cases for WD and WDS.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4411/Q.3052 (02/2016)	https://handle.itu.int/11.1002/1000/12698	This recommendation provides an overview of APIs and protocols for the M2M service layer and the related API and protocol requirements. It describes the component based M2M reference model, including the reference points of the M2M service layer. Then, APIs and protocols for M2M are introduced, including existing APIs and protocols for M2M service layer and M2M protocol structure and stacks. Finally, API and protocol requirements with respect to the M2M service layer are analysed.	S2.2
ITU-T	ITU-T Y.4418 (06/2018)	https://handle.itu.int/11.1002/1000/13640	This recommendation provides the gateway functional architecture for Internet of things (IoT) applications. The scope of this recommendation also includes: a) the gateway functional entities for IoT applications; b) the gateway reference points for IoT applications; c) typical logical flows.	S2.5
ITU-T	ITU-T Y.4451 (09/2016)	https://handle.itu.int/11.1002/1000/13026	The scope of this recommendation includes the following items: a) An overview of constrained node device networking in the IoT environments; b) Communication of constrained node devices; c) Architectures of constrained node device networking; d) Functionalities of constrained node device networking.	S2.5
ITU-T	ITU-T H.560 (12/2017)	https://handle.itu.int/11.1002/1000/13435	This recommendation defines the requirements for vehicle gateway platform (VGP) services, VGP service functionalities and VGP management. The VGP service functions support service capabilities for applications running and data/message processing. The VGP service functionalities support core capabilities used by VGP services such as session management or in-vehicle resource access management. Finally, the VGP management supports functions for VGP configuration and monitoring such as security management. This Recommendation also defines the network requirements for communication interfaces used between the defined VGP services and external applications. These external applications could be running over nomadic devices brought into the vehicle, roadside infrastructure, or cloud-based servers. Applications downloaded to one of the in-vehicle devices after the time of manufacture are also considered external applications since they may not be fully integrated into the driver-vehicle interface (DVI) and require a communications interface.	S2.5, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4466 (01/2020)	https://handle.itu.int/11.1002/1000/14169	This recommendation describes the reference architecture for the smart greenhouse service which provides and maintains optimal conditions for growing crops in greenhouse environment. The scope covered by the framework of smart greenhouse service includes the following issues: a) Overview of the smart green-house service; b) Reference architecture for smart greenhouse service; c) Interfaces for smart greenhouse service; d) Use Cases of smart greenhouse service.	S2.8, S2.14, S2.24
ITU-T	ITU-T Y.4208	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14162	Some of the capabilities offered by the Internet of thing (IoT), e.g., capabilities for computing, storage and analytics, are evolving in closer proximity to IoT data sources. Recommendation ITU-T Y.4208 provides an overview of related challeng-es faced by the IoT and describes how IoT-supporting edge computing (EC) may address these challenges. From the edge-computing deployment perspective, service requirements for support of EC capabilities in the IoT are identified, as well as related functional requirements. As an example, scenarios of EC deployment in different application domains, EC scenar-ios for vehicle-to-everything (V2X) and for smart manufacturing are provided in an appendix.	S2.7
ITU-T	ITU-T Q.3952 (01/2018)	https://handle.itu.int/11.1002/1000/13489	The testing of IoT technologies requires the specific model network which can simu-late different scenarios of IoT implemen-tations. This recommendation describes the architecture and facilities of Model Network for IoT testing.	S2.9
ITU-T	ITU-T Q.4062 (09/2020)	https://handle.itu.int/11.1002/1000/14387	The main goal of this recommendation is the testing framework for Internet of Things definition. Conformity, interoper-ability and benchmarking testing frame-works for IoT are the recommendation scope.	S2.9
ITU-T	ITU-T Q.4063 (09/2020)	https://handle.itu.int/11.1002/1000/14391	The recommendation provides a de-scription and test suites of identification procedures used in Internet of Things (IoT). There are a lot of applications of Internet of Things, the testing of their identity might be considered as a very important issue as it allows customer to ensure the authen-ticity of the IoT. The classification of IoT, in terms of testing of their identification pro-cedures and the relevant testing approach-es are subjects of this Recommendation.	S2.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4001/F.748.2 (11/2015)	https://handle.itu.int/11.1002/1000/12621	This recommendation covers the following: a) overview of machine socialization; b) requirements for machine socialization; and c) reference models of machine socialization including service model, functional model and architectural model.	S2.14
ITU-T	ITU-T Y.4002/F.748.3 (11/2015)	https://handle.itu.int/11.1002/1000/12622	This recommendation covers the following: a) relation management models for machine socialization; b) relation descriptions for machine socialization; and c) use cases for relation management models.	S2.14
ITU-T	ITU-T Y.4100/Y.2066 (06/2014)	https://handle.itu.int/11.1002/1000/12169	This recommendation provides the common requirements of the Internet of things (IoT). These requirements are based on general use cases of the IoT and IoT actors, which are built from the definition of IoT contained in Recommendation ITU-T Y.2060. The common requirements of the IoT are independent of any specific application domain, which refer to the areas of knowledge or activity applied for one specific economic, commercial, social or administrative scope, such as transport application domain and health application domain. This recommendation builds on the overview of IoT (Recommendation ITU-T Y.2060), developing the common requirements based on general use cases of the IoT and the IoT actors and taking into account important areas of consideration from a requirement perspective. Some representative use cases of the IoT, which are abstracted from application domains, are also provided. The common requirements of the IoT specified in this Recommendation are classified into the categories of non-functional requirements, application support requirements, service requirements, communication requirements, device requirements, data management requirements and security and privacy protection requirements.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4101/Y.2067	https://handle.itu.int/11.1002/1000/13384	This Recommendation provides the common requirements and capabilities of a gateway for Internet of things (IoT) applications. The common requirements and capabilities provided are intended to be generally applicable in gateway application scenarios. The scope of this Recommendation includes: - general characteristics of a gateway for IoT applications; - common requirements of a gateway for IoT applications; - common capabilities of a gateway for IoT applications. - Use cases of a gateway for IoT applications are provided in appendices.	
ITU-T	ITU-T Y.4102/Y.2074 (01/2015)	https://handle.itu.int/11.1002/1000/12421	This recommendation provides requirements for IoT devices that can be used for operation of IoT applications in the context of disaster in addition to the common requirements of IoT [ITU-T Y.2066]. It also provides special requirements for operation of IoT applications during disaster. The scope of this Recommendation includes: a) requirements for IoT devices in the context of disaster; b) requirements for operation of IoT applications during disaster (for each of the three identified operating strategies). This Recommendation is relevant for IoT application developers and IoT service providers as well as for emergency service providers.	S2.5
ITU-T	ITU-T Y.4111/Y.2076 (02/2016)	https://handle.itu.int/11.1002/1000/12705	This recommendation specifies semantic related requirements and framework of the Internet of Things (IoT). Taking into consideration the IoT reference model [ITU-T Y.2060], semantic requirements including those related to the four layers (i.e. Application layer, SSAS layer, Network layer and Device layer) and the management and security capabilities [ITU-T Y.2060], as well as semantic requirements across layers are specified. Based on the identified IoT semantic requirements and existing semantic related technologies, the IoT semantic framework is specified. The scope of this recommendation includes: a) Introduction to semantic related technologies; b) IoT semantic requirements; c) IoT semantic framework.	S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4115 (04/2017)	https://handle.itu.int/11.1002/1000/13266	This recommendation specifies the reference architecture for IoT device capabilities exposure. The scope of this recommendation includes: a) the concept, general characteristics and requirements of IoT device capability exposure; b) the reference architecture for IoT device capability exposure including common procedures.	S2.2
ITU-T	ITU-T Y.4118 (06/2018)	https://handle.itu.int/11.1002/1000/13496	This recommendation provides accounting and charging requirements for Internet of things (IoT). Building on the requirements and framework for accounting and charging capabilities in the next generation network (NGN) [ITU-T Y.2233], this Recommendation provides specific requirements derived from the analysis of business use cases specific to the IoT. Based on the identified requirements, an IoT accounting and charging technical capability framework is then specified. The scope of this Recommendation includes: a) business use cases applied to the IoT; b) IoT accounting and charging requirements; c) IoT accounting and charging technical capability framework.	S2.4
ITU-T	ITU-T Y.4121 (06/2018)	https://handle.itu.int/11.1002/1000/13636	This recommendation describes requirements of an Internet of things (IoT) enabled network for support of applications monitoring and studying global processes of the Earth. This concept of "Internet of things for monitoring and studying global processes (IoT GP)" combines geographically distributed IoT devices, and one or more control and management centres (CMCs) for the monitoring of global natural and man-made processes. This Recommendation describes key IoT GP features, deployment schemes of IoT GP devices, and requirements of the IoT GP network.	
ITU-T	ITU-T Y.4203 (02/2019)	https://handle.itu.int/11.1002/1000/13857	The goal of this recommendation is to specify requirements for an effective way of representing things as far as possible in a homogeneous way. The focus of the document is on the following two concerns of things description: a) Representing physical things as virtual things to map the physical things into information world; b) Representing the relationship of virtual things to reflect the relationship of the represented physical things.	S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4206 (06/2019)	https://handle.itu.int/11.1002/1000/13919	The objective of this recommendation is to identify requirements and capabilities of user-centric work space (UCS) service. In particular, the scope of this recommendation includes: a) Requirements of UCS service; b) Capability framework of UCS service; and c) Workflow of UCS service.	S2.14
ITU-T	ITU-T Y.4401/Y.2068 (03/2015)	https://handle.itu.int/11.1002/1000/12419	This recommendation provides the functional framework and associated capabilities of Internet of Things (IoT), in particular components of the functional framework, their capabilities, and the relationships among these components. The recommendation also describes the relationships between the IoT requirements specified in [ITU-T Y.IoT-common-reqts] and the capabilities specified in this Recommendation. Finally, the recommendation provides security considerations for the IoT functional framework.	S2.6
ITU-T	ITU-T Y.4412/F.747.8 (11/2015)	https://handle.itu.int/11.1002/1000/12620	This recommendation defines requirements and reference architecture for audience-selectable media (ASM) service in the IoT environment. The scope of this recommendation includes: a) Concept of ASM service framework; b) - Requirements of ASM service framework; c) Reference architecture of ASM service framework; and, d) Functional entities of ASM service framework.	
ITU-T	ITU-T Y.4413/F.748.5 (11/2015)	https://handle.itu.int/11.1002/1000/12623	The objective of this recommendation is to identify requirements of the M2M service layer, which are common to all M2M verticals or specific to e-health application support, and to provide an architectural framework of the M2M service layer. In particular, the scope of this recommendation includes: a) Definition of the M2M service layer; b) Requirements of the M2M service layer; c) Architectural framework of the M2M service layer; d) Reference points of the M2M service layer.	S2.7
ITU-T	ITU-T Y.4415 (06/2018)	https://handle.itu.int/11.1002/1000/13637	This recommendation describes an architecture of a Web of Objects (WoO) based virtual home network (WVHN) by identifying the following: a) overview of WVHN; b) WVHN objects processing functions; c) WVHN service functions; d) security and trust support of WVHN.	S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4416	https://handle.itu.int/11.1002/1000/13638	This Recommendation describes an architecture of the Internet of things (IoT) based on extensions and enhancement to next generation network evolution (NGNe) functional entities, reference points and components as described in [ITU-T Y.2012], and other related Recommendations. The Recommendation takes into account the IoT reference model specified in [ITU-T Y.4000], the IoT common requirements specified in [ITU-T Y.4100], and the IoT functional framework and capabilities specified in [ITU-T Y.4401]. The scope of this Recommendation includes: - the extension to NGNe functional entities to support the IoT; - the extension of NGNe reference points to support the IoT; - the extension of NGNe components to support the IoT; - the enhancement to NGNe capabilities to support the IoT. Security of the extensions and enhancement specified in this Recommendation is also considered.	S2.6
ITU-T	ITU-T Y.4417 (06/2018)	https://handle.itu.int/11.1002/1000/13639	The scope of this recommendation includes: a) concept of self-organization network in the Internet of Things (IoT) environments; b) characteristics of self-organization network in the IoT environments; c) requirements for self-organization networking in IoT; d) functional architecture for self-organization networking in IoT.	S2.13
ITU-T	ITU-T Y.4452 (09/2016)	https://handle.itu.int/11.1002/1000/13027	This recommendation provides application support models of the Internet of Things (IoT). It includes the basis of IoT application support models; the configurable application support model, the adaptable application support model and the reliable application support model. The three application support models are described in functional view, implementation view and deployment view, in order to identify, respectively, the configurable capabilities, the adaptable capabilities and the reliable capabilities for support of IoT applications having some characteristic requirements.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4453	https://handle.itu.int/11.1002/1000/13028	This Recommendation describes the high-level requirements and functional architecture of the adaptive software framework (ASF) for Internet of things (IoT) devices.. In particular, the scope of this Recommendation includes: - an overview of the ASF, - features and high-level requirements of the ASF: monitoring capability, policy decision capability and management capability; - functional architecture of the ASF: application monitoring manager function, system information manager function and policy manager function.	
ITU-T	ITU-T Y.4553	https://handle.itu.int/11.1002/1000/12779	This Recommendation specifies the common requirements of using the smartphone as sink node for IoT applications and services, while the smartphone could provide the functions of both end-user terminal as well as the mobile gateway to connect the mobile network and the sensor network. More specifically, this recommendation covers the followings: - Concept of IoT sink node of the IoT - Sensing mode of the smartphone work as sink node for IoT applications and services - Requirements of using smartphone as sink node for IoT applications and services	S2.5
ITU-T	ITU-T Y.4702 (03/2016)	https://handle.itu.int/11.1002/1000/12780	This recommendation studies the requirements and capabilities of device management in IoT. The scope of this recommendation includes: a) the requirements of device management in IoT; b) the reference technical framework of device management in IoT; c) the capabilities of device management in IoT.	S2.23
ITU-T	ITU-T Y.4801/F.748.1 (10/2014)	https://handle.itu.int/11.1002/1000/12229	The objective of this Recommendation is to analyse identifiers in existing technologies and networks for IoT service, and describe the requirements of IoT identifier, common characteristics of IoT identifier, and the general architecture of IoT identifier. This Recommendation describes the requirements and common characteristics of IoT identifier for IoT service. The scope of this Recommendation includes: - Analysis of identifiers in existing technologies and networks - Describe requirements of IoT identifier - Describe common characteristics of IoT identifier - Describe the general architecture of IoT identifier	S2.17

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4201 (02/2018)	https://handle.itu.int/11.1002/1000/13388	This recommendation presents the high-level requirements and reference framework of Smart City Platform (SCP). The SCP is a fundamental platform supporting all the services and applications of a smart city, with the objective to improve quality of life, provide urban operation and services for the benefit of the citizens while ensuring city sustainability. These high-level requirements include comprehensive and updated repositories of city information, infrastructure life-cycle management, inter-system communication, security support, maintenance support, controls of processer, decision making support, real-time dissemination of public information, resiliency, and interoperability.	
ITU-T	ITU-T Y.4461 (01/2020)	https://handle.itu.int/11.1002/1000/14164	This recommendation defines a conceptual model of Open Data in Smart Cities, in order to establish and foster a common understanding of Open Data in Smart Cities. The scope of this Recommendation includes: a) definition of Open Data in Smart Cities; b) benefits of Open Data in Smart Cities; c) fundamental requirements of Open Data in Smart Cities; d) conceptual model of Open Data in Smart Cities.	S2.1
ITU-T	ITU-T Y Suppl. 27 (01/2016)	https://handle.itu.int/11.1002/1000/12753	The scope of this standardization work is to describe the ICT architecture development framework of SSC and provide corresponding architecture views and guides with the key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but is not limited to: a) ICT Architecture development methodology; b) SSC ICT Architecture development methodology; c) SSC ICT architecture framework; d) Guidelines for the SSC ICT architecture; e) SSC ICT Architecture interfaces.	S2.8

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y Suppl. 28 (01/2016)	https://handle.itu.int/11.1002/1000/12754	The scope of this standardization work is to provide a technical proposal for integrated management, which can be followed by any municipality interested in improving the management of its infrastructure, operations and citizen interactions, and in addressing critical urban challenges – such as security, criminality, pollution, traffic congestion, inadequate infrastructure, and response to natural hazards. Specifically, the proposed new Supplement covers, but is not limited to: a) Resources, challenges and technologies of integrated management for smart sustainable cities; b) Integrated management for smart sustainable cities; c) Service framework.	S2.8
ITU-T	ITU-T Y Suppl. 29 (01/2016)	https://handle.itu.int/11.1002/1000/12755	The scope of this standardization work is to describe the various infrastructures for a smart sustainable city in a new-development area with a key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but is not limited to: a) Smart Sustainable Building Utility Services; b) SSC (Smart Sustainable Cities) Utility Service Requirements; c) Opportunities for sharing infrastructure at street level.	S2.8
ITU-T	ITU-T Y Suppl. 30 (01/2016)	https://handle.itu.int/11.1002/1000/12756	The scope of this standardization work is to provide a technical overview on infrastructure related to information and communications technology (ICT), specific to developing smart sustainable cities (SSC) with the key objective of highlighting this promising and game-changing area for future IoT standardization. Specifically, the proposed new Supplement will cover, but not limited to: a) SSC stakeholders; b) ICT infrastructure for SSC; c) Physical infrastructure and its intelligent upgrading; d) Planning deployment of ICT infrastructure for SSC; e) Example of open access network for smart cities; f) Strategies for the deployment of digital/ICT infrastructure.	S2.8
ITU-T	ITU-T L.1221 (11/2018)	https://handle.itu.int/11.1002/1000/13721	This recommendation contains the main requirements for evaluating appropriate innovative batteries for stationary use for powering ICT equipment in telecom sites, active network units and data centres or customer premises with standardized power interfaces in –48V, up to 400 VDC or 12V.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T L.1222 (05/2018)	https://handle.itu.int/11.1002/1000/13579	This recommendation provides an overview of available supercapacitor (SC) technology, with details of SC characteristics (electrical, mechanical, thermal) and applicability in the telecommunication/information and communication technology (TLC/ICT) domain.	S2.8, S2.24
ITU-T	ITU-T H.831 (01/2015)	https://handle.itu.int/11.1002/1000/12249	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T H.832 (01/2015)	https://handle.itu.int/11.1002/1000/12250	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T H.833 (01/2015)	https://handle.itu.int/11.1002/1000/12251	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T H.834 (01/2015)	https://handle.itu.int/11.1002/1000/12252	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T H.835 (01/2015)	https://handle.itu.int/11.1002/1000/12253	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T H.836 (01/2015)	https://handle.itu.int/11.1002/1000/12254	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T H.837 (01/2015)	https://handle.itu.int/11.1002/1000/12255	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for WAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21
ITU-T	ITU-T Y.4112/Y.2077 (02/2016)	https://handle.itu.int/11.1002/1000/12706	The document specifies the common requirements for the plug and play capability of the IoT. More specifically, this recommendation covers the followings: a) Concept and scope of plug and play capability of the IoT; b) Plug and play use cases of the IoT; c) Functional requirements for the plug and play capability of the IoT; d) System requirements for the plug and play capability of the IoT.	S2.12 , S2.22
ITU-T	ITU-T Y.4113 (09/2016)	https://handle.itu.int/11.1002/1000/13025	This recommendation describes the requirements of the network for the Internet of things (IoT). The common requirements of the IoT described in [ITU-T Y.4100] are high-level; thus this Recommendation is complementary to [ITU-T Y.4100] in term of specific requirements of the network for the IoT.	
ITU-T	ITU-T F.749.1 (11/2015)	https://handle.itu.int/11.1002/1000/12631	This recommendation specifies functional requirements for vehicle gateway (VG), including transport functional requirements, networking functional requirements, network access functional requirements, communication-with-in-vehicle devices functional requirements, and network access management & security functional requirements. It also describes communications interfaces to support the seamless wired and wireless connectivity in the heterogeneous access network environments.	S2.6, S2.7
ITU-T	ITU-T F.749.2 (03/2017)	https://handle.itu.int/11.1002/1000/13183	This recommendation provides the service description, application scenarios and requirements for Vehicle Gateway Platforms. A series of Recommendations for Vehicle Gateway Platforms is currently opened in ITU- T SG 16. This recommendation is part of that series and gives the service description, application scenarios and requirements.	S2.5, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T Y.4805 (08/2017)	https://handle.itu.int/11.1002/1000/13267	This recommendation specifies a set of requirements for identifier services in smart city applications with a view to ensure that such systems are interoperable and secure. This set of requirements may additionally serve as guidelines for developing new identifier services for smart city. It includes security features for service integrity, data confidentiality. The recommendation defines a full list of identifier service requirement, including security requirements, for the identifier service.	S2.6, S2.10, S2.17
ITU-T	ITU-T H.821 (04/2017)	https://handle.itu.int/11.1002/1000/13200	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for HRN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices by HRN Interface to transfer patient information from a Continua WAN device (HRN Sender) to an Electronic Health Record device (HRN Receiver). This document only focuses on the TSS&TP for HRN Sender because, at this moment, HRN Receiver is out of the scope of Continua Certification Program.	S2.21
ITU-T	ITU-T H.841 (08/2020)	https://handle.itu.int/11.1002/1000/14344	This recommendationprovides a test suite structure (TSS) and the test purposes (TP) for personal health devices using the IEEE 11073-20601 optimized exchange protocol in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITU-T H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.	S2.21
ITU-T	ITU-T H.843 (08/2018)	https://handle.itu.int/11.1002/1000/13680	The scope of this document is to provide Test Suite Structure and Test Purposes (TSS & TP) for PAN/LAN Interface based on the requirements defined in Continua Specifications. The objective of this test specification is to provide a high probability of air interface interoperability between different devices.	S2.21

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	X.1303 bis	https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/T-REC-X.1303bis-201403-.pdf	The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.	
ITU-T	ITU-T Y.4116	https://handle.itu.int/11.1002/1000/13385	This Recommendation addresses requirements for providing transportation safety services based on Internet of things (IoT) technologies. These requirements are applicable to various means of transportation, e.g., road, railway, maritime and air. In this Recommendation, the concepts of transportation safety management according to the processing phases of IoT sensing data and the IoT sensing data necessary for safety management are introduced. An example of a decision-making hierarchy for transportation safety is also described. The requirements for transportation safety services are described and classified according to the ITU T IoT reference model [ITU-T Y.4000]. Use cases and related service scenarios used to extract requirements for the various transportation safety services are described in Appendix I. - Appendix II shows the relationship between the requirements provided in clause 7 and the use cases described in Appendix I.	S2.3, S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ITU-T	ITU-T Y.4457 (06/2018)	https://handle.itu.int/11.1002/1000/13641	This recommendation addresses a transportation safety management model that describes disaster management steps based on Internet of things (IoT) technologies in order to reduce damage from disasters. An architectural model for transportation safety services is described based on [ITU T Y.4116] and on requirements according to the IoT reference model [ITU T Y.4000]. The scope and characteristics of transportation disasters from various transportations (e.g., road, railway, maritime and air transportation) are based on [ITU-T Y.4116]. Transportation safety management parameters (e.g., safety index and driver tiredness) are presented respectively in Annex A and Annex B and sensing data pre-processing procedure and characteristics of transportation application services are described in the appendices of this Recommendation.	S2.3, S2.7
ITU-T	ITU-T L.1383 (10/2021)	https://handle.itu.int/11.1002/1000/14719	This recommendation will focus on smart energy solutions in different applications for saving energy and reducing carbon emissions. With the development of ICT technology, smart energy solutions are not only used for ICT systems, but also in homes, remote islands, businesses, industries, and countries. The following aspects will be taken into consideration in this Recommendation: - Different energy input solutions - Electric characteristic - Safety performances - Environmental impacts - Reliability - Any other items	S2.8 , S2.24
ITU-T	ITU-T H.842 (11/2019)	https://handle.itu.int/11.1002/1000/14116	This recommendation provides a test suite structure (TSS) and the test purposes (TPs) for personal health gateways (PHGs) using the IEEE 11073-20601 optimized exchange protocol in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITUT H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.	S2.21

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T H.844 (11/2019)	https://handle.itu.int/11.1002/1000/14117	This recommendation provides a test suite structure (TSS) and the test purposes (TP) for Personal Health Gateways (PHGs) in the Personal Health Devices (PHD) interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITUT H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.	S2.21
ITU-T	ITU-T L.1371 (06/2020)	https://handle.itu.int/11.1002/1000/14304	This recommendation provides a consistent framework for owners, managers and building operators to critically assess ten (10) key areas of environmental performance and management of office buildings; Energy, Water, Air, Comfort, Health & Wellness, Purchasing, Custodial, Waste, Site, and Stakeholders.	S2.8 , S2.24
ITU-T	ITU-T L.1333 (09/2022)	https://www.itu.int/rec/T-REC-L.1333-202209-I	To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331.	S2.8 , S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	ITU-T L.1410 (12/2014)	https://www.itu.int/rec/T-REC-L.1410-201412-I/en	Recommendation ITU-T L.1410 deals with environmental life cycle assessments (LCAs) of information and communication technology (ICT) goods, networks and services. It is organized in two parts: (a) Part I: ICT life cycle assessment: framework and guidance and (b) Part II: "Comparative analysis between ICT and reference product system (Baseline scenario); framework and guidance". Part I deals with the life cycle assessment (LCA) methodology applied to ICT goods, networks and services. Part II deals with comparative analysis based on LCA results of an ICT goods, networks and services product system, and a reference product system	S2.8, S2.24
ITU-T	(Updated) ITU-T L.1480(07/2025)	https://www.itu.int/rec/T-REC-L.1480-202212-I	Recommendation ITU-T L.1480 provides a methodology for assessing how the use of information and communication technology (ICT) solutions impacts greenhouse gas (GHG) emissions of other sectors. More specifically, the methodology provides guidance on the assessment of the use of ICT solutions covering the net second order effect (i.e., the resulting second order effect after accounting for emissions due to the first order effects of the ICT solution), and the higher order effects such as rebound. By providing a structured methodological approach, it aims to improve the consistency, transparency and comprehensiveness of assessments of how the use of ICT solutions impacts GHG emissions over time. Guidance is provided to assess the net second order effect and higher order effects of the following cases: • ICT solution(s) implemented in a specific context by the user of the ICT solution(s). • ICT solution(s) implemented at different scales, including at an organizational level (whether private or public organizations), at a city level, at a country level or at worldwide level. • ICT solution(s) seen from the perspective of an ICT organization contributing to the ICT solution(s). This includes: o Assessment of the aggregated effect of all ICT solutions provided by an ICT organization across all its customers; o Assessment of the aggregated effect of one or several ICT solutions provided by an ICT organization across some of its customers; o Assessment of the effect of one or more specific ICT solutions implemented in an actual context for a specific customer.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T L.1333	https://www.itu.int/rec/T-REC-L.1333-202209-I	To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331.	S2.8, S2.24
ITU-T	(NEW) ITU_T L.1410	https://www.itu.int/rec/T-REC-L.1410-201412-I/en	Recommendation ITU-T L.1410 deals with environmental life cycle assessments (LCAs) of information and communication technology (ICT) goods, networks and services. It is organized in two parts: (a) Part I: ICT life cycle assessment: framework and guidance and (b) Part II: "Comparative analysis between ICT and reference product system (Baseline scenario); framework and guidance". Part I deals with the life cycle assessment (LCA) methodology applied to ICT goods, networks and services. Part II deals with comparative analysis based on LCA results of an ICT goods, networks and services product system, and a reference product system	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T L.1480	https://www.itu.int/rec/T-REC-L.1480 https://www.itu.int/rec/T-REC-L.1480-202507-P/en https://www.itu.int/rec/T-REC-L.1480-202212-I	Summary Recommendation ITU-T L.1480 provides a methodology for assessing how the use of information and communication technology (ICT) solutions impacts greenhouse gas (GHG) emissions of other sectors. More specifically, the methodology provides guidance on the assessment of the use of ICT solutions covering the net second order effect (i.e., the resulting second order effect after accounting for emissions due to the first order effects of the ICT solution), and the higher order effects such as rebound. By providing a structured methodological approach, it aims to improve the consistency, transparency and comprehensiveness of assessments of how the use of ICT solutions impacts GHG emissions over time. Guidance is provided to assess the net second order effect and higher order effects of the following cases: o) ICT solution(s) implemented in a specific context by the user of the ICT solution(s). o) ICT solution(s) implemented at different scales, including at an organizational level (whether private or public organizations), at a city level, at a country level or at worldwide level. o) ICT solution(s) seen from the perspective of an ICT organization contributing to the ICT solution(s). This includes: 1) Assessment of the aggregated effect of all ICT solutions provided by an ICT organization across all its customers; 2) Assessment of the aggregated effect of one or several ICT solutions provided by an ICT organization across some of its customers; 3) Assessment of the effect of one or more specific ICT solutions implemented in an actual context for a specific customer.	S2.8, S2.24
ITU-T	(NEW) ITU- T Y.4226 (ex Y.isms)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17882	This Recommendation provides an overview of a disaster monitoring system (DMS) for Smart Sustainable Cities (SSC) and identifies requirements and functional framework of the DMS.	S2.7, S2.8
ITU-T	(NEW) ITU_T Y.4505 (ex Y.MIM)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18458	This Recommendation defines the concept, purpose, and structure of Minimal Interoperability Mechanisms (MIMs) that provide the requirements for implementing minimal but sufficient capabilities needed to achieve interoperability based on a minimal common ground. The value of this approach is becoming widely recognised and several organisations and national and regional agencies are showing interest in the development of MIMs covering a range of different topics.	S2.7, S2.8

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T Y.4506 (ex Y.DRI-arch)	https://www.itu.int/rec/T-REC-L.1480-202212-I	This Recommendation is to define the reference architecture for autonomous delivery robots based on the ITU-T Y.4607 that interwork with delivery robot service provider, user devices, and urban infra-structure to facilitate the delivery of goods without human intervention.	S2.13
ITU-T	(NEW) ITU-T Y.4705 (ex Y.nmm-isms)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17883	This Recommendation provides a Sensing Capability Metadata Model (SCMM) for Dis-aster Monitoring System (DMS). It clarifies the basic metadata categories of sensing capability for DMS, and describes the structure and contents of sensing capabili-ty metadata elements of SCMM for DMS.	S2.1, S2.18
ITU-T	(NEW) ITU-T Y.dtmv-if	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19592	Noting the popularization of digital twin applications and metaverse services, the convergence of virtual and physical worlds through the use of digital twins within the metaverse is emerging as a technical challenge. This challenge will be addressed by identifying service scenarios, defining relevant requirements, and specifying a reference model along with its functional entities that perform a set of function-al roles involving data and information exchanges. Some data exchanges may involve digital twin-related actions, while others may occur with external systems or devices such as IoT devices, IoT gate-ways, application systems, management systems, and metaverse systems. This pro-posed interface model focuses specifically on data exchange associations among communication participants. It aims to ensure robust data and information flow between the metaverse's digital twin objects and external entities, enhancing system interoperability and service oper-ability across various platforms, systems, and devices. The interface model will be developed to be protocol-agnostic from a functional perspective and independent of any particular interface technology.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T Y.dtmv-ref	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19591	The metaverse is a vast virtual space comprising numerous distinct virtual worlds, each with its unique purpose and characteristics. Within this diversity of virtual worlds, there exists a specific type of virtual world that incorporates digital twins. In such a virtual world, each digital twin serves as an interface bridging the gap between virtual and physical worlds, enabling bidirectional interaction between virtual objects and the corresponding counterparts. Through this bidirectional interaction facilitated by digital twins, information from physical objects can be transmitted to the corresponding virtual objects in the virtual world, resulting in synchronization between them. Manipulating virtual objects can lead to the control of physical objects. By analyzing service scenarios, requirements can be derived. Based on these derived requirements, it can develop a reference model for integration. This draft Recommendation defines a reference model of integrating virtual and physical worlds through digital twins for the metaverse.	2.25.9, 2.25.15
ITU-T	(NEW) ITU_T Y.dtmv-reqts	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19590	TThe metaverse is a vast virtual space comprising numerous distinct virtual worlds, each with its unique purpose and characteristics. Within this diversity of virtual worlds, there exists a specific type of virtual world that incorporates digital twins. In such a virtual world, each digital twin serves as an interface bridging the gap between virtual and physical worlds, enabling bidirectional interaction between virtual objects and the corresponding counterparts. Through this bidirectional interaction facilitated by digital twins, information from physical objects can be transmitted to the corresponding virtual objects in the virtual world, resulting in synchronization between them. Manipulating virtual objects can lead to the control of physical objects. This draft Recommendation explores the service scenarios and defines the requirements of integrating virtual and physical worlds through digital twins for the metaverse.	2.25.9, 2.25.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T YSTR.ACC-SCC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18454	Smart city services can have a ripple effect beyond improving physical accessibility for persons with disabilities, those with age-related disabilities and those with specific needs. Persons with disabilities can benefit from more efficient and sophisticated city services through smart city services. Thus, it is an important opportunity to improve the quality of life using city functions equivalent to those without disabilities. However, as seen in many other use cases of ICTs, without consideration for persons with disabilities from the design stage, it is bound to be another barrier for persons with disabilities. Using a two-layer structure of accessibility consideration principles, this Technical Report provides development guidelines to be considered at each layer to implement accessible smart city services. Also, exemplar accessible smart city services are illustrated in the appendix.	
ITU-T	(NEW) ITU_T Y.4222 (ex Y.smart-evacuation)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17886	Smart evacuation facilitates effective and efficient solutions for people inside a disaster or emergency zone and for people that need to enter such a zone as part of the response. Internet of things (IoT) and smart cities and communities could be used to provide smart evacuation during a disaster or an emergency. This Recommendation describes concepts and features of smart evacuation control in disaster and emergency situations. It identifies high-level requirements and ICT infrastructure for smart evacuation along with use cases in disaster and emergency situations. The introduction of a smart evacuation service will allow the maintenance of the level of comfort for the population achieved in a smart city even in the event of an emergency. This is fundamental to justify the enormous material costs for the rapid development of smart cities around the world against the background of emergencies that have become more frequent throughout the world.	S2.3

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU_T Y.4227 (ex Y.IoT-BC-reqts-cap)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17932	Blockchain can help IoT and smart city and community related services and applications to establish trust, accountability and transparency while streamlining business processes. In order to promote the integration of blockchain with the IoT infrastructure, as well as enable richer flexible service scenarios for different IoT and smart cities and community verticals, this Recommendation, from the IoT point of view, identifies the functionalities of the blockchain, specifies the requirements of blockchain enabled IoT, and describes the specific IoT capabilities that are necessary to support blockchain.	S2.6, S2.10
ITU-T	(NEW) ITU_T Y.4228 (ex Y.IIoT-infra-SM-fr)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17949	Industrial Internet of things (IIoT) infrastructure for smart manufacturing refers to common facilities based on IoT that support smart manufacturing in industries or sectors. It is independent from the products and production process in specific enterprises. This Recommendation provides requirements and reference framework of the IIoT infrastructure capabilities for smart manufacturing to help service providers implementing their system according to the needs of smart manufacturing, and merge existing and newly developed IIoT infrastructure, in order to give the stakeholders of smart manufacturing guidance for their applications.	S2.3
ITU-T	(NEW) ITU_T Y.4229 (ex Y.IoT-SFFS)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17955	The frequent occurrence of forest fires has become a world-class problem. Although many countries have invested a lot of money in numerous counter-measures there are still several remaining challenges to be overcome. These challenges include the vastness of forest areas that cannot be fully monitored, and the incomplete network coverage of forests preventing efficient information transmission. Additionally, the performance of typical Internet of things (IoT) devices often fails to meet the actual requirements of forest applications. There are also a lack of early warning systems for impending forest fires, which delays the fire-extinguishing and rescue operations when fires occur, as well as a lack of adequate assessment and inspection of post-fire capabilities. With the development of IoT and artificial intelligence (AI), forest firefighting systems have become smarter.	S2.3, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			Smart forest firefighting systems are deployed in forest areas to enable real-time monitoring and early warning before forest fires occur. They can predict, locate, evaluate and extinguish fire when a fire occurs and provide inspection and damage assessment after a fire. This Recommendation introduces the smart forest firefighting system based on IoT and specifies the reference functional model and requirements. This Recommendation is intended to guide the design, development and implementation of the IoT-based smart forest firefighting system.	
ITU-T	(NEW) ITU_T Y.4230 (ex Y.EV-charging)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17954	With the rapid increase in the public usage of electric vehicles (EVs) in the city, more and more EV users put forward high requests for public charging service. Therefore, public smart charging service for EVs is the future development direction, and is an important part of the smart city. Compared with the traditional charging service, public smart charging service has the advantages of highly networked and digitized system, flexible and convenient use and intelligent management of electric power. Public smart charging service will be implemented on smart city infrastructure and it is indispensable for smart city in the future. This Recommendation specifies requirements and capability framework of public smart charging service for EVs, to optimize the EV charging service process and improve the EV charging service experience of EV users.	S2.3
ITU-T	(NEW) ITU_T Y.4231 (ex Y.IoT-Vreqs)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17953	With the popularization and development of smart cities and numerous IoT based verticals, the connotation of the internet of things (IoT) is expanding and is no longer limited to simple sensor data collection and discrimination. The IoT for vision is one of the main development directions of the IoT which use digital cameras and other types of sensors in order to perceive objects of interest (including human beings, vehicles, animals etc.) for diverse applications based on appropriate analysis. This Recommendation provides requirements and capability framework of the IoT for vision, a typical IoT for vision application workflow as well as some relevant IoT for vision use cases.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4232 (ex Y.IoT-RTPS)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18461	RTPS, which refers to roadside traffic perception system, is a system composed of Internet of Things (IoT) infrastructures, including sensing devices, cloud facilities, intelligent traffic lights and smart traffic signs. By utilizing IoT technologies, roadside traffic perception system (RTPS) can enhance traffic safety and efficiency with capabilities of its components. To enhance traffic safety and efficiency, IoT infrastructures in RTPS need to collaborate with each other using IoT technologies. Therefore, common and specific requirements and capabilities for IoT infrastructures are described in this recommendation. Use cases of RTPS are also given in the appendix.	S2.3, S2.7
ITU-T	(NEW) Y.4233 (ex Y.FSPH	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18460	This Recommendation specifies the framework of smart public health management in Smart and Sustainable Cities (SSC). SSCs are capable of fostering data driven smart applications to manage limited resources and implement them to thwart the advent of future pandemics of the same magnitude. Linking SSC with public health frameworks to manage future pandemics/ epidemics to the attainment of the SDGs (3: Global Heath, 1: Poverty Eradication and 11: Make cities inclusive, safe, resilient, and sustainable, and the Sendai Framework for Disaster Risk Reduction) is a challenge and serves a dual purpose. With the utilization of appropriate emergency communication and public health frameworks, it will become easier to develop models to predict the spread of diseases, ascertain the source of illnesses, coordinate lockdowns, detect and report symptoms, identify viral strains and provide remote assistance as required with limited human interaction, through an IoT-based infrastructure. This Recommendation is based on the U4SSC report entitled “Smart public health emergency management and ICT implementations” [b-U4SSC] and its structure is as follows: it starts with an analysis of the public health context and of corresponding frameworks, and returns a generic public health framework, which specifies the pandemic’s lifecycle. Then, this generic framework is interconnected with the SSC and with city resilience. Then, it depicts with UML diagrams how this framework can be executed within the SSC environment and highlights the SSC components that play role in this execution.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4234 (ex Y.RemoteEd)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18751	There is a wide and rising disparity in access to quality education between the remote and rural areas of any country when compared to its urban counterparts. Various international organizations (e.g., UN, ITU, etc.) and national bodies (such as and Ministries) worldwide have acknowledged the need for immediate efforts for the fulfilment of the promise for universalization of education. It is also very clear that the future of education is digital and immersive, and that delivery of the future education will be heavily dependent on access to appropriate ICT infrastructure and connectivity. There is a dire shortage of trained teaching staff in both developed and developing countries, where remote areas are concerned. In most such places, there are very few teachers, only some of which are capable to attend to the demands of fast evolving educational curriculums. In addition to education and learning, these remote areas are disadvantaged by lack of access to other facilities such as health and vocational capability development. To bridge the digital divide, and to ensure that the most vulnerable in society are not increasingly denied access to services, new standards are required to address the digital divide and the threat of growing disparity as more and more services are delivered online. This Recommendation includes a concept of e-learning in Remote Classrooms, i.e., places where ICT infrastructure and e-learning facilities, such as digital connectivity, computers, computer applications, virtual collaboration, online and digital educational catalogues, are made available for willing learners to educate themselves by using the said educational facilities. It develops requirements, capabilities and deployment models to enable high quality e-learning in Remote Classrooms in rural and remote areas, that otherwise lack the connectivity and ICT infrastructure to impart education.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4420-rev	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19606	Recommendation ITU-T Y.4420 describes a framework of Internet of things (IoT) based monitoring and management for lifts, including a protocol and a data model. Lifts need to interact with applications through communication networks to provide different kinds of services to end users. In many cases, lifts cannot connect to communication networks directly. Therefore, gateways support the interconnection of such lifts with communication networks. Y.4420 can be applied to various services that utilise lifts in smart buildings. However, indoor delivery services and lift remote control require remote connectivity to the lift. The revised Y.4420 enhances Y.4420 including the requirements, data models and enhanced use cases that apply to services requiring remote connectivity to the lift.	S2.1, S2.3
ITU-T	(NEW) Y.ACC-ASM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19057	To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.ACC-IoTMV	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19599	The virtual world based on real-world data collected through IoT technology and using XR technology as UX is collectively referred to as a metaverse supporting IoT. The metaverse interface should be designed to alleviate difficulties experienced by persons with disabilities and those with specific needs who struggle with certain senses in the real world. This draft Recommendation defines the accessibility requirements that metaverse services supporting IoT should have. Digital twin technology, implemented through data accumulated through the Internet of Things (IoT) based technology, builds an identical virtual world to the real world. The digital twin can be used to digitally implement the geographical and temporal environment of the real world to monitor various information, conduct complex experiments or predict future events. Immersive extended reality (XR) technologies, such as augmented reality (AR), virtual reality (VR), and mixed reality (MR), can be used as a user experience (UX) in this virtual world. The virtual world based on real-world data collected through IoT technology and using XR technology as UX is collectively referred to as a metaverse supporting IoT. The metaverse supporting IoT can provide services in various fields, such as remote medical services, smart factories, smart agriculture, and simulation education.	S.3, S2.25.9, S.2.25.15
ITU-T	(NEW) Y.DEMC-fra	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19607	This Recommendation aims to achieve the goal of effective management and proactive interaction for distributed energy resources with complex and heterogeneous data in the IoT environment. The core content includes the main aggregation and interaction requirements and overall framework of distributed energy resources management and control services. This Recommendation fits the application scenarios of massive resources access and interaction in the IoT environment, and meets the business needs of distributed energy clusters to participate in power grid interaction, distributed local control, and resource security access, building a distributed, low-cost, and highly reliable power system.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.dt-IWCS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18459	Water conservancy is always a hot topic and it is an important factor in urban and rural governance. Smart water conservancy system driven by digital twin is suggested to be implemented since it can support the intelligent monitor, control and regulate the usage and safety of water conservancy via the digital twin interaction between digital object and physical object of water conservancy. This draft Recommendation addresses requirements and capability framework of digital twin for intelligent water conservancy system.	S2.3, S2.14, S2.23
ITU-T	(NEW) Y.dt-PAF	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19600	Various walking assistance facilities are installed on pedestrian paths throughout the city to help persons with disabilities walk. For example, wheelchair ramps are installed on stairs where wheelchairs are difficult to move for those with physical disabilities who use wheelchairs. Moreover, braille blocks for those with visual disabilities are installed on pedestrian roads, and sound signals that inform the change of traffic lights through audio signals are installed at crossings. These diverse facilities support the independent mobility of persons with disabilities. However, their usage and management are often hindered by the harsh conditions in which they are installed. The challenges range from incorrect installations that render the facilities unusable to accidents that lead to breakages and even instances where the facilities, though present, are underutilised due to a lack of promotion. For persons with disabilities, even a single problem on their walking path can make the entire journey impossible. This underscores the critical importance of the control and management of these facilities. Ensuring independent mobility is not just a matter of convenience, but a fundamental right that we must strive to protect. This Recommendation provides the requirements and capabilities of a digital twin for pedestrian accessibility facilities for persons with disabilities, which supports controlling and managing pedestrian assistance facilities for persons with disabilities installed on pedestrian roads, providing appropriate information to users, and assisting in maintenance and management.	2.3, 2.14, , S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.dt-SComCam	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18750	A complex or campus is a collection of buildings and grounds that belong to a given institution, either academic or non-academic. There are many types of complex, such as complexes for corporates, industries, sport and meeting venues, commerce, etc. A campus refers to a specific area for academic purposes. Complexes and campuses play an important role in people's work and life, and have common requirements in terms of smart management. With the development of the Internet of Things and artificial intelligence, the management of complex and campus has gradually moved towards intelligence, and many smart complex and campus systems have emerged to improve the management and operation efficiency. The digital twin technology can solve the problems like historical record or baseline, operational performance monitoring, testing or predicting future outcomes. It has been widely used in smart complex and campus system. By combining with emerging ICT technologies, such as cloud computing, the Internet of Things, big data, and artificial intelligence, it is possible to access various terminals to collect the data of physical complex and campus in real time, and to model people (without personally identifiable information), devices, things and events in the complex and campus, realize intelligent monitoring and simulation, and realize remote control of the physical complex and campus through the digital twin complex and campus. Digital twin based smart complex and campus system can address challenges of management and operation of complex and campus, such as low management efficiency, poor service experience, serious energy waste, weak comprehensive security, and high operational costs. It implements digital transformation of such complex and campus and enhances service experience.	S2.3, S2.14, S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.EMM-Reqts:	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17952	This draft Recommendation presents the overview and specifies the requirements of a Real-time Event Monitoring and Integrated Management (EMM) platform. The real-time event monitoring and integrated management platform is one of Smart City Platforms [ITU-T Y.4201]. It connects various intelligent facilities equipped with IoT sensors, providing stakeholders with the necessary data (integrated information) to make informed decisions and respond promptly to an event that may rise in a city. The platform is particularly designed for integration of data and allowing the users to utilize data and to monitor city events in real time.	S2.3, S2.7, S2.14,
ITU-T	(NEW) Y.energy-storage	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18749	With the promotion of renewable energy generation in residential communities, a large number of community users are transformed into prosumers with a dual role of producer and consumer. To maximize the interests of community users, it is necessary to introduce energy storage service for residential community (ESSRC) to centrally manage energy. Furthermore, ESSRC operators can earn the price difference through the difference of spot prices in the electricity market, so as to achieve a win-win situation. ESSRC is an important part of smart residential communities in smart cities, and a large number of ESSRC operators have entered this market. But the lack of standards could limit the operators' ability to meet rising demand across the globe. ESSRC is based on an ICT-based information management system, so this Recommendation focuses on requirements and capability framework of ESSRC in smart city. This Recommendation will help to promote the achievement of circular and sustainable smart cities and communities. The use case of ESSRC is provided in Appendix	S2.8, S.2.22. S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.EV-PUD	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19062	Electric vehicle (EV) market is growing, and the power consumption cannot be ignored. For better tracking and management of carbon emission in smart cities, fine-granularity power usage (PU) data is required. This Recommendation provides the requirements for the electric vehicle power usage data acquisition and management. The data collected pertains to the electric vehicle's power usage process, and the smart city infrastructure, including roadside units, cellular base stations, hotspots etc., should be used for EV PU data delivery and utilization in smart city platform. Following the specified requirements, uniform electric vehicle power usage data can be acquired and managed, which can enable smart city to trace vehicle level carbon footprint as well as to provide information support to other applications e.g., power charging station planning, insurance pricing, etc. This Recommendation specifies the requirements and reference system framework for electric vehicle power usage data acquisition and management for smart city, as well as it describes some relevant reference use cases for EV PU data acquisition and management.	S2.7, S2.8, S2.24
ITU-T	(NEW) Y.IoT-APS-Reqts	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19605	The integration of new-generation information technologies such as the fifth-generation mobile communication network (IMT-2020) technologies, AI, big data, and cloud computing has greatly facilitated the development of IoT applications. The applications involved in the IoT verticals place differentiated and dynamic requirements for IoT capabilities. Application-aware service is a service to adapt IoT capabilities as appropriate based on the specific requirements of IoT applications applied in various scenarios. Application-aware service assists IoT in identifying the types, priorities and dynamic needs of applications, and dynamically adapting IoT capabilities in coordination with the network capabilities. At the same time, IoT applications can adjust their status according to the status of IoT resources. The service experience of IoT applications can be optimized through application-aware service. This Recommendation specifies the requirements and capability framework of Internet of Things for support of application-aware service.	2.7, 2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-PD	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19061	Driven by the global efforts to achieve carbon neutrality goals, the cities are accelerating their transformation towards intelligence, greenery, and low-carbon development. Electric power is the main form of energy consumption in cities, achieving electric power data's comprehensive perception and intelligent monitoring will become an important foundation to support smart cities sustainable development. The goal of this draft Recommendation differs from the existing relevant standards of SDOs involved in IoT perception and IoT application in the electric power field. This draft Recommendation aims to address the challenges faced by new energy rapid development. It can fully leverage IoT technical characteristics and propose a framework and requirements for electric power data perception services. It also effectively fills the standard gap, provides technical means and basis for electric power supply departments to comprehensively grasp distributed energy data, and further promotes smart cities sustainable development.	S2.8, S2.24
ITU-T	(NEW) Y.IoT-smart-school	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19059	This Recommendation focuses on the utilization of IoT technologies in school management to improve intelligent level in school security, teaching assessment, academic affairs, and school life, ultimately increasing the effectiveness and efficiency of school management. By sensing, collecting, and identifying school related management information, combined with the appropriate usage of cloud computing and AI technologies, school administrations can achieve real-time monitoring, early warning, and actionable intelligence from a management issues, thereby ensuring the quality of education while safeguarding students' smart school life and life safety. The Recommendation provides overview, device requirements, network requirements, service and application support requirements, and application requirements of IoT-based smart school management system (SSMS).	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-soil	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19058	Soil is vitally important for both human well-being and the health of our planet. It serves as the foundation for maintaining ecological balance, ensuring food safety, promoting sustainable development, and protecting against health risks. By utilizing technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), it is possible to achieve integrated space-air-ground soil environmental monitoring and data-driven intelligent decision-making for soil protection and remediation strategies. This Recommendation provides overview, device requirements, network requirements, service support and application support requirements, and application requirements of IoT-based Soil Environmental Protection and Remediation (SEPR).	
ITU-T	(NEW) Y.LASS-fra	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19601	This Recommendation will specify the requirements and capability framework of IoT-based low-altitude sensing system. It will address the following aspects: Overview of IoT-based low-altitude sensing system. Requirements of IoT-based low-altitude sensing system. Capability framework of IoT-based low-altitude sensing system. Use cases of IoT-based low-altitude sensing system. This Recommendation will specify the requirements and capability framework of IoT-based low-altitude sensing system. It will address the following aspects: -Overview of IoT-based low-altitude sensing system. -Requirements of IoT-based low-altitude sensing system. -Capability framework of IoT-based low-altitude sensing system. -Use cases of IoT-based low-altitude sensing system.	
ITU-T	(NEW) Y.PG-ComNet-Reqts	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18748	The IoT-based power grid communication network provides bidirectional data interaction in all phases of power grid operations, including electric power generation, transmission, distribution and consumption. It is an effective means to achieve comprehensive awareness of power grid status, to enable human-computer interaction and ubiquitous access of the IoT devices of the power grid. This Recommendation specifies the requirements of IoT-based power grid communication network.	S2.3, S2.8, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.SC-CNS-Reqts	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19603	Smart sustainable city is a new concept and model of global urban development. The smart city communication network provides support for different smart city systems (such as energy management, emergency management, etc.) and smart city platforms. There is currently no identified standards specification specifying requirements of smart city communication network. It is needed to study smart city communication network based on the comprehensive requirements of the smart cities. Based on the study of different application scenarios of smart city communication network system, this Recommendation introduces the concept of smart city communication network system (SCCNS), which provides a reliable and secure data transmission service between the SCP and Sensing and Data Collection Systems (SDCS). It then analyses the requirements of the SCCNS and specifies the functions of SCCNS. The study aims to enable enhanced support of the operation of diverse services and applications in smart cities and provide guidance for the design and deployment of smart city communication network by clarifying the requirements and functions of SCCNS.	S2.3, S2.8, S2.14
ITU-T	(NEW) Y.SCGMS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19602	Building up the IoT-based smart crop growth monitoring system is essential to modern agricultural development. Traditional monitoring of crop growth often relies on manual inspection and sampling, which is both inefficient and susceptible to human subjective factors, potentially leading to bias in the monitoring results. Besides, the research and application of crop growth monitoring technology is relatively lagging behind, and the effective linkage with agricultural environment monitoring technology also appears to be insufficient. Therefore, it is necessary to define the IoT-based smart crop growth monitoring system including device layer, network layer, service and application support layer and application layer, from an ICT perspective. The IoT-based smart crop growth status monitoring system can provide real-time monitoring, intelligent analysis of crop growth status, yield prediction and guidance for the growth process.	S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This system can enhance the efficiency of agricultural production, optimize the allocation of resources, reduce production costs, minimize risky losses, and ultimately increase grain yield and quality. It provides solid technical support for the precise management and efficient production of modern agriculture and promotes the sustainable development of agriculture.	
ITU-T	(NEW) Y.Sup. EdgeIoT-use-cases	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19063	Edge computing based Internet of Things is crucial for navigating the evolving global digital economy and advancing digital transformation. This supplement to Y.4208 defines the types of edge computing based Internet of Things, recommended template and classification schemes of use cases. Several use cases are illustrated in details. It also identifies challenges, opportunities, observations as well as suggestions of edge computing based Internet of Things.	S2.7
ITU-T	(NEW) Y.Sup. SmartAqua-use-cases	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18753	Due to climate change and growing population, problems of food shortage are expected globally. Aquaculture, also known as fish farming, adjusts water environments using IoT, AI, and robot technologies to provide better conditions for fish growing. Examples of water environmental parameters which may affect fish growing include dissolved oxygen (DO), air- and water-temperature, pH, carbon dioxide (CO2), electrical conductivity (EC), suspended solid (SS), turbidity, oxidation-reduction potential (ORP), total ammonia nitrogen, and water levels. A number of diverse IoT devices (including sensors, actuators, and robots) are involved in smart aquaculture in order to provide different services such as water monitoring and management, and autonomous fish farm management. Therefore, it is necessary to survey present smart agriculture technologies as well as future-promising technologies. Based on the survey results, meaningful standardization work items can be identified. This new work item surveys use cases related to smart aquaculture.in the perspective of fish farming using IoT, AI, and robot technologies.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Sup-datainter-op-usecases	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19608	ITU-T Y.4563 outlines the requirements and functional model to support data inter-operability in Internet of things environ-ments. However, in ITU-T Y.4563 there is a scarcity of use cases related to the data interoperability in IoT and, more general-ly, data interoperability is not sufficiently addressed for IoT environments. This s draft Supplement to ITU-T Y.4563 provides use cases of data interoperability in IoT. . Types, architectural considerations and classifica-tion of data interoperability in IoT are spec-ified. Use cases corresponding to the types of data interoperability in IoT are described based on the recommended template. Challenges and opportunities are identi-fied to motivate following standardization works related to this work item.	S2.1
ITU-T	(NEW) Y.Sup-IoT-BC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19060	Cities are taking action and embracing cutting-edge solutions such as artificial intelligence (AI), 5G, digital twin, Internet of Things (IoT) and the metaverse to digitize and automate city operations. Digital technologies are at the forefront of creat-ing smart sustainable cities that promote efficiency, economic development and im-proved quality of life for inhabitants. Block-chain is identified as one of the important cutting-edge (also referred as emerging technologies) digital technologies ena-bling city digital transformation. As the lead group of IoT and its applications, as well as the lead group of smart cities and communities and related digital services, ITU-T SG20 has 6 published and 5 on-go-ing blockchain related work items. This Supplement complements the ITU-T SG20 blockchain related Recommendations and is expected to benefit further research and standardization on blockchain integration with IoT The scope of this Supplement includes: - Recommended template for the description of use cases - Use cases	
ITU-T	(NEW) Y.Sup-SCC-AI	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19604	Smart cities and communities (SC&C) share the goal of achieving urban sustain-ability without sacrificing the quality of life (QoL) of their citizens. Artificial intelligence (AI) offers a powerful tool to address these issues, enabling cities to harness vast amounts of data generated from SC&C. AI can analyze and process this data in real-time, providing actionable insights that help city planners and administrators make more informed decisions. This Sup-plement specifies the use cases of smart cities and communities supported by AI.	2,14, 2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) YSTR. Ambient IoT	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18752	In IoT systems, a large number of physical terminals may not have the space to hold batteries or bear the cost of batteries, such scenarios include but are not limited to fast-moving consumer goods, logistics packages, product line packaging, ware-house goods inventory, etc. Huge scenarios may involve up to more than ten thousand IoT nodes, which conventional IoT devices are not able to implement in terms of cost, size, and power mode. An Ambient pow-er-enabled IoT is a global infrastructure for the information society, enabling IoT services by harvesting ambient energy to power the IoT devices. Instead of using bat-teries to power the devices, Ambient-IoT devices are capable of harvesting ambient energy to power electronic modules. The ambient power can be provided by distrib-uted power transfer nodes (e.g., existing network infrastructure, dedicated power transfer device) or natural power (e.g., light, vibration, thermal).	S2.5, S2.7
ITU-T	(NEW) Y.4417-Rev	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19610	The evolution of IoT can be divided into three stages: the first stage being connec-tivity, the second stage being intelligence, and the third stage being autonomy. Currently, IoT technology is positioned at the early phase of the second stage, which focuses on intelligence. In addition, most of the standards development in the field of IoT technology has been focused on connectivity-based IoT standards. However, there is a gradual emergence of standards for intelligent IoT as well. Nevertheless, in the context of autonomous IoT, standard development has been primarily concen-trated on service technologies. Through analyses such as those presented in Table 2, it is evident how the evolution of stand-ard technologies has progressed alongside the evolution of IoT technology. It high-lights that the standardization phase of IoT is still in its early stages when it comes to developing intelligent standards. Recom-mendation ITU-T Y.4417 (06/2018) specifies a framework of self-organization network-ing in IoT environments with character-istics, requirements, functional architec-tures, and functionalities. The framework manages the functionalities to enable intelligent and autonomous services for IoT network technology.	S2.13

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			However, the functionalities within the framework – including the Coordinator election, Initialization and configuration, Identification, Data forwarding and delivery, Network recovery, and Routing and path discovery – are defined without considering the technical concepts and characteristics of intelligent IoT and autonomous IoT. As a result, Recommendation ITU-T Y.4417 needs to be revised to achieve a certain level of standard quality maturity to better configure networks for the coming intelligent and autonomous IoT environments.	
ITU-T	(NEW) Y.4477-Rev	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19064	To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331.	S2.8, S2.24
ITU-T	(NEW) Y.4480Rev0	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18747	This Recommendation defines a protocol for wide area wireless networks, which is optimized for battery-powered end-devices that may be either mobile or mounted at a fixed location.	S2.5
ITU-T	(NEW) Y.4496 (ex Y.RA-PHE)	Recommendation ITU-T Y.4496 is intended to provide the requirements and architecture for a smart service for public health emergency system that can be implemented to address current and future potential public health risks.	Recommendation ITU-T Y.4496 is intended to provide the requirements and architecture for a smart service for public health emergency system that can be implemented to address current and future potential public health risks.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4501 (ex Y.RA-SDL)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17926	This Recommendation describes the functional architecture for the smart door lock (SDL) service framework. With the development of mobile communication technology and smart hardware, various technologies are introduced into the door lock to form the smart door lock. Multiple unlocking methods can be realized, and abnormal alarm reporting and flexible door lock management can be performed. In order to promote the deployment of the smart door lock (SDL) service around the world, a unified standard is needed to specify, and functions should be realized for the SDL service framework. The scope of this Recommendation includes the introduction of the SDL service framework, requirements of the SDL service framework and functional architecture of the SDL service framework.	S2.3, S2.14
ITU-T	(NEW) Y.4502 (ex Y.IoT-SQMS)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17937	Emerging technologies, such as artificial intelligence, crowdsourcing, etc, are enhancing the sensing capabilities of IoT systems in recent years. IoT sensing quality management has become more complex. Consequently, sensing quality management service needs to be compatible with these emerging technologies in order to help in improving service quality of IoT systems. This Recommendation specifies the functions architecture of IoT sensing quality management service.	S2.3, S2.14
ITU-T	(NEW) Y.4507 (ex Y.arc-psfws)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18746	The early warning system of power supply facilities based on the Internet of Things technology can obtain the real-time status parameters of power equipment and realize the equipment status prediction and fault early warning through the status assessment and early warning model. It can improve the operation economy of assets and ensure the reliability of power supply. It is necessary to put forward the warning system for power supply facilities. This Recommendation provides the functional architecture of power supply facilities warning system, use cases and data flows also are provided in this recommendation.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y. EP-WS-fc:	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19613	The power industry is one of the cornerstones of modern human society, providing a stable and reliable energy supply for everyone. As the process of urbanization accelerates, the demand for electricity also grows. The United Nations' "Tracking SDG7: The Energy Progress Report" sets a goal to focus on ensuring that people have access to affordable, reliable, and sustainable modern energy. From environmental protection to sustainable development, an adequate and reliable power supply is an important support for economic transformation and an important guarantee for harmonious social development. The electric power work site (EPWS) is the core place for the operation and maintenance of the power system, characterized complexity in operations. This proposal is going to standardize functional capabilities of electric power work site operation services to improve operational efficiency, providing an important technical means for establishing a safe, scientific, and efficient electric power work site.	S2.8, S2.24
ITU-T	(NEW) Y.AI-DECCS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17929	The maturity of Internet of things technology and the widespread deployment of network provide good infrastructure conditions to the application of AI at the device, edge and cloud for IoT and smart city. The requirements of AI models in IoT and smart city are dynamic, thus how to make AI system continuously and dynamically update, as well as infer and predict in real-time is essential to the application of AI in IoT and smart city. The device-edge-cloud collaborative service enables collaborative inference, and dynamic learning and updating of AI models on the device-edge-cloud architecture, so as to meet the needs of various current and future application scenarios. This recommendation specifies the Functional architecture of AI enabled device-edge-cloud collaborative services for IoT and smart city.	S2.7, S2.14. S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.cnce-IoT-arch	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17894	In traditional hospitals, there might be some issues to be improved, such as low efficiency of medical care, poor service experience of patients and lack of management efficiency. Smart hospital is a new concept to provide digital medical treatment by automatic and remote services based on information and communication technologies, e.g. prevention and diagnosis of illness, treatment and nursing for patients. Smart hospitals have demands for high-precision positioning, and the service quality guarantee of all kinds of local services, which may require network capability exposure to support the mentioned requirements. With the support of network capability exposure, some new services such as high-precision positioning can be provided and better service experience can be achieved. This recommendation provides the functional architecture and functional entities of network capability exposure for smart hospital based on Internet of things. Related use cases are provided in the appendix.	S2.3, S2.14
ITU-T	(NEW) Y.DT-CS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19611	Smart cities support human life by services that reference and analyse digital twins of surrounding environment, and that control actuators and systems including vehicles, traffic systems, lightings, air conditioners, etc. Digital twins provide the basis of control and, therefore, they need to reflect the up-to-date state of the object of interest. Numerous object exist in the real world, and taking their digital twins and maintaining the digital twins up to date requires massive effort due to the amount of the digital twin data. The creation and update of the digital twin data is likely to be performed by cooperation of many entities including municipalities, companies, other organizations, and even individuals by exploiting the concept of "sharing economy". The contribution on digital twins made by those entities should be properly recorded to make the responsibility in contributed digital twins explicit and the digital twins correct. Also, incentive mechanism involving both givers and takers of the incentive is required to promote contribution. This Recommendation specifies the requirements and functional architecture for the infrastructure to create up-to-date digital twins by cooperation of many entities on the basis of blockchain technology.	S2.3, S2.14, S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
ITU-T	(NEW) Y.DTS-arch	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19612	The digital twin concept turns a new view of technology into the power grid. Digital Twin system in power grid can perform online analysis of the grid in real-time and integrates all the information and express the current grid status to the producers and consumers and predicts the future grid status. Thus, the power grid transmission loss and location of the overheated line and power connection missing can be detected in addition decision-making and self-healing can possible. The future prediction saves the power grid from small to large accidents such as power outages and even blackout problems. This draft recommendation provides the architecture of the digital twin power grid, describes the functional entities in the digital twin system, as well as the use cases.	S2.3, S2.8, S2.23
ITU-T	(NEW) Y. Fram-ssdp	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19614	Electric power facilities are increasingly vulnerable to natural disasters exacerbated by global climate change, necessitating urgent action. However, conducting real emergency drills poses challenges due to the complexity of reproducing disaster scenarios, coordinating multi-party personnel collaboration across various agencies, enterprises, and sectors, and the associated high economic costs. The metaverse, an immersive digital environment integrating digital twins, augmented reality, virtual reality, and other digital technologies and information and communication technologies, offers a promising solution. It provides a robust simulation framework for disaster prevention in electric power facilities. This Recommendation specifies the requirements and reference framework of metaverse simulation service for disaster prevention in electric power facilities, which will help to optimize the emergency response strategies and improve the disaster prevention and mitigation capability for electric power facilities.	S2.3, S2.8, S2.23, S2.25.15,

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-BoT-pee	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17936	Recommendation ITU-T Y.4464 "Framework of blockchain of things as decentralized service platform" introduces a decentralized Internet of things (IoT) service platform, blockchain of things (BoT), and provides its common capabilities and functionalities. A BoT entity is a functional entity or physical entity (e.g., IoT server, IoT device, IoT gateway and end user device) that participates in the activities performed in a BoT. A BoT peer is a logic function of a BoT entity to perform BoT-related functionalities in processes of communications, consensus-making, transactions and management. BoT peers are participants of BoTs which create and maintain BoTs. This Recommendation presents common capabilities, functional architecture and general interactions of blockchain of things peers.	S2.6, S2.7, S2.10
ITU-T	(NEW) Y.IoT-CMP-VR	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19615	This Recommendation provides coordination management platform for IoT based vehicle-road, including reference framework and associated capabilities. This Recommendation defines a unified framework that incorporates vehicles and other traffic participants, roadside infrastructure, cloud management platforms, and management applications for intelligent connected vehicle management and intelligent traffic management.	S2.3, S2.14
ITU-T	(NEW) Y.IoT-CONV-fr	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17958	Internet of Things (IoT) has become a fundamental technology in service infrastructure, integrating with the other emerging ICTs to produce intelligent and autonomous solutions. This draft Recommendation describes "Convergence framework for enhancement of service intelligence based on Internet of Things". This document outlines a framework detailing how IoT can be integrated with technologies of AI (Artificial Intelligence), Cloud, Edge computing, Distributed Ledger Technology (DLT) and, Big data to enhance service intelligence.	S2.3, S2.7, S2.10, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-DPE	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18745	In recent years, the trend towards the intelligence and IoT integration of power equipment has become increasingly evident. Utilizing various distributed sensors and their IoT systems enables functions such as power equipment status monitoring, diagnostic evaluation, and maintenance decision-making. Meanwhile, the safe, stable, and reliable operation of power equipment also depends on the effective collaboration of numerous IoT sensing and controlling devices. Consequently, the need for unified management and coordination of power equipment and their sensing/controlling devices using distributed IoT technology has become increasingly urgent. This Recommendation provides the management framework for IoT-based distributed power equipment, including the framework, functional systems, and reference interfaces.	S2.3, S2.7, S2.8
ITU-T	(NEW) Y.IoT-ES-SB	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19616	Smart buildings suffer from issues such as uncoordinated equipment operation and low energy utilization rates, resulting in a series of industry pain points, including high energy consumption, low data utilization, high operation and maintenance costs. Through IoT technology, smart buildings can achieve real-time monitoring and remote control of energy consumption data, allowing for refined management and intelligent optimization of energy use. This Recommendation specifies the functional architecture of IoT-based energy-saving service for smart buildings. This Recommendation is intended to guide the design, development, implementation, and application of IoT-based energy-saving service for smart buildings	S2.3, S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-ISP	hhttps://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19065	Data security and dependable exchange are critical to the industry's digital revolution. IoT and blockchain technologies will provide new technological solutions for industrial transformation. It aim to connect devices securely and share data reliably among different industrial platforms by leveraging IoT and blockchain technology, which could improve collaboration between supply chain and production processes. The object of this Recommendation is to define the the smart industry service platform based blockchian and IoT, and provide requirements and functional framework for the the the smart industry service platform based blockchian and IoT. IoT and blockchain technologies will provide new technological solutions for industrial transformation. Smart industry service platform based blockchian and IoT aims to connect devices securely and share data reliably among different industrial platforms by leveraging IoT and blockchain technology, which could improve collaboration between supply chain and production processes. The object of this Recommendation is to define the smart industry service platform based IoT and blockchian, and provide requirements and functional framework for the smart industry service platform.	S2.6, S2.10
ITU-T	(NEW) Y.IoT-MVarch	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19620	With the popularization and development of smart cities, intelligent agriculture and smart manufacturing, the connotation of the internet of things (IoT) is also expanding and is no longer limited to simple sensor data collection and discrimination. The IoT based machine vision will become one of the main development directions of the IoT which use cameras and cloud-network systems to capture the objects (including human being, vehicle, animal etc.) in real time and transmit them in the way of fusion networks and make analysis. The applications built based on the existing IoT architecture cannot perceive the cloud-network capabilities and resource distribution. Some applications are built in private network, the services unable to scale deployment, interconnectivity, and flexible expansion. The data unable to be fully utilized due to the capabilities of network and computing resource are not well managed in the IoT platform. This draft Technical Report analysis the functional architecture as well as functional entities and reference points for IoT based machine vision system.	S2.3, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-NCM-arch	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18462	This Recommendation provides the functional architecture of network connectivity management in the Internet of things, including the functional entities, relevant reference points and logical flows.	S2.7
ITU-T	(NEW) Y.IoT-SAS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19617	Accessibility services are typically designed for public facilities or personal devices and depend on the ability of persons with disabilities to learn and adapt. These individuals must familiarize themselves with the functions of these services to select the ones that best meet their needs. With the continuous advancement of technologies such as the Internet of Things (IoT) and artificial intelligence, more intelligent applications, services, and devices are becoming integrated into smart community life. Unlike existing accessibility services, the use of these emerging technologies can significantly reduce the reliance on the learning abilities of persons with disabilities, enhancing their quality of life and ensuring their equal integration into the digital society. The Recommendation focuses on how to realize IoT-based smart accessibility services in the context of smart communities from the functional architecture perspective, mainly concentrating on the service support and application support layer and device layers. The users of the IoT-enable smart accessibility service standardized in this standard include persons with disabilities, persons with age-related disabilities, and those with specific needs. It is beneficial for communities worldwide to initiate a new Recommendation - Functional architecture of IoT-enabled smart accessibility services in smart communities.	S2.3, S2.14, S2.15
ITU-T	(NEW) Y.IoT-SPA	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19067	This Recommendation provides the functional architecture of smart park based on Internet of Things, including the concept, goals and key components, the requirements and the functional architecture of the smart park based on Internet of Things.	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.NCE. arch.EIoT	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17934	Compared to communication between humans, communication between machines in enterprise IoT services is much more challenging. Different customers may have different needs, for example, some manufacturing customers mainly use lots of sensors which needs high network capacity and delay insensitive, some manufacturing customers mainly use robots which needs high network reliability and delay sensitive, and some customers have multiple types of terminals in the same factory, such as sensors, cameras, robots and PLC controllers. In general, different services and applications requires different network capability exposure. Flexible QoS requirements and QoE requirements need to be considered as important elements for building functional architectures to support enterprise services. This draft new Recommendation specifies functional architecture enhancement with network capability exposure to support flexible QoS and QoE requirements, and functional entities and reference points of the proposed functional architecture.	S2.3, S2.14
ITU-T	(NEW) Y.RA-FML	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17924	The widespread popularity of data-driven services and applications transforms the IoT and Smart City & Community (SC&C) system from a traditional data collecting and transportation network into a more holistic architecture with AI-native data processing and service delivery capability. One of the key challenges in designing an AI-based architecture for large IoT and SC&C networking systems is to implement distributed data processing and learning across a large number of decentralized datasets that can be owned or managed by different entities such as cities, communities, buildings, devices, government and business entities. Federated machine learning (FML) is an emerging distributed AI framework that enables collaborative machine learning (ML) and model construction across decentralized datasets. It offers a viable solution for data-driven data learning and synthesis across a wide variety of entities across large SC&C networking systems. The main purpose of this recommendation is to provide a feasible and standardized solution for the IoT and SC&C relevant services and applications to use and deploy FML-enabled collaborative data learning across distributed and decentralized data sources.	2.7, 2.14, 2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.SA-DSC-SSC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19618	Digital supply chain for SSC is a complex system engineering covering strategic transformation, organizational restructuring, function upgrading, data mining and technology introduction. For managers and stakeholders of SSC, the research, design, construction and management of digital supply chain are not systematic. Therefore, there is an urgent need to standardize a set of conceptual model and general reference framework covering the whole elements and the whole process of the digital supply chain. This recommendation presents system architecture of digital supply chain for SSC, expounds the constituent elements and interrelationship of digital supply chain from the aspects of device, network, service and application support, service function, security and management, and explain the construction method of digital supply chain for SSC.	
ITU-T	(NEW) Y.SC-DESMS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19609	This proposal introduces the functional architecture of an IoT-based distributed energy storage(DES) management system for smart cities. It comprises the application layer, the service and application support layer, the network layer, and the device layer, covering specific needs in areas such as data collection, intelligent analysis, services, networking, equipment inspection, and security. Additionally, it defines the specific functional units of the IoT-based DES management system for smart cities. The draft recommendation provides guidance for the design, development, and application of IoT-based DES management systems for smart cities, promoting the global development of distributed energy storage and supporting the construction of smart cities.	S2.7, S2.8, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.SFPP	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19066	The development of smart farmland is an important issue of global concern. Smart farmland production has evolved from the primary stage to the advanced stage. A large number of manufacturers provide various types of sensors and subsystems. But these vertical subsystems are independent of each other, and the data and information are not effectively shared. In order to integrate these vertical subsystems and fully utilize the data and information, it is necessary to define a unified farmland production platform, which can effectively utilize resources, and support multiple applications. This platform can effectively integrate multiple subsystems, improve data usage efficiency, and support farmland production decision-making ability. It can provide comprehensive and clear guidance for the production of smart farmland, and can guide the development of the entire industry chain towards more advanced level. This draft new Recommendation introduces the farmland production platform, and specifies its requirements and reference framework.	S2.14
	(NEW) Y.smart-PBRS	https://www.itu.int/rec/T-REC-L.1333-202209-I	With the adoption of Internet of Things (IoT) technology, Smart Power Bank Rental (SPBR) service can satisfy the on-the-go charging needs for people, improve the service efficiency and provide real-time service monitoring and management for the service providers. Relevant products of SPBR service have emerged and developed in a certain scale in several countries and regions. Lack of standards might cause deviating capabilities and uneven performance of the service, which can lead to inconsistent service experience and limit vendors' ability to meet rising demand across the global, thus affecting the market acceptance of this service. This Recommendation introduces SPBR Service, and specifies functional requirements of SPBR Service and functional architecture of SPBR Service framework to provide guidance for device manufacturers and service providers when developing the SPBR equipment and services.	S2.7, S2.8

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Sup. IoT-CONV (ex YSTR.IoT-CONV)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17959	Internet of Things has become fundamental technology of service infrastructure with convergence with the other emerging ICT to produce intelligent and autonomous solution. At the beginning, IoT technology focuses on "something connected". After connecting devices or sensors, ICT services obtain the useful information and have utilized it for accomplishing life convenience and increasing productivity. These days, Human being does not think of 'connectivity' is not a new technology anymore. Human being expects more convenient life style and accomplishes much more products and better services. Such expectations make it that IoT does not just remain technology of 'connectivity' itself but also developing and evolving into 'intelligence' and 'autonomy'. In fact, there are a lot of things to be developed for future IoT. In IoT, intelligence and connectivity enable an entirely new set of product functions and capabilities, which can be grouped into four areas: monitoring, control, optimization, and autonomy. IoT can be categorized into three stages: 1st Stage: connectivity, 2nd Stage: intelligence, 3rd Stage: autonomy. The state of IoT technology remains at the beginning of 2nd stage for intelligence. Connectivity can be achieved with two or more devices only. However, the intelligence and autonomy of IoT require the other emerging technologies, such as AI, Cloud, Edge computing, DLT, Big Data and so on for convergence services. This new technical report is to provide a overview how IoT is merged with technologies of AI, Cloud, Edge computing, DLT and, (Big) data for enhancement of service intelligence.	S2.7, S2.13, S2.14, S2.15,
ITU-T	(NEW) Y.Sup. IoT-SEDR	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19069	This supplement specifies the functional framework and capabilities for digital resources in smart education that is defined in ITU-T Y.4485. This supplement provides the overview of digital resources in smart education, service and application of digital resources, sensing and acquisition capabilities of digital resources, services and application support capabilities, services integrate and data exchange capabilities of digital educational resources.	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Sup. VFS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19070	This Supplement provides the functional architecture of connected vehicle formation supporting based on edge computing, including functional architecture, functional entity, and reference point, which is a supplementary to ITU-T Y.4471 Recommendation.	S2.14
ITU-T	(NEW) Y.Sup_SUPS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19619	This proposal proposes to initiate a new work item on functional architecture of Internet of Things (IoT) based underground smart parking services (SUPS). This contribution discusses the important role of SUPS in urban traffic management. SUPS is based on IoT technology and its functional architecture is divided into four layers: device, network, support, and application, aiming to provide information services for both people and vehicles in underground parking lots to enhance user experience and management efficiency.	S2.14
ITU-T	(NEW) YSTR. SemComm.IoT	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17960	This Technical Report specifies the requirements and architectural framework for semantic communication services in IoT and Smart City & Community.	S2.18
ITU-T	(NEW) Y.4463	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19073	Recommendation ITU-T Y.4463 is a framework of the delegation service for transferring ownership (i.e., access rights to the Internet of things (IoT) devices) among authorized IoT devices. This Recommendation gives an overview and types of delegation service in IoT environment. It also describes the requirements and architectural models of delegation service.	S2.6
ITU-T	(NEW) Y.4499 (ex Y.UIM-cs-framework)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17944	Recommendation ITU-T Y.4499 specifies a framework for urban infrastructure monitoring based on crowdsourcing, including requirements, functional architecture, common procedures, as well as security and privacy considerations. Urban infrastructure includes the physical facilities and systems that a city must have for its operation and development. It has the characteristics of large quantity, wide distribution and high management difficulty. Crowdsourcing is the practice of engaging a group of people for a common goal. It can provide a scalable and financially viable way to monitor urban infrastructure. Comment: -	S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4503 (ex Y.IoT-CRE-fr)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18466	The Internet of Things (IoT) brings a diverse range of devices to the network, which are managed by rule-enabled IoT platforms that react to events dynamically and automatically. However, the heterogeneity of the IoT networks makes it challenging to deploy consistent rule scenarios across multiple platforms due to differences in protocols and data formats. The IoT rule agent is a platform that implements the framework of common rule enablement. The agent is deployed in the proxy layer to bridge clients and devices in heterogeneous IoT networks. Between different IoT networks, the heterogeneity of the platforms is handled by the agent to deliver the corresponding format of rule profile to the destination platform through the platform-specific protocol. The agent includes the device proxies to enable the heterogeneous rule profiles to be a common format and registered through the rule registry for the further deployment process. For deploying the rules to the heterogeneous IoT platforms, the device proxies translate the common format to platform-specific style and deliver to the corresponding platforms. In the agent, each device proxy only considers the corresponding IoT network to perform translation and deployment. Based on the agent, the heterogeneous IoT platforms operate the common rule scenario although heterogeneous rules are delivered to the environment. This Recommendation specifies a framework of common rule enablement for intelligent IoT services in heterogeneous IoT platform environments.	S2.1, S2.7, S2.14, S2.15
ITU-T	(NEW) Y.4504 (ex Y.SF-prediction)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18465	As the artificial intelligence (AI) technology develops and begins to be applied to various fields, enhanced internet of things (IoT) services using the AI technology are being developed. Machine learning, the core of the AI technology, has been mostly researched in the direction of increasing the accuracy of inference. To apply the AI technology into real fields and to provide intelligent IoT services, the AI services must be operated at a level that can be provided to customers effectively. It is needed to study the technologies to efficiently provide the AI services by focusing on inference(prediction) rather than training(learning).	S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This draft Recommendation describes the service framework in terms of prediction for intelligent IoT services by reflecting the development of the AI technology and the requirements from the market. To do this, this draft Recommendation introduces the concept of service framework of prediction for intelligent IoT and the requirements. And this draft Recommendations describes a functional architecture of service framework of prediction for intelligent IoT.	
ITU-T	(NEW) Y.4508 (ex Y.DPM-alm-fra)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18467	There are many Internet of things (IoT) platforms to process and manage same IoT data in different stages and in different areas. In traditional solutions, each of the IoT platforms usually stores its activity logs for processing and managing IoT data (IoT DPM) into its storage separately. Those activity logs are separated and managed by the IoT platforms respectively. Therefore, the accessibility and trustworthiness of those activity logs are not guaranteed. In this case, it is uneasy to trace activities about IoT DPM in full lifecycle for the activity logs are stored and managed by different IoT platforms. In order to trace activities about IoT DPM, different IoT platforms may use same activity log storage and related functionalities. Activity logs management (ALM) enabled by blockchain technologies provides functionalities to manage activity logs for IoT DPM in full lifecycle across IoT platforms. Different IoT platforms can save activity logs of IoT DPM into the trustworthy shared storages via the ALM for IoT DPM individually. And then when they read activity logs of IoT DPM via the ALM, they can get all the relevant activity logs of IoT DPM in full lifecycle from the trustworthy shared storages via the ALM for IoT DPM, if authorized. The ALM and the trustworthy shared storages are based on blockchain technologies and can keep the activity logs un-tampered. The ALM can facilitate the IoT platforms to store and trace activity logs of IoT DPM in full lifecycle transparently and trustworthily. This Recommendation presents a blockchain-based activity logs management for IoT data processing and management, and specifies its characteristics, functional requirements and architecture.	S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.4706 (ex Y.dem-IoT)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18743	The Internet of things (IoT) devices in the power transmission and transformation equipment can meet the demand for comprehensive and accurate data acquisition of power transmission and transformation equipment. It is necessary to develop a data exchange model for enable applications, sharing, coordination when constructing the system for power transmission and transformation equipment based on IoT. This Recommendation provides the requirements and model of IoT data exchange in power transmission and transformation equipment.	S2.3, S2.8
ITU-T	(NEW) Y.AIoT-dfs-arc	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19626	Data fusion service (DFS) is a converged data service in artificial intelligence of things (AIoT), which merges, combines and integrates metadata (not raw data) from different data resources (such as IoT devices, IoT systems, databases, cloud data platforms) into a coherent form, and provides data processing and management (DPM) capabilities to data consumers (such as for machine learning model training). The DFS can be enhanced by knowledge database (such as relational, graph), artificial intelligence (AI) and machine learning (ML). The DFS dynamically collects metadata (not raw data) from different data resources and make intelligent data catalogs in real-time by using AI/ML and knowledge database, and provides smart data provision capability to allow data consumers in AIoT to access data with QoE/QoS and security assurance. The DFS supports smart data integration capability. By using the DFS, the data organizations and consumers don't need to integrate and bring raw data together from different data resources. The DFS can enable organizations in AIoT to unify their disparate data systems, improve data governance capability, provide intelligent data accessibility and integration across multiple data platforms, and to enhance data collaboration within organizations. This draft new Recommendation specifies the data fusion service in artificial intelligence of things (AIoT), and provides relevant technical characteristics, functional requirements, reference architecture and capabilities of the data fusion service in AIoT.	S2.1, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.AIoT-dpsm	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19627	Smart manufacturing with Artificial Intelligence of Things(AIoT) integrates advanced technologies like AI to transform manufacturing and production processes. AIoT enables smart manufacturing in high level intelligence and autonomous. Data processing for smart manufacturing with AIoT improves production efficiency, reduces operational costs and enhances quality control by enabling real-time data processing based on the data collected from smart manufacturing environments. This Recommendation describes the requirements and framework of data processing for smart manufacturing with AIoT.	S2.3, S2.14, S2.15
ITU-T	(NEW) Y.AIoT-fr	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19624	The Artificial Intelligence of Things (AIoT) is the combination of artificial intelligence (AI) technologies with the Internet of Things (IoT) infrastructure to achieve more efficient IoT operations, improve human-machine interactions and enhance data management and analytics, but not limited to. From a comprehensive review of existing standardization efforts on AI and IoT, this draft Recommendation describes concepts, characteristics, technical features and approaches of AIoT. Then, it presents a conceptual model for AIoT.	S2.3, S2.14, S2.15
ITU-T	(NEW) Y.AIoT-FRA	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19625	To meet the targets of the Paris Agreement, telecom operators, like other industries, need to set targets for emission reduction to arrive at a net zero situation as reported in Recommendation ITU-T L.1470. For a situation in which network traffic will increase, this Recommendation defines a key performance indicator (KPI) useful to evaluate network emission and give an indication on how a network can reduce its emission due to energy usage. Recommendation ITU-T L.1333 defines a KPI called network carbon intensity energy (NCIe); it also defines how to apply the Recommendation: which part of the network is covered and how to calculate the metric continuously in network evolution. This Recommendation also defines the correlation between the carbon intensity indicator and energy efficiency metric. The carbon KPI defined in this Recommendation refers to the energy efficiency metric defined in Recommendation ITU-T L.1331.	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.cii (ex Y.rrm-data)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17900	This Recommendation specifies requirements and reference model of IoT related data from city infrastructure. The scope of this recommendation includes: –Overview of IoT related data from city infrastructure –Requirements of IoT related data from city infrastructure –Reference model of IoT related data from city infrastructure All content related to data collection, storage, retrieval and delete covered in this document is recommended to conducted in accordance with the laws and regulations of the country or region where the standard is used.	S2.1, S2.7, S2.14
ITU-T	(NEW) Y. CL-EDM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18463	This draft Recommendation specifies an energy data model of the city-level energy management platform (CL-EMP) to support building energy services and to share energy data with other city platforms for integrated city energy services in a smart sustainable city. It describes requirements, energy data model and energy data sharing. The energy data model defines what data is shared to support the integration of the CL-EMP and other city platforms. As a result, the model enables a variety of integrated city energy services in which multiple city sectors are linked.	S2.1, S2.8
ITU-T	(NEW) Y.CSDL	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18744	Building up distributed learning mode for crowdsourced system and enhance the crowdsourced service data security is important. The distributed learning mode can effectively solve the data security problem in the crowdsourcing process. The crowdsourced raw data will be computed on the distributed worker node and only encrypted intermediate computation result will be transferred to the crowdsourced platform. Besides, compared with the traditional crowdsourced systems utilizing the centralized computation mode, which was defined in ITU-T Y.4217, the realization of crowdsourced system based on distributed learning can also provide intelligent cooperation capabilities between crowdsourced resources and reduce bandwidth consumption and transmission time consumption. This recommendation specifies the requirements and framework for crowdsourced system based on distributed learning in order to solve the distributed model parallelism and data parallelism issues for complex crowdsourced task, crowdsourced nodes communication strategy under distributed learning, coordination mode of heterogeneous models and data.	S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.DM-SLF	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18470	Smart livestock farming (SLF) is a convergence service where Information and Communication Technologies (ICT) are applied into the livestock value chains. Apart from ICT technology, for a more productive and sustainable production smart livestock it is highly required to integrate various domain-specific information; examples of such information include precision livestock farming, management information systems, stockbreeding, and transportation. In order to integrate various domain-specific information, a well-defined data model is required. The well-defined data model can accelerate a number of new smart livestock related services as well as AI, data acquisition. Because it can facilitate automatization, interoperability and composability for the IoT applications and AI. For this purpose, this draft Recommendation defines data entities required for smart livestock service, their relationship, and then it addresses conceptual data model of smart livestock farming service.	S2.1, S2.14, S2.15
ITU-T	(NEW) Y.DSE-LISF	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19630	Artificial intelligence has been growing rapidly through deep learning technology, and large amounts of training data are needed to create accurate learning models. To overcome this problem, it has become necessary to share and exchange not only training data but also the learning models (e.g., federated learning model). Additionally, federated learning may be used to collect data from multiple IoT devices and to share and collaborate a learning model with the assistance of a server via exchanging model parameters rather than directly sharing decentralized datasets, which can break data islands and meanwhile bring the advantage of data privacy protection and legal compliance. Nevertheless, the problem of cultural and social bias in the training data itself still needs to be resolved. This draft Recommendation specifies the data (i.e, sensing data, management data and learning model) sharing and exchange principles between a server/edge system and IoT devices equipped with the lightweight intelligent software framework (LISF) that supports Internet of things (IoT) applications requiring intelligent processing and enables such processing to work on resource-limited IoT devices. This draft also identifies general requirements and provides a functional architecture for the data sharing and exchange based on the LISF.	S2.1, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.EDSS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19632	The rapid development of smart grids and the increasing deployment of IoT devices have resulted in a significant increase in electricity data generation (including consumption data, generation data, grid status data, etc.), which is collected and transmitted by IoT devices such as smart meters, sensors, and smart appliances. Efficient utilization of electricity data can lead to substantial benefits such as optimizing grid operations, enhancing energy efficiency, regulatory compliance and reporting, infrastructure planning and investment and improving customer services. However, the collection, storage, and sharing of electricity data pose significant challenges, particularly in terms of privacy and security. This draft new Recommendation introduces the framework, requirements and use cases of electricity data sharing system, and aims to establish a robust system for the secure and privacy-preserving sharing of electricity data. This framework leverages advanced techniques to ensure that data privacy is maintained throughout the data lifecycle, from collection to processing and sharing.	S2.3, S2.6, S2.8, S2.10
ITU-T	(NEW) Y.Interop-DPM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19633	SG20 has carried out a considerable amount of work on data interoperability from a technical point of view with many recommendations on different aspects of this topic. However, without a clear understanding of how to achieve semantic and operational interoperability the impact of the work may be limited. ITU has developed a foundational piece of work on this topic in FG-DPM. Other work has been done elsewhere, including the European Interoperability Framework for Smart Cities and Communities. This work would build on these to provide a framework for interoperability that sets technical interoperability alongside, for instance, semantic and operational interoperability. The U4SSC report "Redefining smart city platforms: Setting the stage for Minimal Interoperability Mechanisms" points out that: "Interoperability is one of the main challenges – and opportunities – in the development of smart sustainable cities and communities, using digital technologies to become more resilient, liveable and attractive for inhabitants and businesses.	S2.3, S2.7, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
			"The goal is to develop platforms that can allow key stakeholders, including govern-ments, businesses, knowledge institutions and inhabitants, to communicate and work together across domains. The key to achieving this goal is in defining modular and scalable, multi-layered ICT solutions to enable cross-domain interoperability, moving beyond existing siloed solutions that address specific challenges such as improvement of traffic flows, surveillance, smart lighting, among others. The report goes on to say that: "It is also important to recognize that interoperability is not just related to digital technology. The GridWise Architecture Council's eight-layer stack can help in understanding the context for determining interoperability requirements and defining exchanges of information. The Gridwise eight layer stack highlights that iteroparity is needed, not simply to cover technical issues, but also semantic, operational and regulatory. This Recom-mendation would explore those aspects of interoperability that are not usually the focus of SG20 deliverables and would pro-vide guidance as to how smart cities and communities could address the organisa-tional and other barriers to interoperability of data.	
ITU-T	(NEW) Y.IoT-3DMS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19072	This draft Recommendation defines the requirements for providing 3D mod-el-based monitoring services and describes functional capabilities for a 3-dimensional model monitoring system by utilizing IoT sensing metadata. Three dimensional modelling is essential technology for IoT monitoring service, especially facilities to access difficulties by humans. For example, monitoring high-risk building structures, bridges, dams, monitoring natural environ-ments, etc. This 3D modelling is important to predict potential risks (falling, peeling, cracking, etc.) in such environment. And, 3D model-based capabilities are to provide IoT monitoring services in smart city envi-ronments	S2.3, S2.14, S2.25.9
ITU-T	(NEW) Y.IoT-IIEC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19628	Framework of the integrated intelligent IoT service based on multi edge computing	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-IWAT	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19629	Vehicles in the transportation are equipped with a various IoT devices, which can be defined as things based on agent like software in terms of IoT. These IoT devices collect and generate various types of IoT data related to IoT-based smart city services in real time. In addition, the things in the transportation can be interworked with external IoT services to provide new intelligent IoT services by fusing them with the collected or generated IoT data. Therefore, the interworking of IoT data between things in the transportation and intelligent IoT services in the smart city can facilitate the development of various intelligent IoT convergence services. In particular, the smart city is equipped with an infrastructure that enables things to send and receive IoT data to and from various things in the smart city through V2X (Vehicle to Everything) communication. Therefore, it is possible to deliver and exchange data between things in the transportation, and to configure new intelligent IoT convergence services through data fusion between them. To this end, this draft Recommendation introduces the concept of interworking with agent-based transportation for intelligent IoT services and the requirements needed to configure intelligent IoT convergence services through it. And this draft Recommendation also describes the functional architecture, functional components, and interactions between them.	S2.3, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.KCI-IM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19631	The Internet of Things (IoT) is characterized by a massive number of devices, complex and variable network structures, and highly specified and diverse service scenarios, which present significant challenges for IoT management. According to ITU-T Y.4000, the IoT management capabilities can be categorized into generic management capabilities and specific management capabilities. Essential generic management capabilities in the IoT include device management, local network topology management, traffic and congestion management, service management, etc. Specific management capabilities are closely coupled with application-specific requirements of different industries. Knowledge construction and implementation techniques can enhance the management efficiency and effectiveness of devices, networks and services within Internet of Things (IoT). Utilizing knowledge technologies can more comprehensively mine and extract hidden information from multimodal data collected from IoT devices, networks, and vertical industries. Through the process of knowledge construction and implementation, the massive data can be transformed into multidimensional and multi-layered associated knowledge, which can effectively support the various needs of IoT management along with other AI technologies.	S2.7, S2.22
ITU-T	(NEW) Y.metadata-EPI (ex Y.Sup.metadata-EPI)	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19074	The extensive deployment of IoT-based electric power infrastructure monitoring systems has improved the intelligence and digitization of power systems. However, due to the uneven nature of systems, the suitability and performance vary greatly when monitoring a specific event, which increases the difficulty of efficient application of monitoring system. Constructing metadata of IoT-based electric power infrastructure monitoring system, can effectively enhance the data management and application capabilities of electric power infrastructure monitoring system, and improve more transparent, intelligent, and advanced energy services in smart cities.	S2.1, S2.7, S2.8

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.MIM-based-arch	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19634	Recommendation Y.MIM will be proposed for consent in the July 2024 SG20 plenary meeting. Once this is done, the next step would be to develop a minimal architectural framework that would strike a balance of precision in the technical specifications, neither over- nor under-specifying the requirements. The goals of a Y.MIM-based architecture framework for a digital ecosystem for cities and communities would be to ensure that the capabilities of interoperable data platforms take into account both the functional and the non-functional requirements needed to implement the minimal interoperability that cities and communities need to deliver a prosperous, sustainable, and inclusive future for their citizens. The fundamental perspective is that of the technical capabilities required for minimal data interoperability. This focus would background many implementation aspects, e.g., related to specific software and hardware stacks, and would allow great flexibility when it comes to adapting concrete deployment and integration to a local context. It would also be based on a realisation from current experiences that establishing data spaces on a minimal but sufficient common ground can be a catalyst to deliver mainstream trusted services for cities and communities in a connected world. The requirements for interoperable city data platforms would lead to specifications that ensure that the platforms are reliable, durable, future proof and efficient so that the city can build on the platforms and foster further innovations and evolution. These specifications would also ensure that the platforms can: extend to a 'system of systems' with all relevant digital means of a community, scale to the needs of the cities and communities; and guarantee privacy and security by design, making the platforms trustworthy. Open-source development and the involvement of communities are powerful methods in order to guarantee transparency and consequently trust in the platforms for public operators. This particular aspect will be particularly relevant when injecting algorithms based on AI mechanisms into the platforms. The implementation of minimal interoperability provides the common technical ground that cities and communities need to enable choice, flexibility, value for money and independence, through avoiding vendor lock-in.	

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			The architectural framework would support formal, de-facto and emerging standards, in order to ensure they are future-proof and stable. The trustworthiness and the interoperability of the platforms addresses the triple baseline of social, environmental, and economic benefits, and supports strategic aims such as the United Nations Sustainable Development Goals.	
ITU-T	(NEW) Y.Smart-Building-Integration : Framework	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19071	This Recommendation will set the framework for interoperability to ensure that different building systems can communicate with smart city functionalities. It will enable the seamless integration of smart buildings with broader smart city infrastructure. This Recommendation will provide guidelines for data exchange, communication protocols and system interfaces, allowing smart buildings to connect with transportation systems, utilities, emergency services, and other city-level services. By developing this Recommendation, cities can benefit from a harmonized approach to smart building implementation and advance the adoption of smart technology in the urban environment.	S2.7
ITU-T	(NEW) Y.SPDM-reqts	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19636	Smart Pest and Disease Management (SPDM) is an approach to managing pests and diseases in agriculture or other settings that emphasizes the use of multiple techniques in a coordinated manner. The goal of SPDM is to minimize the damage caused by pests and diseases while minimizing risks to human health, the environment, and non-target organisms. Existing pesticide control systems based on Internet of Things can minimize the impact of chemicals on human health as well as reduce labour but have difficulties in achieving optimal pest and disease control. In order to efficiently provide SPDM service by enabling sophisticated data analytics and the widespread adoption of AI-powered surveillance systems, a large amount of data is needed to be involved. However, this data is difficult to collect because of lack of meaningful existing data and lack of common data formats. In order to efficiently manage and analyze vast amounts of data and to create various services based on the analyzed data, a standardized data model including data collection and management system is required.	S2.7, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			In particular, compatibility of data generated and consumed by heterogeneous devices must be guaranteed to ensure interoperability between devices of heterogeneous vendors. However, the SPDM data model currently used in the market is vendor-specific, and thus interoperability between devices is not guaranteed. In other words, data sharing and real-time data communication between heterogeneous devices is not supported. For data interoperability, this draft Recommendation defines requirements and reference model of data for SPDM service.	
ITU-T	(NEW) YSTR. dscm	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18468	With the continuous transformation and upgrading of digital economy, data sharing becomes the driving force and also bottleneck to further generate data value. It is crucial to ensure that data sharing among various stakeholders is secure and trustworthy in smart cities and communities. Representations of security and trustworthy factors and their enforcement are two main challenges in trusted data sharing. To address the aforementioned challenges, this technical report presents the life-cycle of data sharing. This technical report analyses data sharing control models regarding data transmission, data storage, data usage and data destruction, and illustrates use cases.	S2.1, S2.6, S2.7, S2.10
ITU-T	(NEW) YSTR. GenAI-Sem-Interop	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19635	GenAI can be utilised for a broad range of technical and non-technical challenges smart cities and communities face. One aspect of particular importance in advancing their digital ecosystems is semantic interoperability. Making systems interoperable is key to reap the benefits of having digital ecosystems in the first place, and the use of proprietary systems, outdated/non-conformant standards, and/or lack of technical expertise creates unnecessary challenges for smart cities and communities. Although large language model (LLM) output quality needs to be closely monitored, in particular for complex operations, GenAI offers an increasingly robust approach for improving semantic interoperability, helping to connect systems that are otherwise (partially) incompatible. When using LLMs in live cloud environments, i.e. to continuously transform/harmonise data, additional security implications need to be considered.	S2.1, S2.14, S2.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			This technical report aims at exploring how GenAI is already used to solve semantic interoperability challenges within smart cities and communities – and how reliable and secure existing solutions are; finding commonalities among existing solutions; and recommending normative work items to standardise GenAI usage for increasing interoperability across decentralised smart city and community data infrastructure, helping to process, manage, and share data across digital services such as digital twins and metaverse applications.	
ITU-T	(NEW) Y.CIP	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19637	Chemical Industrial Parks (CIPs) are specialized zones which contains a diverse range of chemical factories. Leveraging exceptional infrastructure and shared services within the parks, CIPs aim to streamline operations and facilitate efficient business operations within the chemical sector. This management style means to enhance energy and resource efficiency, environmental performance, and economic competitiveness. However, as a high concentration of those hazards in a limited space, CIPs may cause a chain reaction in the event of an accident. Once an accident happens, it may result in large scale loss of life and property. Thus, emergency response in CIPs requires more proactive measures to prevent accidents. This document focuses on establishing a set of comprehensive application requirements designed to mitigate risks and strengthen emergency response capabilities within CIPs. It details overview of emergency response in CIPs, requirements of metaverse-based emergency response in CIPs, and framework of metaverse-based emergency response in CIPs. It provides guidance to improve situational awareness, response times, and overall safety through more dynamic and interactive emergency response.	S2.3, S2.8, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) YSTR. DIC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19638l/en	With the advancement of artificial intelligence application based on IoT, it introduces new features like ubiquitous intelligence perception, cloud-edge collaborative computing, distributed machine learning, and more. Physical computing resources are required to match the new intelligent IoT characteristics of terminal intelligence, especially for the IoT ubiquitous intelligence and distributed intelligence. It is necessary to have a computing architecture that is consistent with the development of the intelligent computing for Internet of Things. This technical report describes the status of the distributed intelligent computing (DIC) based on IoT. It also specifies gaps and challenges in existing work, as well as the reference framework and typical functional entities which would support the DIC.	S2.3, S2.14, S2.15
ITU-T	(NEW) Y.bsis-sec	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19640	Base stations refer to outdoor stations in smart cities that provide public services, such as power transmission stations, communication base stations, weather monitoring stations, and water quality monitoring stations. These stations are typically located outdoors and are susceptible to damage due to weather changes and material aging. Therefore, they require timely and periodic inspections. Unlike traditional IoT security, inspection services for these base stations face significant and unique security threats. The large number and widespread deployment of UAVs, especially with remote docker, resulting in a wide exposure surface for information security and making the service process vulnerable to attacks. Such vulnerabilities could lead to data leakage, including the unauthorized access to sensitive images of restricted areas, which poses significant security risks overall. This draft new Recommendation focuses on security requirements and capabilities for base station inspection (BSI) services using unmanned aerial vehicles (UAVs). It aims to enhance the information security protection when conducting BSI services using UAVs. By doing so, it aims to prevent information security incidents such as errors, malicious intrusions, and data tampering, thereby ensuring the overall security of base stations and maintaining the quality of public services in smart cities.	2.6, 2.7, 2.10, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.iepi-dm-sa	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19081	Security assessment for data management encompasses various aspects of the IoT-EPI data lifecycle, including data collection, transmission, storage, processing, and services. By evaluating the security capabilities at each stage, it aims to demonstrate the overall security level, thereby mitigating security risks associated with IoT-based electric power infrastructure and ensuring the provision of efficient and secure data services in smart cities. This draft new Recommendation specifies security assessment framework and security assessment factors for data management for IoT-based electric power infrastructure.	S2.6, S2.8, S2.9
ITU-T	(NEW) Y.IoT-acs-fra	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18740	There are many big challenges for Internet of things (IoT) platforms in decentralized environments to make trust among the IoT entities (such as IoT devices, IoT services, IoT gateways, and other IoT resources) when they interact with each other. The traditional access control solutions of IoT platforms (such as perimeter control, password authentication, virtual private network) could not fully cope with those challenges, especially when IoT entities are deployed in decentralized environments. Zero trust (ZT) is one type of cybersecurity principles, which provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised [b-NIST SP 800-207]. In ZT-based access control solutions, it is no longer to determine access rights, by location and security domain for IoT entities to discover and access other IoT entities in same or different IoT platforms. It is required to be determined for any requests to discover and access to any IoT entities in IoT platforms. Therefore, ZT-based access control solutions are apt to IoT platforms in decentralized environments. This draft new Recommendation introduces an access control service of IoT platform in decentralized environments as enabled by zero trust technologies, and specifies its characteristics, functional requirements and architecture.	S2.6, S2.7, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-IADS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19643	This draft new Recommendation proposes an Intelligent Anomaly Detection System for IoT (IADS), which leverages advanced technologies to identify and mitigate anomalous behaviors in IoT-based systems. This system utilizes a hybrid approach, combining rule-based security mechanisms for known attacks with machine learning techniques to detect and adapt to new anomalies. This dual-method approach enhances the security of IoT applications and systems by bringing protection closer to the IoT devices. The IADS framework includes comprehensive guidelines and best practices designed for policymakers, developers, and researchers involved in IoT deployment and management. It addresses various aspects crucial for implementing robust anomaly detection systems. This draft new Recommendation aims to establish a standardized framework that promotes the deployment and management of intelligent anomaly detection systems in IoT environments. By offering detailed guidelines and best practices, it seeks to bolster the security, reliability, and efficiency of IoT applications and systems, thereby fostering greater trust and adoption of IoT technologies across various sectors.	S2.6, S2.7, S2.10
ITU-T	(NEW) Y.IoT-Smartcity-Risk	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17916	This recommendation contains a reference framework for the process of cybersecurity risk management of IoT ecosystems in smart cities, which provides a series of key risk indicators (KRI). So, city officials can assess the level of risk in IoT ecosystems that are used in the development of a smart city, in order to support their sustainability and resilience goals. The Guidelines include: To describe the elements of an IoT system and analyzing the contribution of each one to the total value of cyber risk in a smart city environment. To analyze the risk factors that should be considered when applying a cyber risk management methodology in IoT systems in smart city environments. To assist governments at all levels to do self-evaluations and encourage them to share the results with others.	S2.6, S2.10

SDO	Specification			Relevant AIOTI/ EUOS identified IoT chal-lenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Sec-outdoor	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19075	As part of the outdoor electric power infra-structure monitoring system, the IoT man-agement platform has various capability requirements, with security requirements being a critical aspect. Classifying the se-curity requirements and capabilities of IoT management platform can enhance the information security protection capabilities of the IoT management platform during its operation and maintenance, prevent-ing information security incidents such as errors, tampering, or malicious intrusions from affecting the overall safety of smart city outdoor electric power infrastructure. This draft new Recommendation specifies security requirements and capability of IoT Management platform for outdoor electric power infrastructure.	S2.6, S2.7, S2.10
ITU-T	(NEW) Y.sup. access-sec	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19641	IoT-based electric power infrastructure monitoring system (IoT-EPIMS) relies on a large number of sensing devices for data acquisition and operational control. With the digitalization of the electric power in-dustry, the number and diversity of sensing devices have been increasing, especially different security requirements stemming from the different electric power services. To enhance the security of IoT-EPIMS, the security risks and security framework for sensing devices to access IoT-EPIMS, secu-rity requirements for three types of sensing devices to access IoT-EPIMS and use cases are supplemented to ITU-T Y.4221.	S2.6, S2.7, S2.10
ITU-T	(NEW) Y.Sup. SRS-SR :	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19642	Retail stores are one of the important application fields of the IoT. The usage of IoT enables "smart retail stores". More and more smart retail stores rely on various IoT devices and are closely integrated with electronic shelf labels, product manage-ment system, etc., resulting in complex network structures and diverse appli-cation in smart retail store. This Supple-ment focuses on the security threats and requirements of IoT based smart retail stores. The purpose is to improve the security protection capability of the smart retail store systems during operation and maintenance.	S2.6, S2.7, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y. Supp-Imp-CSIADE	https://www.itu.int/rec/T-REC-L.1410-201412-I/en	Recommendation ITU-T Y.4811 specifies a converged service for identification and authentication for IoT devices in decentralized environment (CSIADE), and provides its common characteristics, general requirements, functional architecture, main capabilities and procedures. CSIADE can facilitate IoT devices and IoT services to identify and authenticate each other in IoT decentralized environments when they use same or different types of decentralized IoT identification and authentication solutions. This draft Supplement provides a set of implementation guidelines to perform the CSIADE defined in Recommendation ITU-T Y.4811, including that of CSIADE as an independent system and as subsystem embedded in IoT devices and services, to improve compatibility when using self-resolving identities for IoT devices and services, to use self-controllable storage to manage identities of IoT devices and services, to support online and offline endorsement for the identity of IoT devices and services, and to support multiple solutions of identification and authentication in CSIADE. This draft Supplement is to promote the implementation and deployment of CSIADE.	S2.6, S2.7, S2.17
ITU-T	(NEW) Y.uas-dc-fr	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19083	The power system utilizes IoT-based electric power infrastructure to collect, aggregate, and distribute IoT data, which is used to enhance the digitization and intelligence of energy and electricity, has become a development trend. In terms of data collaboration, an entity is required to get data from multiple power information systems. However, the authetication methods of the power information systems varies , as a result, entities are required to develop multiple functions to cope with corresponding authentication methods, which results in a high cost for development and maintainance . Therefore, a unified authentication service for data collaboration is required. The unified authentication service is deployed between entities and power information systems, and can be deployed in a centralized way for better efficiency or distributed way for security issues.	S2.4, S2.6, S2.8, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			It receives authentication requests from different entities with unified format, convert data format to adapt for target systems, distribute them to destinations and return information to entities.which reduces the development and maintainance cost. This draft new Recommendation specifies a framework of unified authentication service for data collaboration.	
ITU-T	(NEW) YSTR. IoT-IMS	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18473	To support complex IoT scenarios, identification management service of the IoT device is needed. The proposed identification management service of the IoT device can help IoT platform service providers to manage the access control of the IoT device for platform services. The main purpose of this proposed draft technical report is to help IoT platform service providers write identification data to IoT devices of different venders, and to help IoT platforms identify identification data from a variety of IoT devices. The requirements related to the modification and deletion of identification data in IoT devices are also included in the proposed draft technical report. The significance of this proposed draft technical report is to improve the operation efficiency of the IoT platform on the identification data of IoT devices, so as to reduce the time and money spent on the integration of IoT devices and platforms.	S2.17
ITU-T	(NEW) Y.DT-SSC-CVP	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19645	Digital twin technology has become a crucial component of smart city systems, and enabling urban planners and managers to simulate, analyze, and predict various scenarios of urban development by creating virtual replicas of the physical urban environment, offering intuitive tools for management and decision-making. Its foundation lies in providing a 3D model representation of objects in the physical world in digital space. However, the precision of 3D model representation varies in different digital twin systems, which equates to different precision levels of visualization for digital twin systems. This Recommendation established a unified digital twin visualization precision levels classification framework, which can assist decision makers identify the general requirements that different precision levels should meet, choose appropriate precision levels for the construction of digital twin systems, avoid unnecessary consumption of resource and cost. This can also promote the interoperability and comparability between different systems and projects.	S2.3, S2.14, S2.15, S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Evaluation-dfp	hhttps://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19644	At present, while many countries and cities worldwide recognize the importance of data as a factor of production and smart city initiatives, there exist disparities in the level of data quality evaluation and smart city maturity across different regions and municipalities. Thus, it is essential to develop standards and guidelines for evaluating the quality of data as a factor of production that underpin various smart city applications and services. Data plays a crucial role in smart cities, enabling data-driven decision-making, optimized urban planning, efficient resource allocation, and improved public services. However, the quality of data, such as completeness, accuracy, timeliness, consistency, and interoperability, can significantly impact the effectiveness and reliability of smart city solutions. This draft Recommendation focuses on the requirements for quality evaluation of data as a factor of production for smart sustainable cities. It will benefit city administrators, stakeholders, and citizens by ensuring the high quality of data across domains . By establishing comprehensive standards and best practices for evaluating data quality, this work item will facilitate the integration and harmonization of data from multiple sources, enhance the reliability of data-driven decision-making processes, and foster innovation and collaboration among smart city stakeholders. Evaluating and improving the quality of data is crucial for maximizing the potential of data, increasing operational efficiency, and creating a more livable, inclusive, and sustainable urban environment for citizens. This work item will ultimately contribute to the effective and efficient development of smart sustainable cities worldwide.	S2.1, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.Evaluation-SE	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19086	IoT-enabled smart education systems leverage extensive digitalization, interactive and smart services to substantially enhance learning experiences, teaching efficiency, and adaptability of content. The capabilities for these systems have direct impacts on the improvement of educational quality. The evaluation of these capabilities plays a significant role in effectively advancing the application of smart education and guiding the evolution of smart education system platforms. The establishment of comprehensive and unified key performance indicators for the assessment of the capabilities in IoT-enabled smart education can promote the widespread adoption of smart education and guide the evolution of smart education system platforms. This recommendation specifies the evaluation of capabilities for IoT-enabled frameworks of smart education. It provides the key performance indicators of capabilities evaluation based on the dimensions of user experience and engagement, digital information management, intelligent processing, rationality and reliability of information and algorithms, digital information sensing and acquisition for the smart education.	S2.14
ITU-T	(NEW) Y.Highway-KPI	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18476	This Recommendation gives a general guidance to cities and provides a set of key performance indicators (KPIs) related to the use of information and communication technology (ICT) in the context of highway traffic safety assessment (HTSA). This Recommendation can help assess highway traffic safety by offering a set of KPIs when identifying, analyzing and evaluating the highway traffic risk.	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.IoT-BEMS-af	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19088	IoT is already having a significant impact on the smart building sector. With the integration of the Internet of Things (IoT) into the field of building energy management system (BEMS), opportunities have emerged to enhance energy efficiency and reduce capital expenditures in buildings. Consequently, implementation and assessment of IoT infrastructure in BEMS has become crucial. Therefore, this contribution proposes a new work item, "Assessment framework of IoT infrastructure in building energy management system". This document provides an assessment framework and assessment factors for the IoT infrastructure of BEMS, taking into consideration an IoT reference model, with the aim of enhancing implementation efficiency for stakeholders.	S2.8, S2.24
ITU-T	(NEW) Y.KHI-PE	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18742	This Recommendation specifies the evaluation model of key health indicators and implementation methods for smart power equipment. Based on smart power equipment maintenance, operation and environmental information, and characteristic information of the same type of device, a health indicator quantitative evaluation model is established, which includes three steps of parameter type collection, performance / component collection, and comprehensive evaluation. The establishment of the health indicator evaluation model combines the accumulation of experience in equipment maintenance, and the health evaluation driven by intelligent equipment data. For the urban power equipment group, it provides the overall decision-making basis of equipment operation and maintenance and power grid risk management for the power supply management.	S2.7, S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.K-PEM-SM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18474	This criteria specifies technically oriented key performance indicators used in the life cycle of smart manufacturing. It provides the key performance evaluation framework, indicators and methods for digital transformation of manufacturing, quantitatively evaluate the value and benefits of digital transformation from the aspects of business innovation, operation optimization and sustainable development, provides a basis for city managers to make decisions and accelerates the process of digital transformation of manufacturing. It is designed as a practical tool for city managers, and all relevant stakeholders to study the performance and benefits of digital transformation of manufacturing from a technical perspective. Thus, it gives general guidance for accurately assessing the benefits of digital transformation and helping cities achieve sustainable development goals.	S2.3, S2.14
ITU-T	(NEW) Y.KPI-Flood	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17963	Flood disaster is a critical issue influencing the safety of a city. There are many kinds of flood prevention and mitigation measures, however, no comprehensive assessment of these measures is provided yet. This recommendation presents methodology of evaluating ICT based urban disaster prevention and mitigation capability for floods. It provides a set of key performance indicators to quantitatively assess the flood disaster prevention and mitigation capability of cities.	S2.3, S2.14
ITU-T	(NEW) Y.QE-DMI-SSC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18475	As the foundation of smart sustainable cities (SSC), industry has become a critical element in SSCs. With the advancements in information technology, industrial digital twins are driving industrial innovation. The industrial digital twin is the real-time connection and interaction between industrial digital models and industrial assets, such as products, production facilities, transport vehicles, etc. Thus, the industrial digital model is an abstract representation of real industrial assets, which is the foundation of the industrial digital twin. At present, the digital model in industry is widely used for the simulation, analysis and optimization of industrial products. As the digital representation of industrial knowledge mechanisms, they reflect the structure, knowledge and spatio-temporal characteristics of industrial products.	S2.3, S2.14, S2.23

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			Therefore, the quality of digital models of industrial products is essential for the promotion of industrial development, and helps in the construction and management of SSC. This draft new Recommendation comprehensively evaluates the quality of industrial digital models from three aspects:the digital model construction quality, the digital model application quality and the digital models cost-effectiveness. It aims to provide all relevant stakeholders with a practical assessment tool that gives general guidance for accurately assessing the quality of digital models in industry to help improve industrial product quality.	
ITU-T	(NEW) Y.SN-PG-ref	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19646	Traditional power grid is undergoing profound transformations, with large-scale renewable energy generation and distributed clean energy increasingly becoming dominant. As high proportions of clean energy and a massive number of intelligent power distribution terminals equipped with power sensing technologies are integrated, the types, frequency, and quality of data collected by power grid sensing information are enhanced. The volume and dimensions of data are experiencing exponential growth, forming a vast sensing network in power grid. The Internet of things (IoT) as a relatively new technology is transforming sensing network in power grid to further enhance sensing data transformation services. However, this transformation concomitantly creates a need for effective reliability evaluation frameworks of sensing network in power grid. This recommendation specifies the reliability evaluation frameworks of sensing network in power grid. Based on existing network evaluation standards, the main factors of the reliability evaluation are stability, fault-tolerance, maintainability and security. This framework provides a comprehensive reference for reliability evaluation of sensing network in power grid.	S2.3, S2.6, S2.7, S2.8

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y.SSC-NGUM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17914	Smart and sustainable cities and communities measure their performance through well-defined Key Performance Indicators (KPIs). Measurement of these KPIs rely on collected data and their accuracy. Next Generation Urban Measurements methodology described in this Recommendation uses innovative sensing techniques to collect extensive and more frequent city data from various locations in the city at different times. Hence data for city KPIs such as air quality, noise pollution, road quality and traffic congestion, among others, may potentially be collected by using the Next Generation Urban Measurements methodology described in this Recommendation. This Recommendation provides a structured step-wise methodology to help cities apply the Next Generation Urban Measurements techniques. It also indicates big data implications and related high-level building blocks required for implementing Next Generation Urban Measurements.	S2.1, S2.7, S2.14
ITU-T	(NEW) Y.Sup. MM-EDMC-SSC	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18741	As the basic carrier of manufacturing activities, the digital management capability of equipment is of great significance to the value creation activities of industry in SSC. With the rapid development of advanced information technologies such as the Internet of Things, big data and artificial intelligence, the intelligent level of equipment has been continuously improved. Enhancing the digital management capacity of equipment contributes to improve production efficiency, reduce operation cost and increase economic benefits. Therefore, digital management of equipment provides a feasible way for urban innovation and sustainable development. This draft Supplement provides a maturity model of digital management capability of industrial equipment for SSC. The maturity model helps to identify the maturity levels, dimensions and guidelines of digital management capability of industrial equipment for SSC. It is designed as a practical tool for city managers and related stakeholders to study the effectiveness of digital management of equipment from resource, environment, operation and other dimensions. Thus, it provides overall guidance for assessing the maturity of digital management capability of industrial equipment and helping cities achieve sustainable development goals.	S2.1, S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) Y. Sup-NGUM	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17915	This draft Supplement provides practical use cases from real cities on how to measure selected city KPIs such as air quality, noise pollution, road quality, among others, by using the Next Generation Urban Measurements methodology described in ITU-T Y.SSC-NGUM. This draft Supplement complements the Recommendation ITU-T Y.4903/L.1603 which gives general guidance to cities and provides key performance indicators (KPIs) for smart sustainable cities (SSCs) to help cities achieve sustainable development goals (SDGs). Next Generation Urban Measurements methodology in ITU-T Y.SSC-NGUM uses innovative sensing techniques to collect extensive and more frequent city data from various locations in the city at different times. This draft Supplement will illustrate how real cities collect extensive amount of data from various locations in the city through fixed (e.g. buildings) and mobile units (e.g. taxis, satellites), at different times during the day (and the week), and will discuss how KPIs are measured by these cities. It will also illustrate the high-level architectures adopted by these cities to collect, store and process measurements data by using various technologies (e.g. IoT, AI).	S2.1, S2.7, S2.14, S2.15
ITU-T	(NEW) Y.Sup-Proc-SSC :	https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19089	Summary This draft Supplement will provide guidance on how to effectively procure and implement smart city solutions that are sustainable, resilient, and inclusive. It aims to provide practical procurement processes or steps to take throughout the digital data and technology buying cycle - planning, informing the market, evaluation and managing delivery. It will also delve into effective and efficient procurement during emergencies/ crises. This draft Supplement is based on the U4SSC report entitled "Procurement guidelines for smart sustainable cities".	S2.7, S2.14
ITU-T	(NEW) ITU-T Y Suppl. 76	https://www.intertekinform.com/en-gb/standards/itu-t-y-suppl-76-09-2023--1344020_saig_itu_itu_3342182/	Supplement 76 to ITU-T Y-series Recommendations surveys use cases related to smart agriculture from the perspective of, but not limited to: 1) smart greenhouse; 2) smart open field; 3) smart hydroponics; 4) smart livestock barn; and 5) smart agriculture data service.	S2.7, S2.14
ITU-T	(NEW) ITU-T FGMV-01	http://handle.itu.int/11.1002/pub/82047d78-en	Exploring the metaverse: opportunities and challenges (WG1- General)	S2.25.9
ITU-T	(NEW) ITU-T FGMV-02	http://handle.itu.int/11.1002/pub/822e1df0-en	Metaverse: an analysis of definitions (WG1 – General)	S2.25.9

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU-T FGMV-03	http://handle.itu.int/11.1002/pub/822e1f34-en	Guidelines to assess inclusion and accessibility in metaverse standard development (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.9, S2.25.10, S2.25.14
ITU-T	(NEW) ITU-T FGMV-04	http://handle.itu.int/11.1002/pub/822e20cf-en	Requirements of accessible products and services in the metaverse: Part I – System design perspective (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.9, S2.25.14
ITU-T	(NEW) ITU-T FGMV-05	http://handle.itu.int/11.1002/pub/822e20f7-en	Requirements of accessible products and services in the metaverse: Part II – User perspective (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.9, S2.25.14
ITU-T	(NEW) ITU-T FGMV-06	http://handle.itu.int/11.1002/pub/822f50e6-en	Guidelines for consideration of ethical issues in standards that build confidence and security in the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.10, S2.25.11
ITU-T	(NEW) ITU-T FGMV-07	http://handle.itu.int/11.1002/pub/822f50e7-en	Policy and regulation opportunities and challenges in the metaverse (WG7 - Economic, regulatory & competition aspects)	S2.12, S2.25.13, S2.25.14
ITU-T	(NEW) ITU-T FGMV-08	http://handle.itu.int/11.1002/pub/822f50e8-en	Design criteria and technical requirements for sustainable metaverse ecosystems (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.9, S2.25.12, S2.25.13, S2.25.14
ITU-T	(NEW) ITU-T FGMV-09	http://handle.itu.int/11.1002/pub/822f50e9-en	Power metaverse: Use cases relevant to grid side and user side (WG2 - Applications & Services)	S2.25.9, S2.25.13, S2.25.16
ITU-T	(NEW) ITU-T FGMV-10	http://handle.itu.int/11.1002/pub/822e2292-en	Cyber risks, threats, and harms in the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-11	http://handle.itu.int/11.1002/pub/822e22ae-en	Embedding safety standards and the user control of Personally Identifiable Information (PII) in the development of the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.10, S2.25.11
ITU-T	(NEW) ITU-T FGMV-12	http://handle.itu.int/11.1002/pub/822e22fb-en	Children's age verification in the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-13	http://handle.itu.int/11.1002/pub/822e2315-en	Responsible Use of AI for Child Protection in the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-14	http://handle.itu.int/11.1002/pub/822f50ea-en	Regulatory and economic aspects in the metaverse: Data protection (WG7 - Economic, regulatory & competition aspects)	S2.25.14, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-15	http://handle.itu.int/11.1002/pub/822f50eb-en	Accessibility requirements for metaverse services supporting IoT (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU-T FGMV-16	http://handle.itu.int/11.1002/pub/822f50ec-en	Accessibility in a sustainable metaverse (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.14
ITU-T	(NEW) ITU-T FGMV-17	http://handle.itu.int/11.1002/pub/822f50ed-en	Guidelines and requirements on interpreting in the metaverse (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.14
ITU-T	(NEW) ITU-T FGMV-18	http://handle.itu.int/11.1002/pub/822f50ee-en	Guidance on how to build a metaverse for all – Part I: Legal Framework (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.14
ITU-T	(NEW) ITU-T FGMV-19	http://handle.itu.int/11.1002/pub/822f50ef-en	Service scenarios and high-level requirements for metaverse cross-platform interoperability (WG5 - Interoperability)	S2.25.10
ITU-T	(NEW) ITU-T FGMV-20	http://handle.itu.int/11.1002/pub/822f50fd-en	Definition of metaverse (WG1 – General)	S2.25.9
ITU-T	(NEW) ITU-T FGMV-21	http://handle.itu.int/11.1002/pub/822f50fe-en	Principles for building concepts and definitions related to metaverse (WG1 – General)	S2.25.9
ITU-T	(NEW) ITU-T FGMV-22	http://handle.itu.int/11.1002/pub/822f50ff-en	Capabilities and requirements of generative artificial intelligence in metaverse applications and services (WG2 - Applications & Services)	S2.15, S2.25.5, S2.25.9
ITU-T	(NEW) ITU-T FGMV-23	http://handle.itu.int/11.1002/pub/822f5100-en	Considering online and offline implications in efforts to build confidence and security in the metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-24	http://handle.itu.int/11.1002/pub/822f5101-en	A framework for confidence in the metaverse (WG1 – General)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-25	http://handle.itu.int/11.1002/pub/822f5102-en	Near-term and long-term Implications for people in the metaverse (WG1 – General)	S2.25.9, S2.25.14
ITU-T	(NEW) ITU-T FGMV-26	http://handle.itu.int/11.1002/pub/822f5103-en	Requirements for communication between human-avatar languages in the metaverse (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.3, S2.25.5, S2.25.14
ITU-T	(NEW) ITU-T FGMV-27	http://handle.itu.int/11.1002/pub/822f5104-en	Guidelines for metaverse application in power system (WG2 - Applications & Services)	S2.25.13, S2.25.14, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-28	http://handle.itu.int/11.1002/pub/822f5105-en	Requirements for the metaverse based on digital twins enabling integration of virtual and physical worlds (WG4 - Virtual/Real World Integration)	S2.5, S2.25.4, S2.25.13, S2.25.15
ITU-T	(NEW) ITU-T FGMV-29	http://handle.itu.int/11.1002/pub/822f5106-en	Reference model for the metaverse based on a digital twin enabling integration of virtual and physical worlds (WG4 - Virtual/Real World Integration)	S2.15, S2.25.4, S2.25.13, S2.25.15

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU-T FGMV-30	http://handle.itu.int/11.1002/pub/822f5115-en	Overview of the application requirements of metaverse on emergency management in chemical industrial parks (WG2 - Applications & Services)	S2.25.9, S2.25.13, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-31	http://handle.itu.int/11.1002/pub/822f5116-en	Requirements, functional framework and capability of IoT for metaverse (WG3 - Architecture & Infrastructure)	S2.7, S2.25.7, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-32	http://handle.itu.int/11.1002/pub/824b4875-en	Overview of metaverse (WG1 – General)	S2.25.8, S2.25.9
ITU-T	(NEW) ITU-T FGMV-33	http://handle.itu.int/11.1002/pub/824b4899-en	Glossary for metaverse (WG1 – General)	S2.25.8, S2.25.9
ITU-T	(NEW) ITU-T FGMV-34	http://handle.itu.int/11.1002/pub/824b48c2-en	Definitions of CitiVerse (WG1 – General)	S2.25.8, S2.25.9, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-35	http://handle.itu.int/11.1002/pub/824b48e8-en	Building a People-centred CitiVerse (WG1 – General)	S2.25.8, S2.25.9, S2.25.14, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-36	http://handle.itu.int/11.1002/pub/824b4906-en	The future of travel in the metaverse: landscape and use cases (WG2 - Applications & Services)	S2.25.8, S2.25.9, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-37	http://handle.itu.int/11.1002/pub/824b4936-en	Landscape and use cases for the industrial metaverse (WG2 - Applications & Services)	S2.25.8, S2.25.9, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-38	http://handle.itu.int/11.1002/pub/824b4951-en	Framework and requirements for the construction of human-driven 3D digital human application system for metaverse (WG2 - Applications & Services)	S2.25.8, S2.25.9, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-39	http://handle.itu.int/11.1002/pub/824b4970-en	Use cases and requirements for virtual and real fusion coding in metaverse applications (WG2 - Applications & Services)	S2.25.8, S2.25.9, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-40	http://handle.itu.int/11.1002/pub/824b498d-en	Multimedia aspect of metaverse architecture (WG3 - Architecture & Infrastructure)	S2.25.5, S2.25.8, S2.25.9, S2.25.12
ITU-T	(NEW) ITU-T FGMV-41	http://handle.itu.int/11.1002/pub/824b498d-en	The reference framework of industrial metaverse (WG3 - Architecture & Infrastructure)	S2.25.8, S2.25.9, S2.25.12, S2.25.13, S2.25.15, S2.25.16

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ITU-T	(NEW) ITU-T FGMV-42	http://handle.itu.int/11.1002/pub/824b4b9d-en	Interoperability of identity of things across metaverse platforms (WG5 - Interoperability)	S2.25.7, S2.25.10, S2.25.11
ITU-T	(NEW) ITU-T FGMV-43	http://handle.itu.int/11.1002/pub/824b4b-bf-en	High-level interoperability architecture for cross-platform metaverse (WG5 - Interoperability)	S2.25.7, 2.33.10, S2.25.13, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-44	http://handle.itu.int/11.1002/pub/824b-4be8-en	Security for things across metaverses in aspects of data processing and management (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.7, S2.25.11, S2.253.13
ITU-T	(NEW) ITU-T FGMV-45	http://handle.itu.int/11.1002/pub/824b-4c0f-en	Challenges to achieving trustworthy metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-46	http://handle.itu.int/11.1002/pub/824b4e0f-en	The essential components of trusted data use in building a trustworthy metaverse (WG6 - Security, Data & Personally identifiable information (PII) Protection)	S2.25.11
ITU-T	(NEW) ITU-T FGMV-47	http://handle.itu.int/11.1002/pub/824b4e2c-en	Economic Value Creation and Competition in metaverse (WG7 - Economic, regulatory & competition aspects)	S2.25.14
ITU-T	(NEW) ITU-T FGMV-48	http://handle.itu.int/11.1002/pub/824b4e5e-en	Guidance on how to build a metaverse for all: Part II – Survey (WG8 -Sustainability, Accessibility & Inclusion)	S2.25.12, S2.25.13, S2.25.14, S2.25.15, S2.25.16
ITU-T	(NEW) ITU-T FGMV-49	http://handle.itu.int/11.1002/pub/824b4e8b-en	Metaverse Sustainability: Driving energy efficiency and GHG emissions reduction (WG8 -Sustainability, Accessibility & Inclusion)	S2.8, S2.24, S2.25.14
ITU-T	(NEW) ITU-T FGMV-50	http://handle.itu.int/11.1002/pub/824b4f00-en	Methodology on assessment of GHG emissions of metaverse (WG8 -Sustainability, Accessibility & Inclusion)	S2.8, S2.24, S2.25.14
ITU-T	(NEW) ITU-T FGMV-51	http://handle.itu.int/11.1002/pub/824b4f27-en	Standardization roadmap for metaverse (WG9 – Collaboration)	S2.25.10
ITU-T	(NEW) ITU-T FGMV-52	http://handle.itu.int/11.1002/pub/824b4f48-en	Metaverse standardization landscape for gap analyses (WG9 – Collaboration)	S2.25.10

Table 10: AIOTI/EUOS indentified IoT challenges covered/addressed by W3C

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
W3C	(Updated) Thing Description (TD)	https://www.w3.org/2019/wot/td	The Thing Description (TD) ontology is an RDF axiomatization of the TD information model, one of the building blocks of the Web of Things (WoT). Besides providing an alternative to the standard JSON representation format for TD documents, the TD ontology can also be used to process contextual information on Things and for alignments with other WoT-related ontologies.	S2.1, S2.18
W3C	DIDs	www.w3.org/TR/did-core/	Data and Information Management, Security and Trustworthiness - Create identifiers that enable verifiable, decentralized digital identities in a multi-party setting	S2.17
W3C	JSON-LD 1.1	www.w3.org/TR/json-ld11/	Data and Information Management - JSON is a data serialization and messaging format. This specification defines JSON-LD, a JSON-based format to serialize Linked Data. The syntax is designed to easily integrate into deployed systems that already use JSON, and provides a smooth upgrade path from JSON to JSON-LD. It is primarily intended to be a way to use Linked Data in Web-based programming environments, to build interoperable Web services, and to store Linked Data in JSON-based storage engines.	S2.1 , S2.18
W3C	ODRL Information Model 2.2	www.w3.org/TR/odrl-model/	Data and Information Management, Security and Trustworthiness - A policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. The ODRL Information Model describes the underlying concepts, entities, and relationships that form the foundational basis for the semantics of the ODRL policies.	S2.12
W3C	OGC 16-079	https://www.w3.org/TR/vocab-ssn/	The Semantic Sensor Network (SSN) ontology is an ontology for describing sensors and their observations, the involved procedures, the studied features of interest, the samples used to do so, and the observed properties, as well as actuators. SSN follows a horizontal and vertical modularization architecture by including a lightweight but self-contained core ontology called SOSA (Sensor, Observation, Sample, and Actuator) for its elementary classes and properties. With their different scope and different degrees of axiomatization, SSN and SOSA are able to support a wide range of applications and use cases, including satellite imagery, large-scale scientific monitoring, industrial and household infrastructures, social sensing, citizen science, observation-driven ontology engineering, and the Web of Things. Both ontologies are described below, and examples of their usage are given.	S2.1 , S2.18

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
W3C	RDF	www.w3.org/RDF/	Enterprise/Systems Integration, Data and Information Management, Analytics and AI - RDF is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.	S2.1 , S2.18
W3C	Verifiable Credentials Data Model v1.1	www.w3.org/TR/vc-data-model/	Data and Information Management, Security and Trustworthiness - Create cryptographically secure, privacy respecting, and machine-verifiable credentials for establishing trust among different entities in a decentralized setting	S2.17
W3C	(NEW) W3C Web of Things (WoT) Architecture 1.1	https://www.w3.org/TR/wot-architecture11/	The W3C Web of Things (WoT) enables interoperability across IoT platforms and application domains. The goal of the WoT is to preserve and complement existing IoT standards and solutions. The W3C WoT architecture is designed to describe what exists, and only prescribes new mechanisms when necessary.	S2.1, S2.7, S2.16
W3C	(NEW) W3C Web of Things (WoT) Thing Description 1.1	https://www.w3.org/TR/wot-thing-description11/	This document describes a formal information model and a common representation for a Web of Things (WoT) Thing Description 1.1. 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. Furthermore, this document introduces the Thing Model, which allows authors to describe only the model or class of an Internet of Things (IoT) entity. Thing Models can be seen as a template for Thing Description instances, but with reduced constraints such as no or few requirements for specific communication metadata.	S2.1, S2.16
W3C	(NEW) W3C Web of Things (WoT) Discovery	https://www.w3.org/TR/wot-discovery/	The WoT Discovery process is divided into 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.	S2.1, S2.6, S2.7, S2.16

Table 11: AIOTI/EUOS indentified IoT challenges covered/addressed by IETF

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	(Updated) IETF draft-ietf-asdf-sdf Semantic Definition Format (SDF) for Data and Interactions of Things	https://datatracker.ietf.org/doc/draft-ietf-asdf-sdf/	In this document, an SDF specification describes definitions of SDF Objects and their associated interactions (Events, Actions, Properties), as well as the Data types for the information exchanged in those interactions.	S2.1, S2.2, S2.18
IETF	(Updated) IETF RFC 9365 IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases	https://datatracker.ietf.org/doc/rfc9365/	This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation systems (ITS).	S2.7
IETF	(Updated) IETF RFC9528 Ephemeral Diffie-Hellman Over COSE (EDHOC)	https://datatracker.ietf.org/doc/rfc9528/	This document specifies Ephemeral Diffie-Hellman Over COSE (EDHOC), a very compact and lightweight authenticated Diffie-Hellman key exchange with ephemeral keys.	S2.6
IETF	IETF draft-ietf-lake-traces Traces of EDHOC	https://datatracker.ietf.org/doc/draft-ietf-lake-traces/	This document contains some example traces of Ephemeral Diffie-Hellman Over COSE (EDHOC).	S2.6
IETF	(Updated) IETF draft-ietf-rats-ar4si Attestation Results for Secure Interactions	https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/	This document defines reusable Attestation Result information elements. When these elements are offered to Relying Parties as Evidence, different aspects of Attester trustworthiness can be evaluated.	S2.6
IETF	(Updated) IETF RFC 9334 Remote Attestation Procedures Architecture	https://datatracker.ietf.org/doc/rfc9334/	This document provides an architectural overview of the entities involved that make such tests possible through the process of generating, conveying, and evaluating evidentiary claims.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	(Updated) IETF draft-ietf-rats-daa Direct Anonymous Attestation for the Remote Attestation Procedures Architecture	https://datatracker.ietf.org/doc/draft-ietf-rats-daa/	This document maps the concept of Direct Anonymous Attestation (DAA) to the Remote Attestation Procedures (RATS) Architecture. The role DAA Issuer is introduced and its interactions with existing RATS roles is specified.	S2.6
IETF	(Update) IETF draft-ietf-rats-eat The Entity Attestation Token (EAT)	https://datatracker.ietf.org/doc/draft-ietf-rats-eat/	This document extends CBOR Web Token (CWT) and JSON Web Token (JWT).	S2.6
IETF	(Updated) IETF draft-ietf-rats-network-device-subscription Attestation Event Stream Subscription	https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/	This memo provides the methods and means to define additional Event Streams for other Conceptual Message as illustrated in the RATS Architecture, e.g. Attestation Results, Endorsements, or Event Logs.	S2.6
IETF	(Updated) IETF draft-ietf-rats-reference-interaction-models Reference Interaction Models for Remote Attestation Procedures	https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/	This document describes interaction models for remote attestation procedures (RATS). Three conveying mechanisms -- Challenge/Response, Uni-Directional, and Streaming Remote Attestation -- are illustrated and defined.	S2.1, S2.6
IETF	(Updated) IETF draft-ietf-rats-tpm-based-network-device-attest TPM-based Network Device Remote Integrity Verification	https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/	This document describes a workflow for remote attestation of the integrity of firmware and software installed on network devices that contain Trusted Platform Modules [TPM1.2], [TPM2.0], as defined by the Trusted Computing Group (TCG)), or equivalent hardware implementations that include the protected capabilities, as provided by TPMs.	S2.6
IETF	(Updated) IETF draft-ietf-rats-uccs A CBOR Tag for Unprotected CWT Claims Sets	https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/	This specification defines a CBOR tag for such unprotected CWT Claims Sets (UCCS) and discusses conditions for its proper use.	S2.1, S2.6
IETF	(Updated) IETF draft-ietf-rats-yang-tpm-charra A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs.	https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/	This document defines YANG RPCs and a few configuration nodes required to retrieve attestation evidence about integrity measurements from a device, following the operational context defined in TPM-based Network Device Remote Integrity Verification.	S2.7
IETF	(Updated) IETF draft-ietf-raw-architecture Reliable and Available Wireless Architecture	https://datatracker.ietf.org/doc/draft-ietf-raw-architecture/	This document defines the RAW Architecture following an OODA loop that involves OAM, PCE, PSE and PAREO functions. It builds on the DetNet Architecture and discusses specific challenges and technology considerations needed to deliver DetNet service utilizing scheduled wireless segments and other media, e.g., frequency/time-sharing physical media resources with stochastic traffic.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	(Updated) IETF draft-ietf-raw-framework Reliable and Available Wireless Framework	https://datatracker.ietf.org/doc/draft-ietf-raw-framework/	Reliable and Available Wireless Framework following an OODA loop that involves OAM, PCE, PSE and PAREO functions.	S2.7
IETF	(Updated) IETF draft-ietf-raw-industrial-requirements Requirements for Reliable Wireless Industrial Services	https://datatracker.ietf.org/doc/draft-ietf-raw-industrial-requirements/	This document provides an overview on communication requirements for handling reliable wireless services within the context of industrial environments.	S2.7
IETF	Updated) IETF RFC 9372 L-band Digital Aeronautical Communications System (LDACS)	https://www.rfc-editor.org/info/rfc9372	This document gives an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation.	S2.7
IETF	(Updated) IETF draft-ietf-raw-oam-support Operations, Administration and Maintenance (OAM) features for RAW	https://datatracker.ietf.org/doc/draft-ietf-raw-oam-support/	This document lists the requirements of the Operation, Administration, and Maintenance (OAM) features are recommended to construct a predictable communication infrastructure on top of a collection of wireless segments.	S2.7
IETF	(Updated) IETF draft-ietf-raw-technologies Reliable and Available Wireless Technologies	https://datatracker.ietf.org/doc/draft-ietf-raw-technologies/	This document presents a series of recent technologies that are capable of time synchronization and scheduling of transmission, making them suitable to carry time-sensitive flows with high reliability and availability	S2.7
IETF	(Updated) IETF RFC 9450 RAW use-cases	https://datatracker.ietf.org/doc/rfc9450/	This document presents wireless use-cases (such as aeronautical communications, amusement parks, industrial applications, pro audio and video, gaming, UAV and V2V control, edge robotics and emergency vehicles) demanding reliable and available behavior.	S2.7
IETF	(Updated) IETF RFC 9397 Trusted Execution Environment Provisioning (TEEP) Architecture	https://datatracker.ietf.org/doc/rfc9397/	This architecture document motivates the design and standardization of a protocol for managing the lifecycle of trusted applications running inside such a TEE.	S2.6
IETF	(Updated) IETF draft-ietf-teep-otrp-over-http HTTP Transport for Trusted Execution Environment Provisioning: Agent Initiated Communication	https://datatracker.ietf.org/doc/draft-ietf-teep-otrp-over-http/	This document specifies the HTTP transport for TEEP communication where a Trusted Application Manager (TAM) service is used to manage code and data in TEEs on devices that can initiate communication to the TAM.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	(Updated) IETF draft-ietf-teep-protocol Trusted Execution Environment Provisioning (TEEP) Protocol	https://datatracker.ietf.org/doc/draft-ietf-teep-protocol/	This document specifies a protocol that installs, updates, and deletes Trusted Components in a device with a Trusted Execution Environment (TEE). This specification defines an interoperable protocol for managing the lifecycle of Trusted Components.	S2.6
IETF	(Updated) IETF draft-km-iotops-iiot-frwk Virtualization of PLC in Industrial Networks - Problem Statement	https://datatracker.ietf.org/doc/draft-km-iotops-iiot-frwk/	This document introduces virtual PLC concept, describes the details and benefits of virtualized PLCs, then focuses on the problem statement and requirements.	S2.7
IETF	(Updated) IETF draft-morais-iotops-inxu Intra-Network eXposure analyzer Utility Specification	https://datatracker.ietf.org/doc/draft-morais-iotops-inxu/	This document proposes the Intra-Network eXposure analyzer Utility (INXU) as a vulnerability management solution for IoT networks.	S2.7
IETF	IETF RFC4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals	https://datatracker.ietf.org/doc/rfc4919/	This document describes the assumptions, problem statement, and goals for transmitting IP over IEEE 802.15.4 networks. The set of goals enumerated in this document form an initial set only.	S2.7
IETF	IETF RFC4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks	https://datatracker.ietf.org/doc/rfc4944/	This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. Additional specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes.	S2.7
IETF	IETF RFC5548 Routing Requirements for Urban Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc5548/	This documents aims to specify a set of IPv6 routing requirements reflecting these and further U-LLNs' tailored characteristics.	S2.7
IETF	IETF RFC5673 Industrial Routing Requirements in Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc5673/	The wide deployment of lower-cost wireless devices will significantly improve the productivity and safety of industrial plants while increasing the efficiency of plant workers by extending the information set available about the plant operations. The aim of this document is to analyze the functional requirements for a routing protocol used in industrial Low-power and Lossy Networks (LLNs) of field devices.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC5826 Home Automation Routing Requirements in Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc5826/	This document presents requirements specific to home control and automation applications for Routing Over Low power and Lossy (ROLL) networks. In the near future, many homes will contain high numbers of wireless devices for a wide set of purposes. Examples include actuators (relay, light dimmer, heating valve), sensors (wall switch, water leak, blood pressure), and advanced controllers (radio-frequency-based AV remote control, central server for light and heat control). Because such devices only cover a limited radio range, routing is often required. The aim of this document is to specify the routing requirements for networks comprising such constrained devices in a home-control and automation environment.	S2.7
IETF	IETF RFC5867 Building Automation Routing Requirements in Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc5867/	The Routing Over Low-Power and Lossy (ROLL) networks Working Group has been chartered to work on routing solutions for Low-Power and Lossy Networks (LLNs) in various markets: industrial, commercial (building), home, and urban networks. Pursuant to this effort, this document defines the IPv6 routing requirements for building automation.	S2.7
IETF	IETF RFC6206 The Trickle Algorithm	https://datatracker.ietf.org/doc/rfc6206/	This document describes the Trickle algorithm and considerations in its use.	S2.7
IETF	IETF RFC6282 Compression Format for IPv6 Datagramas over IEEE 802.15.4-Based Networks	https://datatracker.ietf.org/doc/rfc6282/	This document updates RFC 4944, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”. This document specifies an IPv6 header compression format for IPv6 packet delivery in Low Power Wireless Personal Area Networks (6LoWPANs). The compression format relies on shared context to allow compression of arbitrary prefixes. How the information is maintained in that shared context is out of scope. This document specifies compression of multicast addresses and a framework for compressing next headers. UDP header compression is specified within this framework	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc6550/	This document specifies the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), which provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point as well as point-to-multipoint traffic from the central control point to the devices inside the LLN are supported. Support for point-to-point traffic is also available.	S2.7
IETF	IETF RFC6551 Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc6551/	This document specifies a set of link and node routing metrics and constraints suitable to LLNs to be used by the Routing Protocol for Low-Power and Lossy Networks (RPL).	S2.7
IETF	IETF RFC6552 Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)	https://datatracker.ietf.org/doc/rfc6552/	This document specifies a basic Objective Function that relies only on the objects that are defined in the RPL and does not use any protocol extensions.	S2.7
IETF	IETF RFC6568 Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	https://datatracker.ietf.org/doc/rfc6568/	This document investigates potential application scenarios and use cases for low-power wireless personal area networks (LoWPANs). This document provides dimensions of design space for LoWPAN applications. A list of use cases and market domains that may benefit and motivate the work currently done in the 6LoWPAN Working Group is provided with the characteristics of each dimension. A complete list of practical use cases is not the goal of this document.	S2.7
IETF	IETF RFC6606 Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing	https://datatracker.ietf.org/doc/rfc6606/	This document provides the problem statement and design space for 6LoWPAN routing. It defines the routing requirements for 6LoWPANs, considering the low-power and other particular characteristics of the devices and links. The purpose of this document is not to recommend specific solutions but to provide general, layer-agnostic guidelines about the design of 6LoWPAN routing that can lead to further analysis and protocol design.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC6690 Constrained RESTful Environments (CoRE) Link Format	https://datatracker.ietf.org/doc/rfc6690/	This specification defines Web Linking using a link format for use by constrained web servers to describe hosted resources, their attributes, and other relationships between links. Based on the HTTP Link Header field defined in RFC 5988, the Constrained RESTful Environments (CoRE) Link Format is carried as a payload and is assigned an Internet media type. "RESTful" refers to the Representational State Transfer (REST) architecture. A well-known URI is defined as a default entry point for requesting the links hosted by a server.	S2.7
IETF	IETF RFC6719 The Minimum Rank with Hysteresis Objective Function	https://datatracker.ietf.org/doc/rfc6719/	This specification describes the Minimum Rank with Hysteresis Objective Function (MRHOF), an Objective Function that selects routes that minimize a metric, while using hysteresis to reduce churn in response to small metric changes. MRHOF works with additive metrics along a route, and the metrics it uses are determined by the metrics that the RPL Destination Information Object (DIO) messages advertise.	S2.7
IETF	IETF RFC6775 Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	https://datatracker.ietf.org/doc/rfc6775/	The IETF work in IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) defines 6LoWPANs such as IEEE 802.15.4. This and other similar link technologies have limited or no usage of multicast signaling due to energy conservation. In addition, the wireless network may not strictly follow the traditional concept of IP subnets and IP links. IPv6 Neighbor Discovery was not designed for non-transitive wireless links, as its reliance on the traditional IPv6 link concept and its heavy use of multicast make it inefficient and sometimes impractical in a low-power and lossy network. This document describes simple optimizations to IPv6 Neighbor Discovery, its addressing mechanisms, and duplicate address detection for Low-power Wireless Personal Area Networks and similar networks. The document thus updates RFC 4944 to specify the use of the optimizations defined here.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC6997 Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc6997/	This document specifies a point-to-point route discovery mechanism, complementary to the Routing Protocol for Low-power and Lossy Networks (RPL) core functionality. This mechanism allows an IPv6 router to discover "on demand" routes to one or more IPv6 routers in a Low-power and Lossy Network (LLN) such that the discovered routes meet specified metrics constraints.	S2.7
IETF	IETF RFC6998 A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network	https://datatracker.ietf.org/doc/rfc6998/	This document specifies a mechanism that enables a Routing Protocol for Low-power and Lossy Networks (RPL) router to measure the aggregated values of given routing metrics along an existing route towards another RPL router, thereby allowing the router to decide if it wants to initiate the discovery of a better route.	S2.7
IETF	IETF RFC7102 Terms Used in Routing for Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc7102/	This document provides a glossary of terminology used in routing requirements and solutions for networks referred to as Low-Power and Lossy Networks (LLNs). An LLN is typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links. There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (e.g., heating, ventilation, air conditioning, lighting, access control, fire), connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration.	S2.7
IETF	IETF RFC 7228 Terminology for Constrained-Node Networks	https://datatracker.ietf.org/doc/rfc7228/	This document provides a number of basic terms that have been useful in the standardization work for constrained-node networks.	S2.7
IETF	IETF RFC7252 The Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc7252/	The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. The nodes often have 8-bit microcontrollers with small amounts of ROM and RAM, while constrained networks such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) often have high packet error rates and a typical throughput of 10s of kbit/s. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.	S2.2

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	IETF RFC 7388 Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	https://datatracker.ietf.org/doc/rfc7388/	This document defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for managing IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs).	S2.7
IETF	IETF RFC7390 Group Communication for the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc7390/	This specification defines how CoAP should be used in a group communication context. An approach for using CoAP on top of IP multicast is detailed based on existing CoAP functionality as well as new features introduced in this specification. Also, various use cases and corresponding protocol flows are provided to illustrate important concepts. Finally, guidance is provided for deployment in various network topologies.	S2.2
IETF	IETF RFC7400 6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	https://datatracker.ietf.org/doc/rfc7400/	RFC 6282 defines header compression in 6LoWPAN packets (where “6LoWPAN” refers to “IPv6 over Low-Power Wireless Personal Area Network”). The present document specifies a simple addition that enables the compression of generic headers and header-like payloads, without a need to define a new header compression scheme for each such new header or header-like payload.	S2.7
IETF	IETF RFC7416 A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)	https://datatracker.ietf.org/doc/rfc7416/	This document presents a security threat analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). The development builds upon previous work on routing security and adapts the assessments to the issues and constraints specific to low-power and lossy networks. A systematic approach is used in defining and evaluating the security threats. Applicable countermeasures are application specific and are addressed in relevant applicability statements.	S2.6
IETF	IETF RFC7428 Transmission of IPv6 Packets over ITU-T G.9959 Networks	https://datatracker.ietf.org/doc/rfc7428/	This document describes the frame format for transmission of IPv6 packets as well as a method of forming IPv6 link-local addresses and statelessly autoconfigured IPv6 addresses on ITU-T G.9959 networks.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC7554 Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement	https://datatracker.ietf.org/doc/rfc7554/	This document describes the environment, problem statement, and goals for using the Time-Slotted Channel Hopping (TSCH) Medium Access Control (MAC) protocol of IEEE 802.14.4e in the context of Low-Power and Lossy Networks (LLNs). The set of goals enumerated in this document form an initial set only.	S2.2
IETF	IETF RFC7641 Observing Resources in the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc7641/	This document specifies a simple protocol extension for CoAP that enables CoAP clients to "observe" resources, i.e., to retrieve a representation of a resource and keep this representation updated by the server over a period of time. The protocol follows a best-effort approach for sending new representations to clients and provides eventual consistency between the state observed by each client and the actual resource state at the server.	S2.7
IETF	IETF RFC7668 IPv6 over BLUETOOTH(R) Low Energy	https://datatracker.ietf.org/doc/rfc7668/	Bluetooth Smart is the brand name for the Bluetooth low energy feature in the Bluetooth specification defined by the Bluetooth Special Interest Group. The standard Bluetooth radio has been widely implemented and available in mobile phones, notebook computers, audio headsets, and many other devices. The low-power version of Bluetooth is a specification that enables the use of this air interface with devices such as sensors, smart meters, appliances, etc. The low-power variant of Bluetooth has been standardized since revision 4.0 of the Bluetooth specifications, although version 4.1 or newer is required for IPv6. This document describes how IPv6 is transported over Bluetooth low energy using IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) techniques.	S2.7
IETF	IETF RFC7731 Multicast Protocol for Low-Power and Lossy Networks (MPL)	https://datatracker.ietf.org/doc/rfc7731/	This document specifies the Multicast Protocol for Low-Power and lossy Networks (MPL), which provides IPv6 multicast forwarding in constrained networks. MPL avoids the need to construct or maintain any multicast forwarding topology, disseminating messages to all MPL Forwarders in an MPL Domain.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC7732 Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)	https://datatracker.ietf.org/doc/rfc7732/	The purpose of this document is to specify an automated policy for the routing of Multicast Protocol for Low-Power and Lossy Networks (MPL) multicast messages with Admin-Local scope in a border router.	S2.7
IETF	IETF RFC7733 Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control	https://datatracker.ietf.org/doc/rfc7733/	The purpose of this document is to provide guidance in the selection and use of protocols from the Routing Protocol for Low-Power and Lossy Networks (RPL) protocol suite to implement the features required for control in building and home environments.	S2.7
IETF	IETF RFC7744 Use Cases for Authentication and Authorization in Constrained Environments	https://datatracker.ietf.org/doc/rfc7744/	This document includes a collection of representative use cases for authentication and authorization in constrained environments. These use cases aim at identifying authorization problems that arise during the life cycle of a constrained device and are intended to provide a guideline for developing a comprehensive authentication and authorization solution for this class of scenarios.	S2.6
IETF	IETF RFC7774 Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6	https://datatracker.ietf.org/doc/rfc7774/	This document defines a way to configure a parameter set for MPL (Multicast Protocol for Low-Power and Lossy Networks) via a DHCPv6 option. MPL has a set of parameters to control its behavior, and the parameter set is often configured as a network-wide parameter because the parameter set should be identical for each MPL Forwarder in an MPL Domain. Using the MPL Parameter Configuration Option defined in this document, a network can easily be configured with a single set of MPL parameters.	S2.7
IETF	IETF RFC7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation	https://datatracker.ietf.org/doc/rfc7815/	This document describes a minimal initiator version of the Internet Key Exchange version 2 (IKEv2) protocol for constrained nodes.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	IETF RFC7959 Block-Wise Transfers in the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc7959/	this specification extends basic CoAP with a pair of "Block" options for transferring multiple blocks of information from a resource representation in multiple request-response pairs. In many important cases, the Block options enable a server to be truly stateless: the server can handle each block transfer separately, with no need for a connection setup or other server-side memory of previous block transfers. Essentially, the Block options provide a minimal way to transfer larger representations in a block-wise fashion.	S2.6
IETF	IETF RFC 7973 Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation	https://datatracker.ietf.org/doc/rfc7973/	When carried over Layer 2 technologies such as Ethernet, IPv6 datagrams using Low-Power Wireless Personal Area Network (LoWPAN) encapsulation as defined in RFC 4944 must be identified so the receiver can correctly interpret the encoded IPv6 datagram. The IETF officially requested the assignment of an Ethertype for that purpose and this document reports that assignment.	S2.7
IETF	IETF RFC 8025 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch	https://datatracker.ietf.org/doc/rfc8025/	This specification updates RFC 4944 to introduce a new context switch mechanism for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) compression, expressed in terms of Pages and signaled by a new Paging Dispatch.	S2.7
IETF	IETF RFC 8036 Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks	https://datatracker.ietf.org/doc/rfc8036/	This document discusses the applicability of the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) networks.	S2.7
IETF	IETF RFC 8065 Privacy Considerations for IPv6 Adaptation-Layer Mechanisms	https://datatracker.ietf.org/doc/rfc8065/	This document discusses how a number of privacy threats apply to technologies designed for IPv6 over various link-layer protocols, and it provides advice to protocol designers on how to address such threats in adaptation-layer specifications for IPv6 over such links.	S2.6 S2.11, S2.12

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8066 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines	https://datatracker.ietf.org/doc/rfc8066/	RFC 4944 defines the ESC dispatch type to allow additional dispatch octets in the 6LoWPAN header. The value of the ESC dispatch type was updated by RFC 6282; however, its usage was not defined in either RFC 6282 or RFC 4944. This document updates RFC 4944 and RFC 6282 by defining the ESC extension octet code points and listing registration entries for known use cases at the time of writing of this document.	S2.6
IETF	IETF RFC 8075 Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc8075/	This document provides reference information for implementing a cross-protocol network proxy that performs translation from the HTTP protocol to the Constrained Application Protocol (CoAP). This will enable an HTTP client to access resources on a CoAP server through the proxy. This document describes how an HTTP request is mapped to a CoAP request and how a CoAP response is mapped back to an HTTP response. This includes guidelines for status code, URI, and media type mappings, as well as additional interworking advice.	S2.7
IETF	IETF RFC 8105 Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)	https://datatracker.ietf.org/doc/rfc8105/	This document describes how IPv6 is transported over DECT ULE using IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques.	S2.7
IETF	IETF RFC 8132 PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc8132/	This specification defines the new CoAP methods, FETCH, PATCH, and iPATCH, which are used to access and update parts of a resource.	S2.7
IETF	IETF RFC 8138 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header	https://datatracker.ietf.org/doc/rfc8138/	This specification introduces a new IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) dispatch type for use in 6LoWPAN route-over topologies, which initially covers the needs of Routing Protocol for Low-Power and Lossy Networks (RPL) data packet compression (RFC 6550). Using this dispatch type, this specification defines a method to compress the RPL Option (RFC 6553) information and Routing Header type 3 (RFC 6554), an efficient IP-in-IP technique, and is extensible for more applications.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8152 CBOR Object Signing and Encryption (COSE)	https://datatracker.ietf.org/doc/rfc8152/	This specification describes how to create and process signatures, message authentication codes, and encryption using CBOR for serialization. This specification additionally describes how to represent cryptographic keys using CBOR.	S2.6
IETF	IETF RFC 8163 Transmission of IPv6 over Master-Slave/ Token-Passing (MS/TP) Networks	https://datatracker.ietf.org/doc/rfc8163/	Master-Slave/Token-Passing (MS/TP) is a medium access control method for the RS-485 physical layer and is used primarily in building automation networks. This specification defines the frame format for transmission of IPv6 packets and the method of forming link-local and statelessly autoconfigured IPv6 addresses on MS/TP networks.	S2.7
IETF	IETF RFC 8180 Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration	https://datatracker.ietf.org/doc/rfc8180/	This document describes a minimal mode of operation for an IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) network. This minimal mode of operation specifies the baseline set of protocols that need to be supported and the recommended configurations and modes of operation sufficient to enable a 6TiSCH functional network. 6TiSCH provides IPv6 connectivity over a Time-Slotted Channel Hopping (TSCH) mesh composed of IEEE Std 802.15.4 TSCH links. This minimal mode uses a collection of protocols with the respective configurations, including the IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) framework, enabling interoperable IPv6 connectivity over IEEE Std 802.15.4 TSCH. This minimal configuration provides the necessary bandwidth for network and security bootstrapping and defines the proper link between the IETF protocols that interface to IEEE Std 802.15.4 TSCH. This minimal mode of operation should be implemented by all 6TiSCH-compliant devices.	S2.7
IETF	IETF RFC 8323 CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets	https://datatracker.ietf.org/doc/rfc8323/	This document outlines the changes required to use CoAP over TCP,TLS, and WebSockets transports. It also formally updates RFC 7641 for use with these transports and RFC 7959 to enable the use of larger messages over a reliable transport.	S2.2
IETF	IETF RFC 8352 Energy-Efficient Features of Internet of Things Protocols	https://datatracker.ietf.org/doc/rfc8352/	This document describes the challenges for energy-efficient protocol operation on constrained devices and the current practices used to overcome those challenges	S2.8, S2.24

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	IETF RFC 8366 A Voucher Artifact for Bootstrapping Protocols	https://datatracker.ietf.org/doc/rfc8366/	This document defines a strategy to securely assign a pledge to an owner using an artifact signed, directly or indirectly, by the pledge's manufacturer. This artifact is known as a "voucher".	S2.7
IETF	IETF RFC 8368 Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)	https://datatracker.ietf.org/doc/rfc8368/	This document describes how to integrate OAM processes with an autonomic control plane in order to provide stable and secure connectivity for those OAM processes.	S2.7
IETF	IETF RFC 8376 Low-Power Wide Area Network (LPWAN) Overview	https://datatracker.ietf.org/doc/rfc8376/	This memo is an informational overview of the set of LPWAN technologies being considered in the IETF and of the gaps that exist between the needs of those technologies and the goal of running IP in LPWANs.	S2.7
IETF	IETF RFC 8387 Practical Considerations and Implementation Experiences in Securing Smart Object Networks	https://datatracker.ietf.org/doc/rfc8387/	This memo describes challenges associated with securing resource-constrained smart object devices	S2.6
IETF	IETF RFC 8392 CBOR Web Token (CWT)	https://datatracker.ietf.org/doc/rfc8392/	CBOR Web Token (CWT) is a compact means of representing claims to be transferred between two parties. The claims in a CWT are encoded in the Concise Binary Object Representation (CBOR), and CBOR Object Signing and Encryption (COSE) is used for added application-layer security protection. A claim is a piece of information asserted about a subject and is represented as a name/value pair consisting of a claim name and a claim value. CWT is derived from JSON Web Token (JWT) but uses CBOR rather than JSON.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8428 Sensor Measurement Lists (SenML)	https://datatracker.ietf.org/doc/rfc8428/	This specification defines a format for representing simple sensor measurements and device parameters in Sensor Measurement Lists (SenML). Representations are defined in JavaScript Object Notation (JSON), Concise Binary Object Representation (CBOR), Extensible Markup Language (XML), and Efficient XML Interchange (EXI), which share the common SenML data model. A simple sensor, such as a temperature sensor, could use one of these media types in protocols such as HTTP or the Constrained Application Protocol (CoAP) to transport the measurements of the sensor or to be configured.	S2.1
IETF	IETF RFC 8480 6TiSCH Operation Sublayer (6top) Protocol (6P)	https://datatracker.ietf.org/doc/rfc8480/	This document defines the "IPv6 over the TSCH mode of IEEE 802.15.4e" (6TiSCH) Operation Sublayer (6top) Protocol (6P), which enables distributed scheduling in 6TiSCH networks. 6P allows neighbor nodes to add/delete Time-Slotted Channel Hopping (TSCH) cells to/on one another. 6P is part of the 6TiSCH Operation Sublayer (6top), the layer just above the IEEE Std 802.15.4 TSCH Medium Access Control layer. 6top is composed of one or more Scheduling Functions (SFs) and the 6top Protocol defined in this document. A 6top SF decides when to add/delete cells, and it triggers 6P Transactions. The definition of SFs is out of scope for this document; however, this document provides the requirements for an SF.	S2.7
IETF	IETF RFC 8505 Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery	https://datatracker.ietf.org/doc/rfc8505/	This specification updates RFC 6775 -- the Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery specification -- to clarify the role of the protocol as a registration technique and simplify the registration operation in 6LoWPAN routers, as well as to provide enhancements to the registration capabilities and mobility detection for different network topologies, including the Routing Registrars performing routing for host routes and/or proxy Neighbor Discovery in a low-power network.	S2.7
IETF	IETF RFC 8516 "Too Many Requests" Response Code for the Constrained Application Protocol	https://datatracker.ietf.org/doc/rfc8516/	This document defines a new CoAP response code for a server to indicate that a client should reduce the rate of requests.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8557 Deterministic Networking Problem statement	https://datatracker.ietf.org/doc/rfc8557/	This paper documents the needs in various industries to establish multi-hop paths for characterized flows with deterministic properties.	S2.7
IETF	IETF RFC 8578 Deterministic Networking Use Cases	https://datatracker.ietf.org/doc/rfc8578/	This document presents use cases for diverse industries that have in common a need for "deterministic flows".	S2.7
IETF	IETF RFC 8610 Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures	https://datatracker.ietf.org/doc/rfc8610/	This document proposes a notational convention to express Concise Binary Object Representation (CBOR) data structures (RFC 7049). Its main goal is to provide an easy and unambiguous way to express structures for protocol messages and data formats that use CBOR or JSON.	S2.1
IETF	IETF RFC 8613 Object Security for Constrained RESTful Environments (OSCORE)	https://datatracker.ietf.org/doc/rfc8613/	This document defines Object Security for Constrained RESTful Environments (OSCORE), a method for application-layer protection of the Constrained Application Protocol (CoAP), using CBOR Object Signing and Encryption (COSE). OSCORE provides end-to-end protection between endpoints communicating using CoAP or CoAP-mappable HTTP. OSCORE is designed for constrained nodes and networks supporting a range of proxy operations, including translation between different transport protocols.	S2.6
IETF	IETF RFC 8655 Deterministic Networking Architecture	https://datatracker.ietf.org/doc/rfc8655/	This document provides the overall architecture for Deterministic Networking (DetNet), which provides a capability to carry specified unicast or multicast data flows for real-time applications with extremely low data loss rates and bounded latency within a network domain	S2.7
IETF	IETF RFC 8710 Multipart Content-Format for the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc8710/	This memo defines application/multipart-core, an application- independent media type that can be used to combine representations of zero or more different media types (each with a Constrained Application Protocol (CoAP) Content-Format identifier) into a single representation, with minimal framing overhead.	S2.7
IETF	IETF RFC 8724 SCHC: Generic Framework for Static Context Header Compression and Fragmentation	https://datatracker.ietf.org/doc/rfc8724/	This document defines the Static Context Header Compression and fragmentation (SCHC) framework, which provides both a header compression mechanism and an optional fragmentation mechanism.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	IETF RFC 8742 Concise Binary Object Representation (CBOR) Sequences	https://datatracker.ietf.org/doc/rfc8742/	his document describes the Concise Binary Object Representation (CBOR) Sequence format and associated media type "application/cbor-seq". A CBOR Sequence consists of any number of encoded CBOR data items, simply concatenated in sequence.	S2.1
IETF	IETF RFC 8746 Concise Binary Object Representation (CBOR) Tags for Typed Arrays	https://datatracker.ietf.org/doc/rfc8746/	This document makes use of this extensibility to define a number of CBOR tags for typed arrays of numeric data, as well as additional tags for multi-dimensional and homogeneous arrays. It is intended as the reference document for the IANA registration of the CBOR tags defined.	S2.1
IETF	IETF RFC 8747 Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)	https://datatracker.ietf.org/doc/rfc8747/	This specification describes how to declare in a CBOR Web Token (CWT) (which is defined by RFC 8392) that the presenter of the CWT possesses a particular proof-of-possession key. Being able to prove possession of a key is also sometimes described as being the holder-of-key. This specification provides equivalent functionality to "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)" (RFC 7800) but using Concise Binary Object Representation (CBOR) and CWTs rather than JavaScript Object Notation (JSON) and JSON Web Tokens (JWTs).	S2.1
IETF	IETF RFC 8768 Constrained Application Protocol (CoAP) Hop-Limit Option	https://datatracker.ietf.org/doc/rfc8768/	This document specifies the Hop-Limit CoAP option.	S2.7
IETF	IETF RFC 8778 Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)	https://datatracker.ietf.org/doc/rfc8778/	This document specifies the conventions for using the Hierarchical Signature System (HSS) / Leighton-Micali Signature (LMS) hash-based signature algorithm with the CBOR Object Signing and Encryption (COSE) syntax. The HSS/LMS algorithm is one form of hash-based digital signature; it is described in RFC 8554.	S2.6, S2.9
	IETF RFC 8790 FETCH and PATCH with Sensor Measurement Lists (SenML)	https://datatracker.ietf.org/doc/rfc8790/	This document defines new media types for the CoAP FETCH, PATCH, and iPATCH methods for resources represented using the SenML data model.	S2.2

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8798 Additional Units for Sensor Measurement Lists (SenML)	https://datatracker.ietf.org/doc/rfc8798/	This document registers a number of additional unit names in the IANA registry for units in SenML. It also defines a registry for secondary units that cannot be in SenML's main registry, as they are derived by linear transformation from units already in that registry.	S2.2
IETF	IETF RFC 8812 CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms	https://datatracker.ietf.org/doc/rfc8812/	This specification registers the following algorithms (which are used by WebAuthn and CTAP implementations) in the IANA "COSE Algorithms" registry: RSASSA-PKCS1-v1_5 using SHA-256, SHA-384, SHA-512, and SHA-1; and Elliptic Curve Digital Signature Algorithm (ECDSA) using the secp256k1 curve and SHA-256. It registers the secp256k1 elliptic curve in the IANA "COSE Elliptic Curves" registry. Also, for use with JSON Object Signing and Encryption (JOSE), it registers the algorithm ECDSA using the secp256k1 curve and SHA-256 in the IANA "JSON Web Signature and Encryption Algorithms" registry and the Secp256k1 elliptic curve in the IANA "JSON Web Key Elliptic Curve" registry.	S2.6
IETF	IETF RFC 8824 Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc8824/	This document defines how to compress Constrained Application Protocol (CoAP) headers using the Static Context Header Compression and fragmentation (SCHC) framework	S2.7
IETF	IETF RFC 8928 Address-Protected Neighbor Discovery for Low-Power and Lossy Networks	https://datatracker.ietf.org/doc/rfc8928/	This document updates the IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery (ND) protocol defined in RFCs 6775 and 8505. The new extension is called Address-Protected Neighbor Discovery (AP-ND), and it protects the owner of an address against address theft and impersonation attacks in a Low-Power and Lossy Network (LLN). Nodes supporting this extension compute a cryptographic identifier (Crypto-ID), and use it with one or more of their Registered Addresses. The Crypto-ID identifies the owner of the Registered Address and can be used to provide proof of ownership of the Registered Addresses. Once an address is registered with the Crypto-ID and a proof of ownership is provided, only the owner of that address can modify the registration information, thereby enforcing Source Address Validation	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8929 IPv6 Backbone Router	https://datatracker.ietf.org/doc/rfc8929/	This document updates RFCs 6775 and 8505 in order to enable proxy services for IPv6 Neighbor Discovery by Routing Registrars called "Backbone Routers". Backbone Routers are placed along the wireless edge of a backbone and federate multiple wireless links to form a single Multi-Link Subnet (MLSN).	S2.7
IETF	IETF RFC 8930 On Forwarding 6LoWPAN Fragments over a Multi-Hop IPv6 Network	https://datatracker.ietf.org/doc/rfc8930/	This document provides generic rules to enable the forwarding of an IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) fragment over a route-over network. Forwarding fragments can improve both end-to-end latency and reliability as well as reduce the buffer requirements in intermediate nodes; it may be implemented using RFC 4944 and Virtual Reassembly Buffers (VRBs).	S2.7
IETF	IETF RFC 8931 IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Selective Fragment Recovery	https://datatracker.ietf.org/doc/rfc8931/	This document updates RFC 4944 with a protocol that forwards individual fragments across a route-over mesh and recovers them end to end, with congestion control capabilities to protect the network.	S2.7
IETF	IETF RFC 8938 Deterministic Networking (DetNet) Data Plane Framework	https://datatracker.ietf.org/doc/rfc8938/	This document provides an overall framework for the Deterministic Networking (DetNet) data plane. It covers concepts and considerations that are generally common to any DetNet data plane specification. It describes related Controller Plane considerations as well.	S2.7
IETF	IETF RFC 8939 Deterministic Networking (DetNet) Data Plane: IP	https://datatracker.ietf.org/doc/rfc8939/	This document specifies the Deterministic Networking (DetNet) data plane operation for IP hosts and routers that provide DetNet service to IP-encapsulated data	S2.7
IETF	IETF RFC 8943 Concise Binary Object Representation (CBOR) Tags for Date	https://datatracker.ietf.org/doc/rfc8943/	This specification defines a CBOR tag for a date text string (as per RFC 3339) for applications needing a textual date representation within the Gregorian calendar without a time. It also defines a CBOR tag for days since the date 1970-01-01 in the Gregorian calendar for applications needing a numeric date representation without a time. This specification is the reference document for IANA registration of the CBOR tags defined.	S2.1

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 8949 Concise Binary Object Representation (CBOR)	https://datatracker.ietf.org/doc/rfc8949/	This document obsoletes RFC 7049, providing editorial improvements, new details, and errata fixes while keeping full compatibility with the interchange format of RFC 7049. It does not create a new version of the format	S2.1
IETF	IETF RFC 8964 Deterministic Networking (DetNet) Data Plane: MPLS	https://datatracker.ietf.org/doc/rfc8964/	This document specifies the Deterministic Networking (DetNet) data plane when operating over an MPLS Packet Switched Network	S2.7
IETF	IETF RFC 8974 Extended Tokens and Stateless Clients in the Constrained Application Protocol (CoAP)	https://datatracker.ietf.org/doc/rfc8974/	This document provides considerations for alleviating Constrained Application Protocol (CoAP) clients and intermediaries of keeping per-request state. To facilitate this, this document additionally introduces a new, optional CoAP protocol extension for extended token lengths.	S2.7
IETF	IETF RFC 8990 GeneRic Autonomic Signaling Protocol (GRASP)	https://datatracker.ietf.org/doc/rfc8990/	This document specifies the GeneRic Autonomic Signaling Protocol (GRASP), which enables autonomic nodes and Autonomic Service Agents to dynamically discover peers, to synchronize state with each other, and to negotiate parameter settings with each other	S2.7
IETF	IETF RFC 8991 GeneRic Autonomic Signaling Protocol Application Program Interface (GRASP API)	https://datatracker.ietf.org/doc/rfc8991/	This document is a conceptual outline of an application Programming Interface (API) for the GeneRic Autonomic Signaling Protocol (GRASP).	S2.7
IETF	IETF RFC 8992 Autonomic IPv6 Edge Prefix Management in Large-Scale Networks	https://datatracker.ietf.org/doc/rfc8992/	This document defines two autonomic technical objectives for IPv6 prefix management at the edge of large-scale ISP networks, with an extension to support IPv4 prefixes.	S2.7
IETF	IETF RFC 8993 A Reference Model for Autonomic Networking	https://datatracker.ietf.org/doc/rfc8993/	This document describes a reference model for Autonomic Networking for managed networks.	S2.7
IETF	IETF RFC 8994 An Autonomic Control Plane (ACP)	https://datatracker.ietf.org/doc/rfc8994/	This document defines such a plane and calls it the "Autonomic Control Plane", with the primary use as a control plane for autonomic functions.	S2.7
IETF	IETF RFC 8995 Bootstrapping Remote Secure Key Infrastructure (BRSKI)	https://datatracker.ietf.org/doc/rfc8995/	This document specifies automated bootstrapping of an Autonomic Control Plane.	S2.6
IETF	IETF RFC 9006 TCP Usage Guidance in the Internet of Things (IoT)	https://datatracker.ietf.org/doc/rfc9006/	This document provides guidance on how to implement and use the Transmission Control Protocol (TCP) in Constrained-Node Networks (CNNs), which are a characteristic of the Internet of Things (IoT).	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 9008 Using RPI Option Type, Routing Header for Source Routes, and IPv6-in-IPv6 Encapsulation in the RPL Data Plane	https://datatracker.ietf.org/doc/rfc9008/	This document looks at different data flows through Low-Power and Lossy Networks (LLN) where RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) is used to establish routing. The document enumerates the cases where RPL Packet Information (RPI) Option Type (RFC 6553), RPL Source Route Header (RFC 6554), and IPv6-in-IPv6 encapsulation are required in the data plane. This analysis provides the basis upon which to design efficient compression of these headers. This document updates RFC 6553 by adding a change to the RPI Option Type. Additionally, this document updates RFC 6550 by defining a flag in the DODAG Information Object (DIO) Configuration option to indicate this change and updates RFC 8138 as well to consider the new Option Type when the RPL Option is decompressed.	S2.7
IETF	IETF RFC9009 Efficient Route Invalidation	https://datatracker.ietf.org/doc/rfc9009/	This document explains the problems associated with the use of No-Path Destination Advertisement Object (NPDAO) messaging in RFC 6550 and also discusses the requirements for an optimized route invalidation messaging scheme. Further, this document specifies a new proactive route invalidation message called the “Destination Cleanup Object” (DCO), which fulfills requirements for optimized route invalidation messaging.	S2.7
IETF	IETF RFC9010 Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves	https://datatracker.ietf.org/doc/rfc9010/	This specification provides a mechanism for a host that implements a routing-agnostic interface based on IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery to obtain reachability services across a network that leverages RFC 6550 for its routing operations. It updates RFCs 6550, 6775, and 8505.	S2.7
IETF	IETF RFC 9011 Static Context Header Compression and Fragmentation (SCHC) over LoRaWAN	https://datatracker.ietf.org/doc/rfc9011/	This document defines a profile of SCHC (RFC 8724) for use in LoRaWAN networks and provides elements such as efficient parameterization and modes of operation.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 9016 Flow and Service Information Model for Deterministic Networking (DetNet)	https://datatracker.ietf.org/doc/rfc9016/	This document describes the flow and service information model for Deterministic Networking (DetNet). These models are defined for IP and MPLS DetNet data planes.	S2.7
IETF	IETF RFC 9019 A Firmware Update Architecture for Internet of Things	https://datatracker.ietf.org/doc/rfc9019/	This document provides the motivation for the standardization of a manifest format as a transport-agnostic means for describing and protecting firmware updates.	S2.13
IETF	IETF RFC 9123 Deterministic Networking (DetNet) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking (TSN)	https://datatracker.ietf.org/doc/rfc9023/	This document specifies the Deterministic Networking IP data plane when operating over a Time-Sensitive Networking (TSN) sub-network.	S2.7
IETF	IETF RFC 9024 Deterministic Networking (DetNet) Data Plane: IEEE 802.1 Time-Sensitive Networking over MPLS	https://datatracker.ietf.org/doc/rfc9024/	This document specifies the Deterministic Networking data plane when Time-Sensitive Networking (TSN) networks are interconnected over a DetNet MPLS network.	S2.7
IETF	IETF RFC 9025 Deterministic Networking (DetNet) Data Plane: MPLS over UDP/IP	https://datatracker.ietf.org/doc/rfc9025/	This document specifies the MPLS Deterministic Networking (DetNet) data plane operation and encapsulation over an IP network. The approach is based on the operation of MPLS-over-UDP technology.	S2.7
IETF	IETF RFC 9030 An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)	https://datatracker.ietf.org/doc/rfc9030/	This document describes a network architecture that provides low-latency, low-jitter, and high-reliability packet delivery. It combines a high-speed powered backbone and subnetworks using IEEE 802.15.4 time-slotted channel hopping (TSCH) to meet the requirements of low-power wireless deterministic applications.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 9031 Constrained Join Protocol (CoJP) for 6TiSCH	https://datatracker.ietf.org/doc/rfc9031/	This document describes the minimal framework required for a new device, called a "pledge", to securely join a 6TiSCH (IPv6 over the Time-Slotted Channel Hopping mode of IEEE 802.15.4) network. The framework requires that the pledge and the JRC (Join Registrar/ Coordinator, a central entity), share a symmetric key. How this key is provisioned is out of scope of this document. Through a single CoAP (Constrained Application Protocol) request-response exchange secured by OSCORE (Object Security for Constrained RESTful Environments), the pledge requests admission into the network, and the JRC configures it with link-layer keying material and other parameters. The JRC may at any time update the parameters through another request-response exchange secured by OSCORE. This specification defines the Constrained Join Protocol and its CBOR (Concise Binary Object Representation) data structures, and it describes how to configure the rest of the 6TiSCH communication stack for this join process to occur in a secure manner. Additional security mechanisms may be added on top of this minimal framework.	S2.7
IETF	IETF RFC 9032 Encapsulation of 6TiSCH Join and Enrollment Information Elements	https://datatracker.ietf.org/doc/rfc9032/	In the Time-Slotted Channel Hopping (TSCH) mode of IEEE Std 802.15.4, opportunities for broadcasts are limited to specific times and specific channels. Routers in a TSCH network transmit Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which additional information critical for new nodes (pledges) and long-sleeping nodes may be carried within the EB in order to conserve use of broadcast opportunities.	S2.7
IETF	IETF RFC 9033 6TiSCH Minimal Scheduling Function (MSF)	https://datatracker.ietf.org/doc/rfc9033/	This specification defines the "IPv6 over the TSCH mode of IEEE 802.15.4" (6TiSCH) Minimal Scheduling Function (MSF). This Scheduling Function describes both the behavior of a node when joining the network and how the communication schedule is managed in a distributed fashion. MSF is built upon the 6TiSCH Operation Sublayer Protocol (6P) and the minimal security framework for 6TiSCH.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 9034 Packet Delivery Deadline Time in the Routing Header for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	https://datatracker.ietf.org/doc/rfc9034/	This document specifies a new type for the 6LoWPAN routing header containing the deadline time for data packets, designed for use over constrained networks. The deadline time enables forwarding and scheduling decisions for time-critical machine-to-machine (M2M) applications running on Internet-enabled devices that operate within time-synchronized networks. This document also specifies a representation for the deadline time values in such networks.	S2.7
IETF	IETF RFC 9035 A Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration Option for the 6LoWPAN Routing Header	https://datatracker.ietf.org/doc/rfc9035/	This document updates RFC 8138 by defining a bit in the Routing Protocol for Low-Power and Lossy Networks (RPL) Destination-Oriented Directed Acyclic Graph (DODAG) Configuration option to indicate whether compression is used within the RPL Instance and to specify the behavior of nodes compliant with RFC 8138 when the bit is set and unset.	S2.7
IETF	IETF RFC 9037 Deterministic Networking (DetNet) Data Plane: MPLS over IEEE 802.1 Time-Sensitive Networking (TSN)	https://datatracker.ietf.org/doc/rfc9037/	This document specifies the Deterministic Networking (DetNet) MPLS data plane when operating over an IEEE 802.1 Time-Sensitive Networking (TSN) sub-network.	S2.7
IETF	IETF RFC 9039 Uniform Resource Names for Device Identifiers	https://datatracker.ietf.org/doc/rfc9039/	This document describes a new Uniform Resource Name (URN) namespace for hardware device identifiers. A general representation of device identity can be useful in many applications, such as in sensor data streams and storage or in equipment inventories. A URN-based representation can be passed along in applications that need the information.	S2.2, S2.17
IETF	IETF RFC 9055 Deterministic Networking (DetNet) Security Considerations	https://datatracker.ietf.org/doc/rfc9055/	This document addresses DetNet-specific security considerations from the perspectives of both the DetNet system-level designer and component designer.	S2.6, S2.9
IETF	IETF RFC 9056 Deterministic Networking (DetNet) Data Plane: IP over MPLS	https://datatracker.ietf.org/doc/rfc9056/	This document specifies the Deterministic Networking data plane when encapsulating IP over an MPLS packet-switched network.	S2.5
IETF	IETF RFC 9090 Concise Binary Object Representation (CBOR) Tags for Object Identifiers	https://datatracker.ietf.org/doc/rfc9090/	This document defines CBOR tags for object identifiers (OIDs) and is the reference document for the IANA registration of the CBOR tags so defined.	S2.2

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF RFC 9100 Sensor Measurement Lists (SenML) Features and Versions	https://datatracker.ietf.org/doc/rfc9100/	This short document updates RFC 8428, "Sensor Measurement Lists (SenML)", by specifying the use of independently selectable "SenML Features" and mapping them to SenML version numbers.	S2.2
IETF	IETF RFC 9124 A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices	https://datatracker.ietf.org/doc/rfc9124/	This document describes the information that must be present in the manifest.	S2.1
IETF	IETF RFC 9159 IPv6 Mesh over BLUETOOTH(R) Low Energy Using the Internet Protocol Support Profile (IPSP)	https://datatracker.ietf.org/doc/rfc9159/	RFC 7668 describes the adaptation of IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) techniques to enable IPv6 over Bluetooth Low Energy (Bluetooth LE) networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth LE links established by using the Bluetooth Internet Protocol Support Profile (IPSP). This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.	S2.7
IETF	IETF RFC 9164 Concise Binary Object Representation (CBOR) Tags for IPv4 and IPv6 Addresses and Prefixes	https://datatracker.ietf.org/doc/rfc9164/	This specification defines two Concise Binary Object Representation (CBOR) tags for use with IPv6 and IPv4 addresses and prefixes.	S2.1
IETF	IETF RFC 9165 Additional Control Operators for the Concise Data Definition Language (CDDL)	https://datatracker.ietf.org/doc/rfc9165/	The present document defines a number of control operators that were not yet ready at the time RFC 8610 was completed: .plus, .cat, and .det for the construction of constants; .abnf/.abnfb for including ABNF (RFC 5234 and RFC 7405) in CDDL SPecifications; and .feature for indicating the use of a non-basic feature in an instance.	S2.1
IETF	IETF RFC 9175 Constrained Application Protocol (CoAP): Echo, Request-Tag, and Token Processing	https://datatracker.ietf.org/doc/rfc9175/	This document specifies enhancements to the Constrained Application Protocol (CoAP) that mitigate security issues in particular use cases.	S2.2
IETF	IETF RFC 9222 Guidelines for Autonomic Service Agents	https://datatracker.ietf.org/doc/rfc9222/	This document proposes guidelines for the design of Autonomic Service Agents for autonomic networks.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	(NEW) IETF draft-nichols-iotops-defined-trust-transport Defined-Trust Transport (DeftT) Protocol for Limited Domains	https://datatracker.ietf.org/doc/draft-nichols-iotops-defined-trust-transport/	This document describes a broadcast-oriented, many-to-many Defined- trust Transport (DeftT) framework that makes it simple to express and enforce application and deployment specific integrity, authentication, access control and behavior constraints directly in the protocol stack. DeftT enables secure and completely self-contained (e.g., no external identity servers or certificate authorities) overlay networks where credentialed members can join and leave at any time. DeftT is part of a Defined-trust Communications approach with a specific example implementation available. Combined with IPv6 multicast and modern hardware-based methods for securing keys and code, it provides an easy to use foundation for secure and efficient communications in Limited Domains (RFC8799), in particular for Operational Technology (OT) networks	S2.10
IETF	(NEW) IETF draft-walther-iotops-iot-ops IoT Operational Issues	https://datatracker.ietf.org/doc/draft-walther-iotops-iot-ops/	This I-D is based on a presentation at IETF 119 in the IOTOPS WG.	S2.14
IETF	(NEW) IETF draft-li-iotops-intelligent-security Intelligent Protection Optimization System for IOT	https://datatracker.ietf.org/doc/draft-li-iotops-intelligent-security/	Communication technology is becoming more and more developed, the Internet of Things coverage is becoming more and more comprehensive, and a large number of data and devices are joining, which also makes more data security and privacy issues appear. Therefore, this draft proposes a scheme to build an information-centered network. By analyzing common network attack methods, an intelligent protection optimization system is established from three aspects: naming and parsing, data exchange, and data caching, so as to achieve better content privacy protection without adding additional costs.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
IETF	(NEW) IETF draft-ietf-iotops-security-summary A summary of security-enabling technologies for IoT devices	https://datatracker.ietf.org/doc/draft-ietf-iotops-security-summary/	The IETF has developed security technologies that help to secure the Internet of Things even over constrained networks and when targetting constrained nodes. These technologies can be used independently or can be composed into larger systems to mitigate a variety of threats. This documents illustrates an overview over these technologies and highlights their relationships. Ultimately, a threat model is presented as a basis to derive requirements that interconnect existing and emerging solution technologies.	S2.6
IETF	(NEW) IETF draft-irtf-t2trg-taxonomy-manufacturer-anchors A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors	https://datatracker.ietf.org/doc/draft-irtf-t2trg-taxonomy-manufacturer-anchors/	This document provides a taxonomy of methods used by manufacturers of silicon and devices to secure private keys and public trust anchors. This deals with two related activities: how trust anchors and private keys are installed into devices during manufacturing, and how the related manufacturer held private keys are secured against disclosure.	S2.10
IETF	(NEW) IETF draft-ietf-scitt-software-use-cases Detailed Software Supply Chain Uses Cases for SCITT	https://datatracker.ietf.org/doc/draft-ietf-scitt-software-use-cases/	This document includes a collection of representative Software Supply Chain Use Cases. These use cases aim to identify software supply chain problems that the industry faces today and act as a guideline for developing a comprehensive security architecture and solutions for these scenarios.	S2.17
IETF	(NEW) IETF draft-ietf-scitt-architectur An Architecture for Trustworthy and Transparent Digital Supply Chains	https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/	This document defines a generic, interoperable and scalable architecture to enable transparency across any supply chain with minimum adoption barriers. It provides flexibility, enabling interoperability across different implementations of Transparency Services with various auditing and compliance requirements. Issuers can register their Signed Statements on any Transparency Service, with the guarantee that all Auditors and Verifiers will be able to verify them	S2.10
IETF	(NEW) IETF draft-ietf-scitt-scrapi SCITT Reference APIs	https://datatracker.ietf.org/doc/draft-ietf-scitt-scrapi/	This document describes a REST API that supports the normative requirements of the SCITT Architecture. Optional key discovery and query interfaces are provided to support interoperability issues with Decentralized Identifiers, X509 Certificates and Artifact Reposistories.	S2.2

Table 12: AIOTI/EUOS indentified IoT challenges covered/addressed by IRTF

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IRTF	(Updated) IRTF draft-choi-icnrg-aiot Requirements and Challenges for User-level Service Managements of IoT Network by utilizing Artificial Intelligence	https://datatracker.ietf.org/doc/draft-choi-icnrg-aiot/	This document describes the requirements and challenges to employ artificial intelligence (AI) into the constraint Internet of Things (IoT) service environment for embedding intelligence and increasing efficiency.	S2.14
IRTF	(Updated) IRTF draft-irtf-t2trg-rest-iot Guidance on RESTful Design for Internet of Things Systems	https://datatracker.ietf.org/doc/draft-irtf-t2trg-rest-iot/	This document gives guidance for designing Internet of Things (IoT) systems that follow the principles of the Representational State Transfer (REST) architectural style. This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).	S2.2
IRTF	(Updated) IRTF draft-irtf-t2trg-secure-boot-strapping Terminology and processes for initial security setup of IoT devices	https://datatracker.ietf.org/doc/draft-irtf-t2trg-secure-bootstrapping/	This document provides an overview of terms that are commonly used when discussing the initial security setup of Internet of Things (IoT) devices. This document also presents a brief but illustrative survey of protocols and standards available for initial security setup of IoT devices.	S2.7
IRTF	IRTF RFC 8576 Internet of Things (IoT) Security: State of the Art and Challenges	https://datatracker.ietf.org/doc/rfc8576/	In this document, This document first discuss the various stages in the lifecycle of a thing. Next, we document the security threats to a thing and the challenges that one might face to protect against these threats. Lastly, we discuss the next steps needed to facilitate the deployment of secure IoT systems.	S2.6
IRTF	IRTF RFC 8691 Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11	https://datatracker.ietf.org/doc/rfc8691/	This document provides methods and settings for using IPv6 to communicate among nodes within range of one another over a single IEEE 802.11-OCB link.	S2.7
IRTF	IRTF RFC 9139 Information-Centric Networking (ICN) Adaptation to Low-Power Wireless Personal Area Networks (LoWPANs)	https://datatracker.ietf.org/doc/rfc9139/	This document defines a convergence layer for Content-Centric Networking (CCNx) and Named Data Networking (NDN) over IEEE 802.15.4 Low-Power Wireless Personal Area Networks (LoWPANs)	S2.16

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IRTF	(NEW) IETF draft-irtf-t2trg-security-setup-iot-devices Terminology and processes for initial security setup of IoT devices	https://datatracker.ietf.org/doc/draft-irtf-t2trg-security-setup-iot-devices/	This document provides a taxonomy of methods used by manufacturers of silicon and devices to secure private keys and public trust anchors. This deals with two related activities: how trust anchors and private keys are installed into devices during manufacturing, and how the related manufacturer held private keys are secured against disclosure.	S2.6

Table 13: AIOTI/EUOS indentified IoT challenges covered/addressed by oneM2M

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	**URL**	**Abstract**	**Labels & Sections**
oneM2M	oneM2M-TS-0036-V-0.0.1 Advanced Vehicular Domain Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=24640	Advanced Vehicular Domain Enablement.	S2.7
oneM2M	oneM2M-TR-0041-V-0.4.0 oneM2M Decentralized Authentication	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26293	Technical Report of oneM2M Decentralized Authentication.	S2.6
oneM2M	oneM2M-TR-0042-V-0.4.0 WoT Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=26945	This technical report identifies the interworking scenarios and and its requirements between oneM2M and W3C Web of Things systems and analyze possible architectural solutions to address the requirements.	S2.7
oneM2M	oneM2M TR-0001-V4.3.0 Use Cases Collection	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28153	This oneM2M Technical Report includes a collection of use cases from various M2M industry segments. Use cases focus on the sequence of interactions among actors, and may include potential requirements.	S2.22
oneM2M	oneM2M-TR-0058-V-0.0.1: Railway Domain Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=28240	This Technical Report investigates how to enable oneM2M system working in the railway vertical domain. This TR includes use cases, studies on essential features and summaries of other standards organizations on the railway vertical domain for the next oneM2M release(s) which considers and supports railway domain devices and services.	S2.7
oneM2M	oneM2M TS-0002-V4.6.0 Requirements	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=29274	The present document contains an informative functional role model and normative technical requirements for oneM2M.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TR-0018-V-4.0.0 Industrial Domain Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=29334	This oneM2M Technical Report collects the use cases of the industrial domain and the requirements needed to support them collectively. Furthermore, the Technical Report also identifies necessary technical work needing to be addressed while enhancing future oneM2M specifications.	S2.1
oneM2M	oneM2M-TR-0059-V-0.2.0 oneM2M Services and Platforms Discovery	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30111	The document is describing what services and platforms discovery scenarios are considered beneficial from a oneM2M standpoint and how these can be supported by oneM2M system. Based on the result of the technical report, it will identify possible advanced features and enhancements which the next oneM2M release(s) could support.	S2.22
oneM2M	oneM2M-TR-0043-V-0.2.0 Modbus Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30112	This technical report investigates oneM2M and modbus interworking scenarios and proposes possible solutions to support the interworking scenarios.	S2.7
oneM2M	oneM2M TS-0005-V4.0.0 Management Enablement (OMA)	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30113	Specifies the usage of OMA DM and OMA LwM2M resources and the corresponding message flows including normal cases as well as error cases to fulfill the oneM2M management requirements.	S2.22
oneM2M	oneM2M TS-0006-V4.0.0 Management enablement (BBF)	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30114	Specifies the usage of the BBF TR-069 protocol and the corresponding message flows including normal cases as well as error cases to fulfil the oneM2M management requirements.	S2.22
oneM2M	oneM2M TR-0049-V-0.3.0 Industrial Domain Information Model Mapping & Semantics Support	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30216	Industrial Domain Information Model Mapping & Semantics Support.	S2.1
oneM2M	oneM2M TR-0055-3GPP_V2X_Interworking-V0_5_0 3GPP V2X Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30468	The document is a study of interworking between oneM2M Architecture and 3GPP V2X architecture so that oneM2M can support V2X service for the benefit of IoT applications.	S2.7
oneM2M	oneM2M WI-0095 System enhancements to support Data Protection Regulations	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=30968	Proposes a work item to study oneM2M system enhancement to support data protection regulations such as General Data Protection Regulation from EU.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TR-0033-Study_on_Enhanced_Semantic_Enablement-V4_5_0 Study on Enhanced Semantic Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31093	In this study requirements on enhanced semantic enablement and approaches for addressing these requirements will be developed and discussed. The intention is to achieve agreement between the interested participants on the approaches to be pursued in oneM2M. On this basis normative contributions to Technical Specifications can then be made.	S2.18
oneM2M	oneM2M TR-0063-V-0.0.1 Effective IoT Communication to Protect 3GPP Networks	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31370	This work item describes how a oneM2M service layer hosted on a 3GPP Cellular IoT device can implement the requirements defined in GSMA TS.34 to ensure that a device does not operate in a manner that can impair the 3GPP Cellular network.	S2.7
oneM2M	oneM2M TS-0011-V4.1.0 Common Terminology	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31396	This TS contains a collection of specific technical terms (definitions and abbreviations) used within oneM2M .	S2.7
oneM2M	oneM2M-TR-0026-V-4.8.0 Vehicular Domain Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31410	This oneM2M Technical Report examines how the current oneM2M System can be used in the Vehicular Domain and includes a study of advanced features which the future oneM2M release(s) could support for this vertical domain.	S2.7
oneM2M	oneM2M TS-0034-V4.2.0 Semantics Support	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31425	This specification provides normative text for semantic enablement in oneM2M.	S2.18
oneM2M	oneM2M-TR-0044-V-0.6.0 Physical object heterogeneous identification and tracking in oneM2M	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31631	This technical report investigates the various IoT ID standards and application requirements, discussion on how to be compatible with the IoT ID standards, and providing the heterogeneous identification and tracking services.	S2.7
oneM2M	oneM2M-TR-0053-V-0.6.0 Lightweight oneM2M Services	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31776	The document is a study of lightweight oneM2M services. Based on the result of the study, it identifies proposed optimizations and enhancements to the oneM2M system to streamline and optimize its features and services.	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TR-0024-V4.3.0 3GPP_Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31840	The document is a study of interworking between oneM2M Architecture and 3GPP Rel-16 architecture for Service Capability Exposure as defined in TS 23.682.	S2.7
oneM2M	oneM2M TR-0060-V-0.2.0 Study of action triggering enhancements	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=31865	This work item defines how to autonomously send a series of commands to trigger actions based on the configuration of conditions by M2M application. As the extension to the previous work TR-0021, this TR focuses on Complex Event Processing support in oneM2M.	S2.14
oneM2M	oneM2M-TR-0050-V-0.13.0 Attribute Based Access Control Policy	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32114	This work item develops attribute based access control policy scheme and the corresponding access control policy management mechanism in oneM2M System.	S2.6
oneM2M	oneM2M WI-0102 System enhancements to support Data License Management	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32157	Proposes a work item to study oneM2M system enhancement to support data license management.	S2.22
oneM2M	oneM2M-TR-0054-V-0.8.0 oneM2M Service Subscribers and Users	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32207	This document is a study on the definition of oneM2M service subscribers and their authorized users. This study explores use cases which require oneM2M service subscribers and users. The study also analyses different solutions to support oneM2M service subscribers and users.	S2.22
oneM2M	oneM2M-TR-0064 ZigBee Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32243	This technical report investigates oneM2M and ZigBee interworking scenarios and proposes possible solutions to support the interworking scenarios.	S2.7
oneM2M	oneM2M TS-0040-V0.1.0 Modbus Interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32500	The present document specifies the oneM2M and Modbus interworking technologies that enable Modbus devices and oneM2M entities produce/consume services. This includes the interworking architecture model that describes where the Modbus Interworking Proxy Entity (IPE) is hosted and how the IPE is composed with. This document describes Modbus services to oneM2M resource mapping structure and rules, followed by describing detailed interworking procedures.	S2.7

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TS-0037-V-0.9.0 IoT Public Warning Service Enablement	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32830	This technical specification specifies the information model of the public warning service, and defines the resource mapping rule for the information model of the public warning.	S2.14
oneM2M	oneM2M TR-0046-V-0.9.0 Study on Public Warning Service Enabler	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=32834	The present document studies public warning service enabler for oneM2M system including case studies of similar/existing solutions, oneM2M use cases and requirements, possible architecture enhancement, and security analysis. Also, this TR suggests abstract data models for public warning service over IoT technologies.	S2.14
oneM2M	oneM2M WI-0096 Effective IoT Communication to Protect 3GPP Networks	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33091	This Work Item is intended to produce a specification that describes how a oneM2M service layer hosted on a 3GPP Cellular IoT device ensures that the device operates in an efficient manner that applies the requirements described by GSMA TS.34.	S2.7
oneM2M	oneM2M TR-0062-V-0.3.0 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33146	The document is describing state of the art privacy related regulations and their features followed by gap analysis to find out what features are supported and not supported by the current oneM2M system. Based on the result of the technical report, it will identify possible enhancement features to support data protection regulations which the next oneM2M release(s) could support.	S2.6
oneM2M	oneM2M TS-0026-V4.6.0 3GPP Interworking between oneM2M service layer and 3GPP features	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33174	This document specifies interworking between oneM2M service layer and 3GPP features, so that some 3GPP features can be exposed to oneM2M service layer for the benefit of IoT applications, and viceversa.	S2.7
oneM2M	oneM2M WI-0104 V0_0_1 SDT based Information Model and Mapping for Vertical Industries – SIMVI	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33391	The purpose of this Work Item is to enable the continuation of contributions of Information Models including ModuleClasses and Device models from various domains for TS-0023.	S2.1
oneM2M	oneM2M-TR-0057-V-0.6.0 Getting Started with oneM2M	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33407	Getting Started with oneM2M.	S2.22

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TR-0066-V-0.3.0 System Enhancement to Support Data License Management (DLM)	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33583	The document is analysing existing data license schemes and how these licenses are being used in existing data management platforms to understand essential functions to utilize data license in the oneM2M system. Based on the result of the technical report, it will identify potential requirements and key features to support data license management in the oneM2M system.	S2.22
oneM2M	oneM2M WI-0105 System enhancements to support AI capabilities	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33772	This work item aims to enable oneM2M to utilize Artificial Intelligence models and data management for AI services.	S2.15
oneM2M	oneM2M- TS-0023-V4.8.0 SDT based Information Model and Mapping for Vertical Industries	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33779	This technical specification includes oneM2M defined information model for home appliances and the mapping with other information models from external organization.	S2.1
oneM2M	oneM2M TR-0067-V-0.2.0 Study on Management Object migration to SDT	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33846	The document is a study of how SDT <flexContainer> type resources could replace <mgmtObj> resources in the future.	S2.22
oneM2M	oneM2M TS-0013-V.4.0.0 Interoperability Testing	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=33896	The specification address the testing of the primitives on the oneM2M interfaces as specified in TS-0001 and TS-0004. The purpose of the interoperability testing is to prove end-to-end functionality between Application Entities and Common Service Entities over the Mca and Mcc reference points.	S2.7
oneM2M	oneM2M TS-0008- V-4.2.0 CoAP Protocol Binding	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34132	The specification will cover the protocol specific part of communication protocol used by oneM2M compliant systems as 'CoAP binding'.	S2.7
oneM2M	oneM2M TS-0003-V4.6.0 Security Solutions	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34191	The TS defines security solutions for M2M systems.	S2.6

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M TR-0068-V-0.2.0 AI enablement to oneM2M	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34206	The document is analysing existing AI/ML technologies that can be resourced into oneM2M architecture. The document is also investigating potential AI/ML service use cases that use data collected in the oneM2M system. The study on existing AI/ML technologies and use cases are further analysed in this document to understand what features are supported and unsupported by the oneM2M system. Based on the result of this technical report, it will identify potential requirements and key features to enable AI/ML in the oneM2M system.	S2.15
oneM2M	oneM2M TR-0065 V0.1.0 oneM2M-SensorThings API interworking	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34408	This document investigates in oneM2M-to-SensorThings API interworking.	S2.2
oneM2M	oneM2M TS-0009-V4.4.0 HTTP Protocol Binding	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34550	HTTP Protocol Binding TS.	S2.2
oneM2M	oneM2M WI-0109 IPE-based Device Management with FlexContainers	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34558	Propose a work item for Device Management (DMG) with IPE-based approach with FlexContainers.	S2.22
oneM2M	oneM2M TS-0004-V4.9.0 Service Layer Core Protocol	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34618	The present document specifies the communication protocol(s) for oneM2M compliant Systems, M2M Applications, and/or other M2M Systems. The present document also specifies common data formats, interfaces and message sequences to support reference points(s) defined by oneM2M.	S2.7
oneM2M	oneM2M TS-0001-V4.14.0 Functional Architecture	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34648	This document specifies the functional architecture for the oneM2M Services Platform.	S2.7
oneM2M	(New) oneM2M TS-0002-V5.1.0 Requirements	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=36546	The present document contains an informative functional role model and normative technical requirements for oneM2M.	S2.14

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
oneM2M	oneM2M-TS-0018-V-4.6.0 Test Suite Structure and Test Purposes	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34702	The Test Suite Structure and Test Purposes document for conformance testing consists of: Defining the test suite structure by grouping the test purposes according to different criteria; Specifing test purposes for conformance test. A test purpose is an informal description of the expected test behaviour.	S2.7
oneM2M	oneM2M-TR-0061 -V-0.3.0 Study on ontologies for Smart City Services	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34704	Study on ontologies for Smart City Services.	S2.1
oneM2M	oneM2M TS-0022-V4_3_0 Field Device Configuration	https://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=34724	Field Device Configuration TS.	S2.7

Table 14: AIOTI/EUOS indentified IoT challenges covered/addressed by OMA

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	(Updated) OMA IPSO IPSO Smart Object Guidelines	https://omaspecworks.org/develop-with-oma-specworks/ipso-smart-objects/guidelines/	IPSO Smart Object Guidelines provide a common design pattern, an object model, that can effectively use the IETF CoAP protocol to provide high level interoperability between Smart Object devices and connected software applications on other devices and services.	S2.1, S2.22
OMA	(Updated) OMA IPSO Repo Public IPSO Repository	https://technical.openmobilealliance.org/OMNA/LwM2M/LwM2MRegistry.html	The IPSO Smart Object Registry registry is intended for developers that are building products based on IPSO Objects, it is not intended to be used at runtime by applications.	S2.1, S2.22
OMA	OMA-AD-CPNS-V1_1-20160209-A Converged Personal Network Service Architecture	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-AD-CPNS-V1_1-20160209-A.pdf	The scope of the CPNS (Converged Personal Network Service) architecture document is to define the architecture for the CPNS v1.1 Enabler. This document provides the functional capabilities needed to support the Enabler as described in CPNS requirements document [CPNS-RD].	S2.7
OMA	OMA-ERELD-CPNS-V1_1-20160209-A Enabler Release Definition for Converged Personal Network Service	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-ERELD-CPNS-V1_1-20160209-A.pdf	The scope of this document is limited to the Enabler Release Definition of Converged Personal Network Service (CPNS) enabler according to OMA Release process and the Enabler Release specification baseline listed in section 5. The CPNS Enabler enables CPNS entities in a personal network (PN) to consume services within that PN, services from and to other PNs, and services provided by service providers outside the PN.	S2.14
OMA	OMA-RD-CPNS-V1_1-20160209-A Converged Personal Network Service Requirements	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-RD-CPNS-V1_1-20160209-A.pdf	This Requirement Document (RD) defines the requirements for the Converged Personal Network Service-CPNS 1.1 and deferred requirements that can be used as a base for future version of CPNS. The CPNS Enabler enables CPNS entities in a personal network (PN) to consume services within that PN, services from and to other PNs, and services provided by service providers outside the PN.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-TS-CPNS_Core-V1_1-20160209-A Converged Personal Network Service Core Technical Specification	https://www.openmobilealliance.org/release/CPNS/V1_1-20160209-A/OMA-TS-CPNS_Core-V1_1-20160209-A.pdf	This document specifies the functions, interfaces and behaviour of CPNS entities, then protocols and CPNS System concept together with syntax and semantics of CPNS messages.	S2.22
OMA	OMA-TS-REST_NetAPI_DeviceCapabilities-V1_0_1-20151123-A RESTful Network API for Device Capabilities	https://www.openmobilealliance.org/release/DevCapREST/V1_0_1-20151123-A/OMA-TS-REST_NetAPI_DeviceCapabilities-V1_0_1-20151123-A.pdf	This specification defines a RESTful Device Capabilities API using an HTTP protocol binding, based on the similar API defined in [3GPP 29.199-18].	S2.2
OMA	OMA-AD-DM-V2_0-20160209-A Device Management Architecture	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-AD-DM-V2_0-20160209-A.pdf	The scope of the Device Management architecture document is to define the architecture for the Device Management v2.0 enabler. This document fulfils the functional capabilities and information flows needed to support this enabler as described in the Device Management requirements document.	S2.22
OMA	OMA-ERELD-DM-V2_0-20160209-A Enabler Release Definition for OMA Device Management	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-ERELD-DM-V2_0-20160209-A.pdf	The scope of this document is limited to the Enabler Release Definition of OMA Device Management v2.0 according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA-RD-DM-V2_0-20160209-A Device Management Requirements	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-RD-DM-V2_0-20160209-A.pdf	This document contains use cases and requirements for Device Management 2.0. It describes a set of functional requirements for the management of a Device. These functional requirements MAY be overlapped with the requirements for DM 1.x Enabler.	S2.22
OMA	OMA-TS-DM_Protocol-V2_0-20160209-A OMA Device Management Protocol	https://www.openmobilealliance.org/release/DM/V2_0-20160209-A/OMA-TS-DM_Protocol-V2_0-20160209-A.pdf	This protocol is called the OMA Device Management Protocol version 2.0, and it defines the protocol for various management procedures. The scope for this protocol is to define the interfaces that are used between the DM Server and the DM Client. Interfaces residing within the device or within the server are outside of the scope of this specification.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-RD-ENCap-M-V1_0-20180621-A Exposing Network Capabilities to M2M Requirements	https://www.openmobilealliance.org/release/ENCap/V1_0-20180621-A/OMA-RD-ENCap_M-V1_0-20180621-A.pdf	This document defines the requirements for Exposing Network Capabilities to M2M Applications and/or M2M Service Platforms through APIs. In addition, it contains: Use cases where M2M Applications and/or M2M Service Platforms can leverage network capabilities to enrich the services or to streamline the operations.; Gap analysis to identify any missing Network APIs to address the above use cases.	S2.22
OMA	OMA-RRELD-ENCap-M2M-V1_0-20180621-A Reference Release Definition for for Exposing Network Capabilities to M2M	https://www.openmobilealliance.org/release/ENCap/V1_0-20180621-A/OMA-RRELD-ENCap_M2M-V1_0-20180621-A.pdf	The scope of this document is limited to the Referencer Release Definition of ENCap-M2M according to OMA Release process and the Reference Release specification baseline listed in section 5.	S2.22
OMA	OMA-AD-FUMO-V1_0-20070209-A Firmware Update Management Object Architecture	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-AD-FUMO-V1_0-20070209-A.pdf	The scope of this document is the architecture for the Firmware Update Management Object (FUMO) specifications. In general, the scope includes the DM server environment, download mechanisms and devices.	S2.22
OMA	OMA-ERELD-FUMO-V1_0_4-20090828-A Enabler Release Definition for Firmware Update Management Object	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-ERELD-FUMO-V1_0_4-20090828-A.pdf	The scope of this document is limited to the Enabler Release Definition of Firmware Update Management Object specifications according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA-RD-DM-V1_2-20070209-A Device Management Requirements	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-RD-DM-V1_2-20070209-A.pdf	The scope of this document is a requirements description for Device Management (for the definition of Device see section 3.2). This document describes a set of functional requirements (partly on an abstract level) for the management of a Device's changeable parameters, as seen from the Management Authority's points of view.	S2.22
OMA	OMA-TS-DM-FUMO-V1_0_2-20090828-A Firmware Update Management Object	https://www.openmobilealliance.org/release/FUMO/V1_0_4-20090828-A/OMA-TS-DM_FUMO-V1_0_2-20090828-A.pdf	This document specifies management object(s) and their necessary behaviour to support the updating of firmware in mobile devices. It leverages the OMA DM enabler [OMADM] and supports alternate download mechanisms (such as OMA Download [DLOTA]). This represents the interface between the client and server required to manage the update of a mobile device's firmware.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-ER-GotAPI-V1_1-20180724-A Generic Open Terminal API Framework (GotAPI)	https://www.openmobilealliance.org/release/GOTAPI/V1_1-20180724-A/OMA-ER-GotAPI-V1_1-20180724-A.pdf	This Enabler Release (ER) document is a combined document that includes requirements, architecture and technical specification of the Generic Open Terminal API Framework (GotAPI) Enabler.	S2.2, S2.22
OMA	OMA-AD-GwMO-V1_1-20170725-A Gateway Management Object Architecture	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-AD-GwMO-V1_1-20170725-A.pdf	The scope of the Gateway Management Object architecture document is to define the architecture for the DM Gateway Management Object v1.1 enabler. This document fulfills the functional capabilities and information flows needed to support this enabler as described in the Gateway Management Object requirements document [GwMO-RD].	S2.22
OMA	OMA-ERELD-GwMO-V1_1-20170725-A Enabler Release Definition for Gateway Management Object (GwMO)	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-ERELD-GwMO-V1_1-20170725-A.pdf	The scope of this document is limited to the Enabler Release Definition of Gateway Management Object (GwMO v1.1) according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA-RD-GwMO-V1_1-20170725-A GwMO Requirements	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-RD-GwMO-V1_1-20170725-A.pdf	This document lists the complete set of requirements for the OMA DM Gateway Management Object Enabler v1.1. It includes all the requirement of the OMA DM GatewayMO v1.0. It mainly focuses on requirements to enable a DM Server to manage devices that are not directly accessible to the OMADM Server (for example, because the devices are deployed behind a firewall or because the devices do not support the OMA DM protocol). This document also provides requirements for management of devices in a Machine to Machine (M2M) ecosystem (for example, fanning out DM commands from a DM Server to multiple End Devices and aggregating responses from multiple End Devices so that a consolidated response is sent back to the DM Server).	S2.22
OMA	OMA-TS-DM-GwMO_ZigBeeMO-V1_0-20170725-A Management Objects for ZigBee Devices	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO_ZigBeeMO-V1_0-20170725-A.pdf	This document defines an OMA DM management object (data model) to represent ZigBee devices. This ZigBee MO models specific parameters used to represent a specific ZigBee device and should be used together with GwMO TS v1.1 [GwMOTS]. This ZigBee MO is optional for any OMA DM Gateway implementation.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-TS-GwMO-V1_1-20170725-A Gateway Management Object Technical Specification	https://www.openmobilealliance.org/release/GwMO/V1_1-20170725-A/OMA-TS-GwMO-V1_1-20170725-A.pdf	This technical specification describes Management Objects and Generic Alerts that are needed to provide the DM Gateway functionality, as defined in [DMDICT].	S2.22
OMA	OMA-ETS-LightweightM2M_INT-V1_1-20190912-D Enabler Test Specification (Interoperability) for Lightweight M2M	https://www.openmobilealliance.org/release/LightweightM2M/ETS/OMA-ETS-LightweightM2M-V1_1-20190912-D.pdf	This document describes in detail available test cases for LightweightM2M as specified in OMA-TS-LightweightM2MV1_1-20180710-A and OMA-TS-LightweightM2M_Transport-V1_1-20180710-A.	S2.22
OMA	OMA-EVP-LightweightM2M-V1_0-20140819-C Enabler Validation Plan for Lightweight M2M	https://www.openmobilealliance.org/release/LightweightM2M/EVP/OMA-EVP-LightweightM2M-V1_0-20140819-C.pdf	This document details the Validation plan for the Lightweight M2M V1.0 Enabler Release. The successful accomplishment of the validation activities will be required for the Enabler to be considered for Approved status.	S2.22
OMA	(Updated) OMA-ERELD-Lightweight M2M-V1_2_2-20240613 Enabler Release Definition for LightweightM2M	https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-ERELD-LightweightM2M-V1_2_2-20240613-A.pdf	The scope of this document is limited to the Enabler Release Definition of LightweightM2M v1.2.2 according to OMA Release process and the Enabler Release specification baseline.	S2.22
OMA	OMA-RD-Lightweight M2M-V1_2-20201110 -A OMA Lightweight Machine to Machine Requirements	https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-RD-LightweightM2M-V1_2-20201110-A.pdf	This document represents Lightweight M2M version 1.2 consolidated requirements.	S2.22
OMA	(Updated) OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A Lightweight Machine to Machine Technical Specification: Core	https://www.openmobilealliance.org/release/LightweightM2M/V1_2_2-20240613-A/OMA-TS-LightweightM2M_Core-V1_2_2-20240613-A.pdf	The scope of this document is limited to the Enabler Release Definition of LightweightM2M v1.2.2 according to OMA Release process and the Enabler Release specification baseline.	S2.22
OMA	OMA-TS-LightweightM2M_Transport-V1_2-20201110-A Ligh tweight Machine to Machine Technical Specification: Transport Bindings	https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-TS-LightweightM2M_Transport-V1_2-20201110-A.pdf	This document specifies the transport bindings of the Lightweight Machine-to-Machine (LwM2M) protocol version 1.2. The split between the LwM2M core [LwM2M-CORE] and the transport binding specification improves readability, allows a cleaner separation between the LwM2M messaging layer and the underlying protocols for conveying these messages, and ultimately better extensibility.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-ERELD-LWM2M_BinaryAppData Cont-V1_0_1-20190221-A Enabler Release Definition for LwM2M BinaryAppDataCont	https://www.openmobilealliance.org/release/LwM2M_APPDATA/V1_0_1-20190221-A/OMA-ERELD-LWM2M_BinaryAppDataCont-V1_0_1-20190221-A.pdf	The scope of this document is limited to the Enabler Release Definition of LwM2M BinaryAppDataCont according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA-TS-LWM2M_BinaryApp DataContainer-V1_0_1-20190221-A Lightweight M2M – Binary App Data Container	https://www.openmobilealliance.org/release/LwM2M_APPDATA/V1_0_1-20190221-A/OMA-TS-LWM2M_BinaryAppDataContainer-V1_0_1-20190221-A.pdf	This document defines an Object to be used to transfer Application Data with the Lightweight M2M enabler in order to manage application service data on the device.	S2.22
OMA	OMA-ERELD-LWM2M_Gateway-V1_1-20210518-A Enabler Release Definition for LWM2M Gateway	https://www.openmobilealliance.org/release/LwM2M_Gateway/V1_1-20210518-A/OMA-ERELD-LWM2M_Gateway-V1_1-20210518-A.pdf	The scope of this document is limited to the Enabler Release Definition of LWM2M_Gateway according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA-TS-LWM2M_Gateway-V1_1-20210518-A Lightweight Machine to Machine Gateway Technical Specification	https://www.openmobilealliance.org/release/LwM2M_Gateway/V1_1-20210518-A/OMA-TS-LWM2M_Gateway-V1_1-20210518-A.pdf	This specification extends the LwM2M architecture to support the LwM2M Gateway functionality.	S2.22
OMA	OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A Reference Release Definition for M2M Device Classification	https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-RRELD-M2M_Device_Classification-V1_0-20121030-A.pdf	The scope of this document is limited to the Reference Release Definition of the M2M Device Classification White Paper Reference Release according to OMA Release process and the Reference Release document baseline listed in section 5	S2.22
OMA	OMA-WP-M2M_Device_Classification-20121030-A White Paper on M2M Device Classification	https://www.openmobilealliance.org/release/M2M_Device_Classification/V1_0-20121030-A/OMA-WP-M2M_Device_Classification-20121030-A.pdf	This document is to provide a Machine-to-Machine (M2M) device classification framework based on the horizontal attributes (e.g., wide area communication interface, local area communication interface, IP stack, human I/O capabilities, persistent configuration storage) of interest to communication service providers (CSPs) and M2M service providers (MSPs), independent of vertical markets, such as smart grid, connected cars, e-health, smart home, etc.	S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-RD-M2MInterface-V1_0-20150324-A Management Interface for M2M Requirements	https://www.openmobilealliance.org/release/M2Minterface/V1_0-20150324-A/OMA-RD-M2MInterface-V1_0-20150324-A.pdf	This technical report defines requirements for an interface from Device Management (DM) server to the Machine to Machine (M2M) systems on top. This Northbound Interface (NBI) allows M2M service layer to access the DM server functionality. These requirements are derived from device and service management use cases.	S2.22
OMA	OMA-RRELD-M2Minterface-V1_0-20150324-A Reference Release Definition for M2Minterface	https://www.openmobilealliance.org/release/M2Minterface/V1_0-20150324-A/OMA-RRELD-M2Minterface-V1_0-20150324-A.pdf	The scope of this document is limited to the Enabler Release Definition of M2M interface according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.22
OMA	OMA ObjLwM-2M_5GNR_Conn LIGHT-WEIGHTM2M 5GNR CONNECTIVITY	https://www.openmobilealliance.org/release/ObjLwM2M_5GNR_Conn/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M 5GNR Connectivity v1.0.	S2.1, S2.22
OMA	OMA ObjL-wM2M_ACL LIGHT-WEIGHTM2M ACCESS CONTROL	https://www.openmobilealliance.org/release/ObjLwM2M_ACL/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Access Control v1.1	S2.1, S2.22
OMA	OMA ObjLwM2M_APN_Conn LIGHT-WEIGHTM2M APN CONNECTION PROFILE	https://www.openmobilealliance.org/release/ObjLwM2M_APN_Conn/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M APN Connection Profile v1.1.	S2.1, S2.22
OMA	OMA ObjL-wM2M_Bearer_Conn LIGHT-WEIGHTM2M BEARER SELECTION	https://www.openmobilealliance.org/release/ObjLwM2M_Bearer_Conn/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Bearer Selection v1.1.	S2.1, S2.22
OMA	OMA ObjLwM2M_Cell_Conn LIGHT-WEIGHTM2M CELLULAR CONNECTIVITY	https://www.openmobilealliance.org/release/ObjLwM2M_Cell_Conn/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Cellular Connectivity v1.1.	S2.1, S2.22
OMA	OMA ObjL-wM2M_Conn_Mon LightweightM2M Connectivity Monitoring	https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Mon/V1_3-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Connectivity Monitoring v1.3.	S2.1, S2.22
OMA	OMA ObjL-wM2M_Conn_Stat LightweightM2M Connectivity Statistics	https://www.openmobilealliance.org/release/ObjL-wM2M_Conn_Stat/V1_0_5-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Connectivity Statistics v1.0.5.	S2.1, S2.22

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA ObjLwM2M_COSE LightweightM2M COSE	https://www.openmobilealliance.org/release/ObjLwM2M_COSE/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M COSE v1.0.	S2.1, S2.22
OMA	OMA ObjLwM2M_Device LightweightM2M Device	https://www.openmobilealliance.org/release/ObjLwM2M_Device/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Device v1.2.	S2.1, S2.22
OMA	OMA ObjLwM2M_Firmware LightweightM2M Firmware Update	https://www.openmobilealliance.org/release/ObjLwM2M_Firmware/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Firmware Update v1.1.	S2.1, S2.22
OMA	OMA ObjLwM2M_Gateway LightweightM2M Gateway	https://www.openmobilealliance.org/release/ObjLwM2M_Gateway/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Gateway v1.0.	S2.1, S2.22
OMA	OMA ObjLwM2M_Location LightweightM2M Location	https://www.openmobilealliance.org/release/ObjLwM2M_Location/V1_0_3-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Location v1.0.3.	S2.1, S2.22
OMA	OMA ObjLwM2M_MQTT_Server LightweightM2M MQTT Server	https://www.openmobilealliance.org/release/ObjLwM2M_MQTT_Server/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M MQTT Server v1.0.	S2.1, S2.22
OMA	OMA ObjLwM2M_OSCORE LightweightM2M OSCORE	https://www.openmobilealliance.org/release/ObjLwM2M_OSCORE/V2_0-20211123-A/	DOCUMENT LISTING FOR SUP LightweightM2M OSCORE v2.0.	S2.1, S2.22
OMA	OMA ObjLwM2M_Routing LightweightM2M Routing	https://www.openmobilealliance.org/release/ObjLwM2M_Routing/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Routing v1.0.	S2.1, S2.22
OMA	OMA ObjLwM2M_Security LightweightM2M Security	https://www.openmobilealliance.org/release/ObjLwM2M_Security/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Security v1.2.	S2.1, S2.22
OMA	OMA ObjLwM2M_Server LightweightM2M Server	https://www.openmobilealliance.org/release/ObjLwM2M_Server/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M Server v1.2.	S2.1, S2.22
OMA	OMA ObjLwM2M_WLAN_Conn LightweightM2M WLAN Connectivity	https://www.openmobilealliance.org/release/ObjLwM2M_WLAN_Conn/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP LightweightM2M WLAN Connectivity v1.1.	S2.22
OMA	OMA-AD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Architecture	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-AD-OpenCMAPI-V1_0-20160126-A.pdf	This document provides the architecture for the OpenCMAPI Enabler. This architecture is based on the requirements as listed in the OpenCMAPI Requirement Document [OpenCMAPI-RD].	S2.2

SDO	Specification			Relevant AIOTI/EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-ERELD-OpenCMAPI-V1_0-20160126-A Enabler Release Definition for Open Connection Manager API	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-ERELD-OpenCMAPI-V1_0-20160126-A.pdf	The scope of this document is limited to the Enabler Release Definition of the Open Connection Manager API (OpenCMAPI) Enabler according to OMA Release process and the Enabler Release specification baseline listed in section 5.	S2.2, S2.22
OMA	OMA-RD-OpenCMAPI-V1_0-20160126-A Open Connection Manager API Requirements	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-RD-OpenCMAPI-V1_0-20160126-A.pdf	This document defines the requirements for the OMA Open Connection Manager API (OpenCMAPI) V1.0.	S2.2, S2.22
OMA	OMA-TS-OpenCMAPI-V1_0-20160126-A Open Connection Manager API	https://www.openmobilealliance.org/release/OpenCMAPI/V1_0-20160126-A/OMA-TS-OpenCMAPI-V1_0-20160126-A.pdf	This specification of the OpenCMAPI defines an interface, through which connection management services are made available to different applications.	S2.2, S2.22

Table 15: AIOTI/EUOS indentified IoT challenges covered/addressed by Open Source

SDO	Specification			Relevant AIOTI/ EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
Contiki	(Updated) Contiki-NG Contiki-NG, the OS for Next Generation IoT Devices	https://www.contiki-ng.org/	Contiki-NG is an operating system for resource-constrained devices in the Internet of Things. Contiki-NG contains an RFC-compliant, low-power IPv6 communication stack, enabling Internet connectivity. The system runs on a variety of platforms based on energy-efficient architectures such as the ARM Cortex-M3/M4 and the Texas Instruments MSP430. The code footprint is on the order of a 100 kB, and the memory usage can be configured to be as low as 10 kB. The source code is available as open source with a 3-clause BSD license.	S2.23
FIWARE Foundation	(Updated) FIWARE Foundation FIWARE Internet of Things Framework	https://www.fiware.org/	FIWARE Foundation drives the definition – and the Open Source implementation – of key open standards that enable the development of portable and interoperable smart solutions in a faster, easier and affordable way, avoiding vendor lock-in scenarios, whilst also nurturing FIWARE as a sustainable and innovation-driven business ecosystem.	S2.23
FIT IoT Lab	FIT IoT Lab FIT IoT-LAB Testbed The Very Large Scale Internet of Things Testbed	https://www.iot-lab.info/	IoT-LAB provides a facility suitable for testing networking with small wireless sensor devices and heterogeneous communicating objects.	S2.23
RIOT	RIOT RIOT OS The friendly Operating System for the Internet of Things	https://www.riot-os.org/	RIOT powers the Internet of Things like Linux powers the Internet. RIOT is a free, open source operating system developed by a grassroots community gathering companies, academia, and hobbyists, distributed all around the world.	S2.23

The StandICT.eu 2026 project is funded by the European Union under grant agreement no. 101091933.