standICT.2026.eu

ICT Standardisation Observatory and Support Facility in Europe

StandICT Report

IoT Standardisation Gaps

JUNE 2024

DOI Number: 10.5281/zenodo.10820731

Legal notice

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

Executive Summary

This report applies 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 and IoT standardisation community and to provide consolidated technical elements as well as guidance and recommendations.

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

Foreword by the Editor

Currently, society is experiencing a twin Green and Digital transition, which is revolutionizing several domains, including business targets, technology innovation and development and as well offering of new or enhanced services and applications. An important enabler for this twin transition is considered to be the Internet of Things (IoT). The IoT as a concept has been initiated more than two decades ago. IoT can be considered to be a system that interconnects heterogeneous technologies supporting our daily needs impacting on a large scale our lives as well as the way we do business, locally and globally. IoT systems and IoT applications have been implemented and deployed in almost all vertical industry domains, such as Health, Industry & Manufacturing, Agriculture, Finance, Mobility, Energy, Public safety, Buildings and Cities. Successful deployment of IoT technologies and IoT applications demands standards and protocols.

The development and promotion of these standards and protocols is a cooperative undertaking between governments, academia, industry and the public interest. This depends largely on the work and activities accomplished in SDOs (Standards Development Organizations), Alliances and OSS (Open-Source Software) initiatives.

This report complements the EUOS StandICT.eu Landscape of Internet of Things (IoT) Standards report by presenting an approach reported in AIOTI, for the definition and identification of key IoT standardisation gaps in several key SDO initiatives.

In particular, the TWG IIoT and Edge team members who have collated this report, addressed the work done within the relevant SDOs, which are recommended to cooperate in order to solve these IoT standardisation gaps.

StandICT.eu and the team of TWG IIoT and Edge thanks the European Commission for supporting this work that promotes a structured discussion within the EUOS and IoT standardisation community and to provide consolidated technical elements as well as guidance and recommendations and to provide an approach for the definition and identification of key IoT standardisation gaps in several key SDO initiatives.

By the Editor: Georgios Karagiannis

Foreword by the European Commission

The Internet of Things (IoT) continues to evolve rapidly, driving digital innovation across various sectors worldwide, including mobility, energy, agriculture, manufacturing and more. Over the past two decades, IoT has emerged as a critical component of the twin Green and Digital transition, revolutionizing business models, technological advancements, and service offerings.

To realize the green and digital transition, Europe needs to step up its investments in IoT and connectivity, facilitating data access, create value in orchestrating multi-tiered data processing with control and automation on the edge, and make proactive investments in distributed edge computing infrastructures to ensure that they can scale fast enough. IoT and edge computing will play a significant role in the future of our businesses, economy and society.

As we navigate through these transformations, for European investments to deliver in a fast-paced technological scenario, it becomes increasingly evident that the successful deployment of IoT and edge technologies and applications relies heavily on robust open standards for virtualization, interoperability and secure and trusted data sharing between different stakeholders of the value chain.

This recent report from StandICT.eu on IoT standardization gaps, which complements the Landscape of Internet of Things (IoT) Standards, sheds light on the essential role of standards development organizations (SDOs), alliances, and open-source software initiatives in addressing standardization challenges. This collaborative effort, involving governments, academia, industry, and the public interest, is crucial for ensuring interoperability, security, and scalability in IoT ecosystems.

In the context of IoT standardization effort, we must ensure that investments in IoT and connectivity deliver tangible benefits to society while minimizing costs, preventing lock-in effects and maximizing efficiency. Additionally, strategic industrial cooperation in data processing is required to support open platforms, agreements on common architectures, and standards. They are critical for establishing a vibrant European ecosystem and ensuring coherence in IoT-edge standards development.

Geopolitical and competitive challenges further underscore the need for a unified approach to IoT standardization. By fostering collaboration and knowledge sharing, we can navigate these challenges effectively and ensure that European interests are safeguarded in the global IoT landscape.

Key ingredients to succeed in this process include the need for proactive engagement and continuous improvement in IoT standardization efforts, the necessity of showcasing success stories demonstrating contributions to standardization, and the adoption of a platform approach to ensure the scalability and sustainability of many research initiatives active in the standardization and IoT fields.

Furthermore, legislative initiatives such as the Chips Act and the AI Act provide a regulatory framework to support Europe's competitiveness and open strategic autonomy. By aligning standardization efforts with these legislative initiatives, we can foster a conducive environment for IoT development while addressing regulatory requirements and the arising market opportunities through IoT - Edge innovation.

Dr. Max Lemke,

Head of Unit Internet of Things, DG Connect of the European Commission

Editors and Contributors to this Report

Editor:

Georgios Karagiannis (Huawei)

Contributors:

Name	Company/Organisation
Sascha Hackel	Fraunhofer FOKUS
Georgios Karagiannis	Huawei
Antonio Kung	Trialog
Ana Lavinia Petrache	BEIA Consult
Richard Pitwon	Resolute Photonics
Axel Rennoch	Fraunhofer FOKUS
Maria Ines Robles	Tampere University
Mari-Anais Sachian	BEIA Consult
Natalia Stathakarou	Massive Dynamic
George Suciu	BEIA Consult
XiaoRui Zhang	Adaptcentre.ie
Edward C. Zimmermann	NONMONOTONIC Networks
Orfeas Voutyras	Institute of Communication and Computer Systems
Ray Walshe	Director EUOS
Michelle Wetterwald	Netellany

Abbreviations and Acronyms

3GPP	THIRD GENERATION PARTNERSHIP PROJECT
A/IS	AUTONOMOUS INTELLIGENT SYSTEM
AE	APPLICATION ENTITY
AI	ARTIFICIAL INTELLIGENCE
AIOTI	ALLIANCE FOR INTERNET OF THINGS AND EDGE COMPUTING INNOVATION
APIs	APPLICATION PROGRAMMING INTERFACES
ASN	ACHEVEMENT STANDARDS NETWORK
BBF	BROADBAND FORUM
CEN	EUROPEAN COMMITTEE FOR STANDARDISATION
CENELEC	EUROPEAN COMMITTEE FOR ELECTRONICAL STANDARDISATION
COAP	CONSTRAITED APPLICATION PROTOCOL
COMI	COAP MANAGEMENT INTERFACE
CSE	COMMON SERVICE ENTITY
DM	DEVICE MANAGEMENT
DMT	DIECTIVE MAINTENANCE TEAM
ECSO	EUROPEAN CYBERSECURITY ORGANISATION
ENISA	EUROPEAN UNION AGENCY FOR CYBERSECURITY
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
EUOS	EUROPEAN OBSERVATORY
ICN	INFORMATION CENTRIC NETWORKING
IEC	INTERNATIONAL ELECTRONICAL COMMISSION
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IETF	INTERNET ENGINEERING TASK FORCE
IoT	INTERNET OF THINGS
IRTF	INTERNET RESEARCH TASK FORCE
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ITU-T	INTERNATIONAL TELECOMMUNICATION UNION – TELECOMMUNICATION STANDARDISATION BUREAU
JSON	JAVASCRIPT OBJECT NOTATION
MEC	MULTI-ACCESS EDGE COMPUTING
MQTT	MESSAGE QUEUING TELEMETRY TRANSPORT
MTS	METHODS FOR TESTING AND SPECIFICATION
NETCONF	NETWORKING CONFIGURATION PROTOCOL
OMA	OPEN MOBILE ALLIANCE
OMA LWM2M	OMA LIGHTWEIGHT MACHINE TO MACHINE
OPC UA	OPEN PLATFORM COMMUNICATIONS UNIFIED ARCHITECTURE
OS	OPERATING SYSTEM
OSGi Alliance	OPEN SERVICE GATEWAY INITIATIVE

OSS	OPEN SOURCE SOFTWARE
OWL	WEB ONTOLOGY LANGUAGE
PPPs	PRIVATE PUBLIC PARTNERSHIP
RDF	RESOURCE DESCRIPTION FRAMEWORK
REST	REPRESENTATIONAL STATE TRANSFER
SAREF	SMART APPLICATION REFERENCE ONTOLOGY
SDO	STANDARDS DEVELOPMENT ORGANISATION
SDT	SMART DEVICE TEMPLATE
SLA	SERVICE LEVEL AGREEMENTS
SLO	SERVICE LEVEL OBJECTIVES
SMARTM2M	MACHINE 2 MACHINE
SOA	APPROACH SERVICE ORIENTED ARCHITECTURE
SSN	SEMANTIC SENSOR NTEWORK
SSO	STANDARDS SETTING ORGANISATION
STF 505	SPECIALIST TASK FORCE 505
SUIT	SOFTWARE UPDATES FOR INTERNET OF THINGS
TC	TECHNICAL COMMITTEE
TDL	TEST DESCRIPTION LANGUAGE
TR	TECHNICAL REPORT
TS	TECHNICAL SPECIFICATION
TWG	SECURITY TECHNICAL WORK GROUP
W3C	WORLD WIDE WEB CONSORTIUM
WG TST	WORKING GROUP TESTS
ZTC	ZERO TOUCH CONFIGURATION

1 Goal and motivation

This report presents[1] 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 in "Landscape of Internet of Things (IoT) Standards" 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 Development 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 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 "Landscape of Internet of Things (IoT) Standards" 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.

1 Note that this release of the report has been written by EUOS members that are as well members of the AIOTI WG Standardisation and contributed in AIOTI on writing a similar standardisation Gap analysis report, i.e., AIOTI "High Priority IoT Standardisation Gaps and Relevant SDOs", Release 3.0. Moreover, the AIOTI and EUOS standardisation Gap analysis reports have been edited by the same person. Therefore, a significant part of the text used in the AIOTI and EUOS standardisation Gap analysis reports will be identical.

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 standardization 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 standardization.
- **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 standardization challenges related to the integration and application of AI in IoT and Edge computing environments.

2.1 Smooth interoperability between Data Models

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

- Data Models and Formats

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 standardization or consistency in the way that data is organized and represented.
- A gap in data model refers to a lack of standardization 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 requires 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 standardization 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

- 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

- 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. Standards are defined for smart metering in the domain of Utilities. For example, IEC 62056 family of standards 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, algonside 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, algonside 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

- 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 standardization 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

- 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

- 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 standardization 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

Application/Industry domain:

- Horizontal (Service and applications)

2.19 Ethics and trustworthiness

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

- 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 standardization.
- 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

- 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

- 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

- 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

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

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

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

3.2 Standardisation Gaps: Identification

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

- "2.16 IoT over ICN"
- "2.20 - Open Markets of Digital Services".

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

3.3 Standardadisation 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 standardization landscape.

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

4. Gap analysis and resolution work in SDOs

4.1 Gap Resolution

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

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

4.2 EUOS identified IoT challenges covered/worked out by SDOs

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

The EUOS "Landscape of Internet of Things (IoT) Standards" 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 worked out by this SDOs. The complete analysis is included in tables, such as Table 1 used as an example in this section to show the EUOS identified IoT challenges covered/worked out by ETSI.

The rest of the tables that show how the EUOS identified IoT challenges covered/worked out 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:

Tables including the EUOS identified IoT challenges covered/worked out by SDOs: ANNEX 2

Table 1: EUOS identified IoT challenges covered/worked out by ETSI

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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. 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.	Developing Standards for IoT Security Testing and Validation (2.9)
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_1035970 2v010101p.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.	Developing Standards for IoT Security Testing and Validation (2.9)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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	Semantic interoperability (2.18)
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.	Usability of data and services provided by IoT devices and platform (2.14)
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.	Assurance a RESTFUL Data Exchange APIs (2.2) Device Management (2.22)
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.	Assurance a RESTFUL Data Exchange APIs (2.2)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15)
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15)
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.	Semantic interoperability (2.18)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	Assurance Privacy and Security (2.6)
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.	Assurance Privacy and Security (2.6) Smooth interoperability between Data Models (2.1) Semantic interoperability (2.18)
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.	Smooth interoperability between Data Models (2.1)
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.	Assurance Privacy and Security (2.6) IoT Governance and Regulation (2.12)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI/ oneM2M	ETSI TR 118 518 V2.5.1 (2020-07): Industrial Domain Enable-ment	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.	Need for real-time or near real-time processing and decision-making (2.3)
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	Usability of data and services provided by IoT devices and platform (2.14)
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.	Certification of device classes (2.21)
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.	Simulation and Emulation Environments (2.23)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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_10362 1v010201p.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.	Assurance Privacy and Security (2.6)
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_6 0/tr_10358 2v010101p.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.	Device Management (2.22)
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_118567v04 0000p.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.	Device Management (2.22)
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_118122v0 20301p.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.	Device Management (2.22)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15) Smooth interoperability between Data Models (2.1)
ETSI	ETSI TS 103 646 V1.1.1	https://www.etsi.org/deliver/etsi_ts/103600_103699/103646/01.01.01_60/ts_10364 6v010101p.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.	Developing Standards for IoT Security Testing and Validation (2.9)
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.	Developing Standards for IoT Security Testing and Validation (2.9)
ETSI	ETSI DTR 103 946	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66188	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.	Developing Standards for IoT Security Testing and Validation (2.9)

5. Standards Gaps Analysis and Recommendations

Section 4.2 of this report together with **ANNEX 2** provides an analysis on whether the 24 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 EUOS "Landscape of Internet of Things (IoT) Standards" 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/worked out 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/worked out 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: *EUOS identified IoT challenges covered/worked out 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	43	3		6	7	1		4	15		5	19		9	103
2.2	Assurance a RESTFUL Data Exchange APIs	7	2					2		12	1	2	6		7	32
2.3	Need for real-time or near real-time processing and decision-making	9	1		1	1	2								5	14
2.4	Connectivity Cost				1			1		1					3	3
2.5	Resilience to Intermittent Services				1	1				1					3	3
2.6	Assurance Privacy and Security	11	4		8			1		25	1	5			7	55
2.7	Deployment and management of large-scale distributed network of devices	2		3		3		1	1	89	3	21	1		9	124
2.8	Sustainability, energy consumption, rare minerals and raw materials provisioning	1			10			8		1					5	21
2.9	Developing Standards for IoT Security Testing and Validation	3	5		10	2		4		2					6	26
2.10	Developing and Implementing Trustoworthiness for IoT Systems	4			2										2	6
2.11	IoT and Ethics				2					1					2	3
2.12	IoT Governance and Regulation		1		1			1	1	1					5	5
2.13	Zero Touch Configuration				2	2		1		1					4	6
2.14	Usability of data and services provided by IoT Devices and platform		2									4	1		3	7
2.15	User-level Service Management of IoT Network by Utilizing AI		3									2			2	5
2.16	IoT over ICN														0	0
2.17	Harmonized identification				1				2	1					3	4
2.18	Semantic Interoperability	14	3		9		1	1	4	1		2			8	35
2.19	Ethics and Trustoworthiness				2										1	2
2.20	Open Markets of Digital Services				1										1	1
2.21	Certification of Devices Classes	2	1		2			12							4	17
2.22	Device Management	11	4					1				11	55		6	83
2.23	Simulation and Emulation Environments		1		1			2						4	4	8
2.24	Digital for Green	1			2			8		1					4	12

Figure 1 and Figure 2 provide a more detailed overview of the intensity that an IoT standardisation challenge is covered/worked out by an SDO and by specifications, respectively. The IoT challenge labels from S2.1 to S2.24, depicted in Figure 1 and Figure 2, are representing the descriptions of the challenges described in Section 2, from subsection 2.1 to subsection 2.24, respectively.

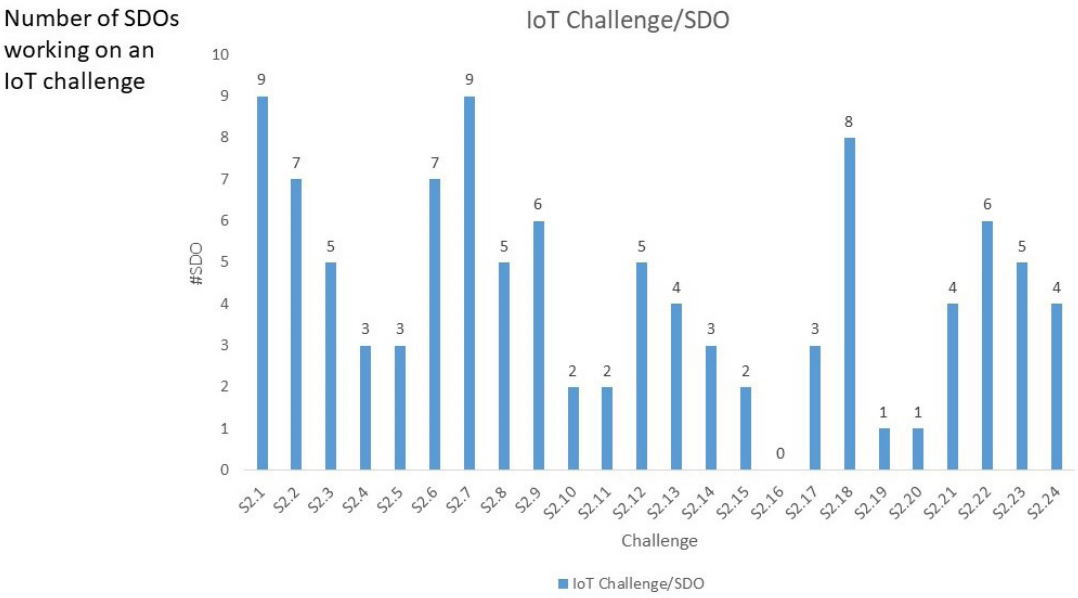

Figure 1: Number of SDOs covering / working out an EUOS IoT identified challenge

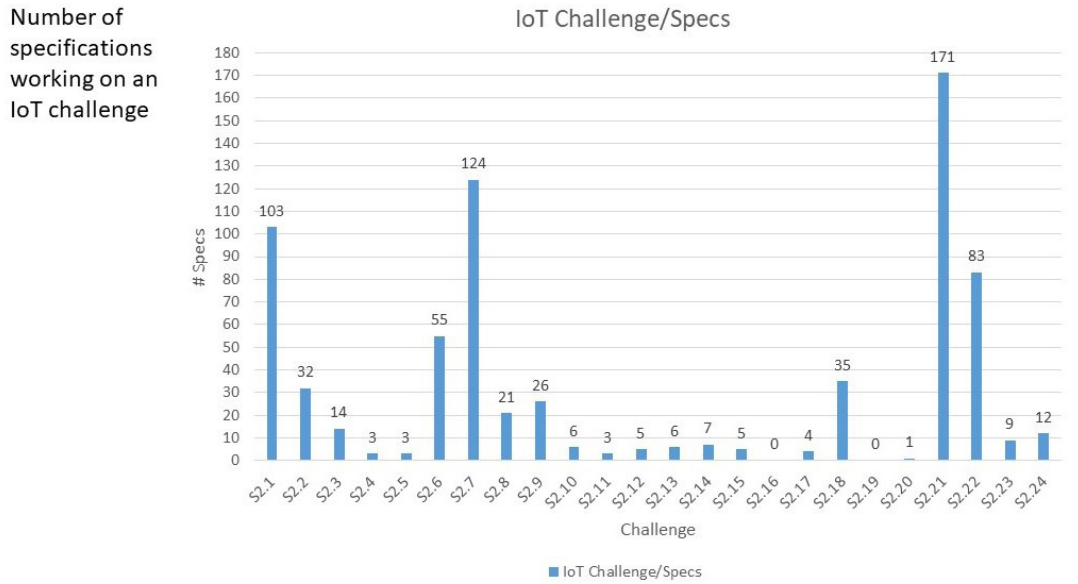

Figure 2: Number of specifications covering / working out an EUOS IoT identified challenge

From this analysis it can be concluded that:

- the IoT challenges: "2.16 IoT over ICN" and "2.20 Open Markets of Digital Services" need more research before being standardised.
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - "2.4 Connectivity Cost"

- "2.5 Resilience to Intermittent Services"
- "2.10 Developing and Implementing Trustoworthiness for IoT Systems"
- "2.11 IoT and Ethics"
- "2.14 Usability of data and services provided by IoT Devices and platform"
- "2.15 User-level Service Management of IoT Network by Utilizing AI"
- "2.17 Harmonized identification"
- "2.19 Ethics and Trustoworthiness"

- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
  - "2.12 IoT Governance and Regulation"
  - "2.13 Zero Touch Configuration".

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" 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 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 670 SDOs specifications to the 24 IoT challenges identified by EUOS and presented in Section 2. Based on this analysis it can be concluded that:

- the IoT challenges: "2.16 IoT over ICN" and 2.20 Open Markets of Digital Services need more research before being standardised:
- the following IoT standardisation challenges are marked as low intensively covered standardisation gap in SDOs and will require the highest level of standardisation work:
  - "2.4 Connectivity Cost"
  - "2.5 Resilience to Intermittent Services"
  - "2.10 Developing and Implementing Trustoworthiness for IoT Systems"
  - "2.11 IoT and Ethics"
  - "2.14 Usability of data and services provided by IoT Devices and platform"
  - "2.15 User-level Service Management of IoT Network by Utilizing AI"
  - "2.17 Harmonized identification"
  - "2.19 Ethics and Trustoworthiness"
- the following IoT standardisation challenges are marked as medium intensively covered standardisation gap in SDOs and will require a lower level of standardisation work:
  - "2.12 IoT Governance and Regulation"
  - "2.13 Zero Touch Configuration"

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 orange field

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 with IoT challenges covered/worked out by SDOs

Table 1: EUOS indentified IoT challenges covered/ workd out by IEC

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61406 ED1	https://www.iec.ch/ords/f?p=103:38:4010308328493310::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,104621	Under development	
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: optical attenuator; optical fuse; optical power limiter. This document also provides generic information including terminology for the IEC 61753-05x series. IEC Published IEC 61753-05x series documents are listed in Bibliography This fifth edition cancels and replaces	S2.3 (Need for real-time or near real-time processing and decision-making);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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; 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.	S2.3 (Need for real-time or near real-time processing and decision-making);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61300-1:2022	https://webstore.iec.ch/publication/67663	IEC 61300-1:2022 is available as https://webstore.iec.ch/publication/75220 IEC 61300-1:2022 RLV which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 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 (Need for real-time or near real-time processing and decision-making);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61753-1:2018	https://webstore.iec.ch/publication/67249	IEC 61753-1:2018 is also available as https://webstore.iec.ch/publication/63751 IEC 61753-1:2018 RLV which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 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 (Need for real-time or near real-time processing and decision-making); S2.7 (Deployment and management of large-scale distributed networks of devices);

SDO	Specification			Relevant 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 EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 61754-4:2022	https://webstore.iec.ch/publication/29284	IEC 61754-4:2022 is available as https://webstore.iec.ch/publication/74619 IEC 61754-4:2022 RLV which contains the International Standard and its Redline 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 (Need for real-time or near real-time processing and decision-making); S2.21 (Certification of device classes);
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 (Need for real-time or near real-time processing and decision-making); S2.21 (Certification of device classes);
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;	S2.3 (Need for real-time or near real-time processing and decision-making);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			▷ 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; ▷ 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	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 (Need for real-time or near real-time processing and decision-making); S2.7 (Deployment and management of large-scale distributed networks of devices);
IEC	IEC 62099:2001	https://webstore.iec.ch/publication/6459	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 (Need for real-time or near real-time processing and decision-making);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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. Also changed StatusResult into StatusCode. Created new version of the type to ProgramDiagnostic2DataType. b) Changed Optional modelling rule to OptionalPlaceHolder for Program control Methods. Following the clarification in IEC 62541-3, this now allows subtypes (or instances) to add arguments.	S2.1 (Smooth interoperability between Data Models);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.22 (Device Management)
IEC	IEC 62541-11:2020	https://webstore.iec.ch/publication/61129	IEC 62541-11:2020 which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition. IEC 62541-11:2020 is part of the OPC Unified Architecture standard series and defines the information model associated with Historical Access (HA). It particularly includes additional and complementary descriptions of the NodeClasses and Attributes needed for Historical Access, additional standard Properties, and other information and behaviour. The complete AddressSpace Model including all NodeClasses and Attributes is specified in IEC 62541-3. The predefined Information Model is defined in IEC 62541-5. The Services to detect and access historical data and events, and description of the ExtensibleParameter types are specified in IEC 62541-4. This document includes functionality to compute and return Aggregates like minimum, maximum, average etc. The Information Model and the concrete working of Aggregates are defined in IEC 62541-13. 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) a new method for determining the first historical point has been added; b) added clarifications on how to add, insert, modify, and delete annotations.	S2.1 (Smooth interoperability between Data Models); S2.22 (Device Management)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.22 (Device Management)
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. 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.	S2.1 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant 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. 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: 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.	S2.1 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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.	
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.	S2.1 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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.	
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: a) Encodings: ▷ added JSON encoding for PubSub (non-reversible); ▷ added JSON encoding for Client/Server (reversible);	S2.1 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			▷ added support for optional fields in structures; ▷ added support for Unions. b) Transport mappings: ▷ added WebSocket secure connection – WSS; ▷ added support for reverse connectivity; ▷ added support for session-less service invocation in HTTPS. c) 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.	
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 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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. c) 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). d) deprecated Transport (missing support on most platforms): ▷ SOAP/HTTP with WS-SecureConversation (all encodings).	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.18 (Semantic interoperability); S2.22 (Device Management);
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.	S2.1 (Smooth interoperability between Data Models); S2.2 (Assurance a RESTFUL Data Exchange APIs); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.18 (Semantic interoperability); S2.22 (Device Management);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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: DiscrepancyAlarm, 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.	
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.	S2.1 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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	
	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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);

SDO	Specification			Relevant 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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
IEC	IEC 63365 ED1	https://www.iec.ch/ords/f?p=103:38:401030832849310:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,104515	Under development	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Smooth interoperability between Data Models);
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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 (Smooth interoperability between Data Models);
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 (Smooth interoperability between Data Models);
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 (Smooth interoperability between Data Models);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models);
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 (Smooth interoperability between Data Models);
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 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 (Smooth interoperability between Data Models);
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 (Assurance Privacy and Security); S2.10 (Developing and Implementing Trustworthiness for IoT Systems)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Assurance Privacy and Security); S2.10 (Developing and Implementing Trustworthiness for IoT Systems)
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 (Smooth interoperability between Data Models);
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 (Smooth interoperability between Data Models);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models);
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 (Smooth interoperability between Data Models); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)
IEC	IEC 63278-1 ED1	https://www.iec.ch/dyn/www/f?p=103:38:731054763917753:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,103536	Under development	
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	Under development	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	IEC 63339 ED1	https://www.iec.ch/dyn/www/f?p=103:38:731054763917753:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,104329	Under development	
IEC	IEC 63376 ED1	https://www.iec.ch/dyn/www/f?p=103:38:731054763917753:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1250,23,104647	Under development	
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 (Smooth interoperability between Data Models
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models);
IEC	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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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).	
IEC	IEC 61987-31 ED1	https://www.iec.ch/ords/f?p=103:38:401030832849310:::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1452,23,102292	Under development	
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.	

SDO	Specification			Relevant 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.	
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	S2.1 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security); S2.10 (Developing and Implementing Trustworthiness for IoT Systems)
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 (Smooth interoperability between Data Models); S2.6 (Assurance Privacy and Security); S2.10 (Developing and Implementing Trustworthiness for IoT Systems)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEC	EC 63237-1 ED1	https://www.iec.ch/dyn/www/f?p=103:7:6028733131419 8733:::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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);

Table 2: EUOS indentified IoT challenges covered/ workd out by ETSI

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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_103596 02v010101p.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. 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.	Developing Standards for IoT Security Testing and Validation (2.9)
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_1035970 2v010101p.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.	Developing Standards for IoT Security Testing and Validation (2.9)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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	Semantic interoperability (2.18)
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.	Usability of data and services provided by IoT devices and platform (2.14)
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.	Assurance a RESTFUL Data Exchange APIs (2.2) Device Management (2.22)
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.	Assurance a RESTFUL Data Exchange APIs (2.2)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15)
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15)
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.	Semantic interoperability (2.18)
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.	Assurance Privacy and Security (2.6)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	Assurance Privacy and Security (2.6) Smooth interoperability between Data Models (2.1) Semantic interoperability (2.18)
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.	Smooth interoperability between Data Models (2.1)
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.	Assurance Privacy and Security (2.6) IoT Governance and Regulation (2.12)
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.	Need for real-time or near real-time processing and decision-making (2.3)
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	Usability of data and services provided by IoT devices and platform (2.14)

SDO	Specification			Relevant 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.	Certification of device classes (2.21)
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.	Simulation and Emulation Environments (2.23)
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.	Assurance Privacy and Security (2.6)
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.	Device Management (2.22)
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.	Device Management (2.22)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	Device Management (2.22)
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.	User-level Service Managements of IoT Network by utilizing Artificial Intelligence (2.15) Smooth interoperability between Data Models (2.1)
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.	Developing Standards for IoT Security Testing and Validation (2.9)
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.	Developing Standards for IoT Security Testing and Validation (2.9)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ETSI	ETSI DTR 103 946	https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=66188	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.	Developing Standards for IoT Security Testing and Validation (2.9)

Table 3: EUOS indentified IoT challenges covered/ workd out by 3GPP

SDO	Specification			Relevant 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 Deployment and management of large-scale distributed networks of devices
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 Deployment and management of large-scale distributed networks of devices
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 Deployment and management of large-scale distributed networks of devices

Table 4: EUOS indentified IoT challenges covered/ workd out byISO/IEC JTC1

SDO	Specification			Relevant 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.	
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.	
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Harmonized identification); S2.18 (Semantic interoperability);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 30183 ED1	https://www.iec.ch/dyn/www/f?p=103:38:20477436329579 6:::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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
ISO/ IEC JTC1	ISO/IEC 30179 ED1	https://www.iec.ch/dyn/www/f?p=103:38:20477436329579 6:::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.	
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.	
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.	
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.	
ISO/ IEC JTC1	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.	

SDO	Specification			Relevant 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.	
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.	
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	
ISO/ IEC JTC1	ISO/ IEC TR 30167: 2021	https://webstore.iec.ch/publication/65619	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.	
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 (Simulation and Emulation Environments); S2.24 (Digital for Green);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	ISO/IEC 27400	+	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation);
ISO/ IEC JTC1	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation);
ISO/ IEC JTC1	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.21 (Certification of device classes);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
ISO/ IEC JTC1	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation);
ISO/ IEC JTC1	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.20 (Open Markets of Digital Services);
ISO/ IEC JTC1	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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation);
ISO/ IEC JTC1	ISO/ IEC TS 30168	https://www.iec.ch/ords/f?p=103:38:7063752284800 80:::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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.21 (Certification of device classes);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Semantic interoperability);
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 (Smooth interoperability between Data Models); S2.12 (IoT Governance and Regulation);
ISO/ IEC JTC1	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 (Digital for Green);
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 (Smooth interoperability between Data Models); S2.18 Semantic interoperability);
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	
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.	
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).	
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	
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.	
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.	
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	
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 (Smooth interoperability between Data Models); S2.18 Semantic interoperability);
ISO/ IEC JTC1	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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.10 (Developing and Implementing Trustworthiness for IoT Systems); S2.11 (IoT and Ethics); S2.13 (Zero Touch Configuration (ZTC)); S2.19 (Ethics and trustworthiness);
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.	
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.	
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.	

SDO	Specification			Relevant 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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability);
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 (Need for real-time or near real-time processing and decision-making); S2.5 (Resilience to Intermittent Services);

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Connectivity Cost);
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.	
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.	
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 endpoints 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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Assurance Privacy and Security); S2.8 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.9 (Developing Standards for IoT Security Testing and Validation); S2.10 (Developing and Implementing Trustworthiness for IoT Systems); S2.11 (IoT and Ethics); S2.13 (Zero Touch Configuration (ZTC)); S2.19 (Ethics and trustworthiness);
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.	
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.	

Table 5: EUOS indentified IoT challenges covered/ workd out by CEN/CENELEC

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	EN 13757-4:2019	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:60262&cs=156CDF6A723103E3251766A065867 79B6	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 (Smooth interoperability between Data Models)
CEN	EN 13757-6:2015	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41515&cs=14E87496D5D72D87C65AB EBFF-CB3BD0AB	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 (Smooth interoperability between Data Models)
CEN	EN 13757-7:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:61822&cs=107399C785EC0B2EDACF-60D74955A90D5	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 (Smooth interoperability between Data Models); S2.6 (Assurance privacy and security)

SDO	Specification			Relevant 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=157EF44C329D0ADE1DB97DF-0406BAA443	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 (Smooth interoperability between Data Models) S2.18 (Semantic interoperability)
CEN	EN 16836-2:2016	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:41099&cs=181323929D1945B36591_4E7CE-01F502AD	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 (Smooth interoperability between Data Models) S2.18 (Semantic interoperability)

SDO	Specification			Relevant 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=1C46C E950442B-0C43F9 EDDA-C4585ACF19	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 (Smooth interoperability between Data Models); S2.24 (Digital for Green)
CEN	CEN/TR 17167:2018	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:61828&cs=1338F0A4C72 39D0EC-0470C6E1605 E2BCF	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 (Smooth interoperability between Data Models); S2.6 (Assurance privacy and security)
CEN	EN ISO 14814:2006	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:21173&cs=184D D778D0F4ED 9BEEC2F72C9 2F3FFFB1	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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability)

SDO	Specification			Relevant 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=19B94878D7D6F9814 2DFDE 0433CC7D3C1	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 (Smooth interoperability between Data Models)
CEN/CENELEC	EN 50090 (ISO 14543)	https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:::::FSP_PROJECT,FSP_ORG_ID:55668,1258281&cs=14BD40 8738BD97FB5CF4581F2 7FF76877	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		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 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=15997C7BB19A97A296D8A7719196409AD	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant EUOS identified IoT challenges
	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=1C3A14008 7AD-1FDE 865115EA 876607C93	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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=13B159A77 84936BDC97A42AFA8C21211A	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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::::FSP_PROJECT:68227&cs=19CD8A5DF8D8A747A2648590BAC670053	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. 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.	S2.1 (Smooth interoperability between Data Models)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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 (Smooth interoperability between Data Models)
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).	S2.1 (Smooth interoperability between Data Models)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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.	
CEN	FprCEN/ TS 16157-6	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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=1888933092FF2E127C49B472E09BA2FB	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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::::FSP_PROJECT:71189&cs=17CE8E7FC7390CF7CC48C34700D0A825D	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 (Smooth interoperability between Data Models) S2.24 (Digital for Green)

SDO	Specification			Relevant 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=1104654 08 B33310 1C137C3B2A AB-C7EE51	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 (Smooth interoperability between Data Models)
CEN	CEN/TS 16157-12	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73 025,25&cs=191FB A7A8FAE57 738466F76 A 27106F67D	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 (Smooth interoperability between Data Models)
CEN	CEN/TS 16157-6:2015	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:40220&cs=108470 2C54C56E35 47969771C 8305250B	This new work item will produce the sixth part of the DATEX II Technical Specifications which deals with a DATEX II Level B extension (two publications and a Truck Parking profile) 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 actions e and f. 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, In-Time CAI and Truck Parking initiatives, and to liaise with the stakeholders involved	S2.1 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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 (Smooth interoperability between Data Models)
CEN	CEN/TS 16157-9	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:68652&cs=18B518A2094371209963638237DDAC	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 9, this document, specifies additional data model structures 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 consistent way with existing C-ITS standards and technical specifications. 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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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. As regards the other exchange protocols, a formal compatibility is ensured with TransXChange (UK), VDV 452 (Germany), NEPTUNE (France), UIC Leaflet, BISON (The Netherlands) and NOPTIS (Nordic Public Transport Interface Standard). The data exchange is possible either through dedicated web services, through data file exchanges, or using the SIRI exchange protocol as described in part 2 of the SIRI documentation.	S2.1 (Smooth interoperability between Data Models)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CENELEC	prEN 50090-6-3	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:74475,25&cs=1046EE8EC4361FACC3F6370EBB7B68089	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 communication 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 notifications 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	
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.	
CEN	EN 13757-2	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:61821,6275&cs=148E2A53815B1043A00AB94D-1340B84A1	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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	
CEN	EN 16836-1	https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:41098,6275&cs=11019FC07793E83E7C3B39E9E3A6DBF78	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.	
CEN	prEN 14154-4	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73396,25&cs=1DA0D2906520CD899CB94F5BB61C72E7F	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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	CEN ISO/TS 17425: 2016	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:35914&cs=10C18F278124980B9F4075E355AB45BC3	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 (Smooth interoperability between Data Models)
CEN	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 241023 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 (Smooth interoperability between Data Models); S2.3 (Need for real time or near real time processing and decision-making); S2.6 (Assurance Privacy and Security); 2.10 (Developing and Implementing Trustworthiness for IoT systems)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant 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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability)
CEN	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 (Smooth interoperability between Data Models)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
CEN	prCEN ISO/TS 19321 rev	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:73937,25&cs=108B9C05FB54333B566ACFD5122C7E1F9	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 (Smooth interoperability between Data Models)
CEN	EN 13757-2:2018/prA1	https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:74544,25&cs=1761F4D6E55C0F87848EB2822BAF9FAAF	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 (Smooth interoperability between Data Models); S2.24 (Digital for Green)
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.	S2.9 (Developing Standards for IoT Security Testing and Validation); S2.10 (Developing and Implementing Trustworthiness for IoT Systems)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
			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.	
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.	
CENELEC	prEN IEC 63345	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.	S.2.24 (Digital for Green)
CENELEC	prEN IEC 63402	https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:7457,5,25&s=167D D57F4AA099C41201ADC1979E157B2	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 (Digital for Green)

Table 6: EUOS indentified IoT challenges covered/ workd out by IEEE

SDO	Specification			Relevant 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 IEEE-GET 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 (Need for real-time or near real-time processing and decision-making);
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 (Need for real-time or near real-time processing and decision-making);
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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability)
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 EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IEEE	IEEE - P1451-99	https://standards.ieee.org/ieee/1451.99/10355/	The 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.	S2.7 (Deployment and management of large-scale distributed networks of devices)

Table 7: EUOS indentified IoT challenges covered/ workd out by ITU-T

SDO	Specification			Relevant 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 (Sustainability, energy consumption, rare minerals and raw materials provisioning) S2.24 (Digital for Green)
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 (Developing Standards for IoT Security Testing and Validation)
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 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 (Assurance a RESTFUL Data Exchange APIs)
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.	
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.	
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.	

SDO	Specification			Relevant 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 greenhouse service; b) Reference architecture for smart greenhouse service; c) Interfaces for smart greenhouse service; d) Use Cases of smart greenhouse service.	
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 challenges 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 scenarios for vehicle-to-everything (V2X) and for smart manufacturing are provided in an appendix.	S2.7 (Deployment and management of large-scale distributed networks of devices);
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 simulate different scenarios of IoT implementations. This recommendation describes the architecture and facilities of Model Network for IoT testing.	S2.9 (Developing Standards for IoT Security Testing and Validation)
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, interoperability and benchmarking testing frameworks for IoT are the recommendation scope.	S2.9 (Developing Standards for IoT Security Testing and Validation)
ITU-T	ITU-T Q.4063 (09/2020)	https://handle.itu.int/11.1002/1000/14391	The recommendation provides a description 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 authenticity of the IoT. The classification of IoT, in terms of testing of their identification procedures and the relevant testing approaches are subjects of this Recommendation.	S2.9 (Developing Standards for IoT Security Testing and Validation)
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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.	
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.	
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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 (Resilience to Intermittent Services)
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 (Semantic interoperability)
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 (Assurance a RESTFUL Data Exchange APIs)
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 (Connectivity Cost)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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 (Simulation and Emulation Environments)
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.	
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.	
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.	

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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.	
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.	
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.	
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.	2.13 (Zero Touch Configuration (ZTC))

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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.	
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	
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.	2.23 (Simulation and Emulation Environments)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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	
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.	
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.	

SDO	Specification			Relevant 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.	
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.	
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.	
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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 Digital for Green

SDO	Specification			Relevant 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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 Digital for Green
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 (Certification of device classes)
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 (Certification of device classes)
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 (Certification of device classes)
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 (Certification of device classes)
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 (Certification of device classes)
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 (Certification of device classes)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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 (Certification of device classes)
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 (IoT Governance and Regulation); 2.22 (Device Management)
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.	
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.	

SDO	Specification			Relevant 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.	
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 (Certification of device classes)
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 (Certification of device classes)
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 (Certification of device classes)

SDO	Specification			Relevant 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.	

SDO	Specification			Relevant 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.	
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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)
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 (Certification of device classes)
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 (Certification of device classes)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)
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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)
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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & sections
ITU-T	ITU-T L.1480 (12/2022)	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 (Sustainability, energy consumption, rare minerals and raw materials provisioning); S2.24 (Digital for Green)

Table 8: EUOS indentified IoT challenges covered/ workd out by W3C

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
W3C	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 (Smooth interoperability between Data Models); S2.18 (Semantic interoperability)
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 (Harmonized identification)
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 (Smooth interoperability between Data Models); 2.18 (Semantic interoperability)
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 (IoT Governance and Regulation)

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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 (Smooth interoperability between Data Models); 2.18 (Semantic interoperability)
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 (Smooth interoperability between Data Models); 2.18 (Semantic interoperability)
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 (Harmonized identification)

Table 9: EUOS indentified IoT challenges covered/ workd out by IETF

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	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.	2.1 Smooth interoperability between Data Models 2.2 Assurance a RESTFUL Data Exchange APIs 2.18 Semantic interoperability
IETF	IETF draft-ietf-ipwave-vehicular-networking IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases	https://datatracker.ietf.org/doc/draft-ietf-ipwave-vehicular-networking/	This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation systems (ITS).	2.7 Deployment and management of large-scale distributed networks of devices
IETF	IETF draft-ietf-lake-edhoc Ephemeral Diffie-Hellman Over COSE (EDHOC)	https://datatracker.ietf.org/doc/draft-ietf-lake-edhoc/	This document specifies Ephemeral Diffie-Hellman Over COSE (EDHOC), a very compact and lightweight authenticated Diffie-Hellman key exchange with ephemeral keys.	2.6 Assurance Privacy and Security
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).	2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF draft-ietf-rats-architecture Remote Attestation Procedures Architecture	https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/	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.	2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security
IETF	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).	2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security
IETF	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.	2.1 Smooth interoperability between Data Models 2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security
IETF	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.	2.1 Smooth interoperability between Data Models 2.6 Assurance Privacy and Security

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	IETF draft-ietf-raw-ldacs L-band Digital Aeronautical Communications System (LDACS)	https://datatracker.ietf.org/doc/draft-ietf-raw-ldacs/	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	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	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	IETF draft-ietf-raw-use-cases RAW use-cases	https://datatracker.ietf.org/doc/draft-ietf- raw-use-cases/	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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	IETF draft-ietf-teep-architecture Trusted Execution Environment Provisioning (TEEP) Architecture	https://datatracker.ietf.org/doc/draft-ietf-teep -architecture/	This architecture document motivates the design and standardization of a protocol for managing the lifecycle of trusted applications running inside such a TEE.	2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security
IETF	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.	2.6 Assurance Privacy and Security
IETF	IETF draft-km-iotops-iiot-frwk Virtualization of PLC in Industrial Networks - Problem Statement	https://datatracker.ietf.org/doc/draft-km-iot-ops-iiot-frwk/	This document introduces virtual PLC concept, describes the details and benefits of virtualized PLCs, then focuses on the problem statement and requirements.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	IETF draft-morais-iotops-inxu Intra-Network eXposure analyzer Utility Specification	https://datatracker.ietf.org/doc/draft-morais-iot-ops-inxu/	This document proposes the Intra-Network eXposure analyzer Utility (INXU) as a vulnerability management solution for IoT networks.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
IETF	IETF RFC6206 The Trickle Algorithm	https://datatracker.ietf.org/doc/rfc6206/	This document describes the Trickle algorithm and considerations in its use.	2.7 Deployment and management of large-scale distributed networks of devices
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	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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).	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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).	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.2 Assurance a RESTFUL Data Exchange APIs

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.6 Assurance Privacy and Security

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security 2.11. IoT and Ethics 2.12. IoT Governance and Regulation
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.	2.6 Assurance Privacy and Security

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.2 Assurance a RESTFUL Data Exchange APIs.
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	2.8 Sustainability, energy consumption, rare minerals, and raw materials provisioning, 2.24 Digital for Green

SDO	Specification			Relevant 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".	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant 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.	2.1 Smooth interoperability between Data Models
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant 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.	2.7 Deployment and management of large-scale distributed networks of devices
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".	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models
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.	2.6 Assurance Privacy and Security
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	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models
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.	2.1 Smooth interoperability between Data Models
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).	2.1 Smooth interoperability between Data Models
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security 2.9 Developing Standards for IoT Security Testing and Validation

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IETF	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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.6 Assurance Privacy and Security
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	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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	2.7 Deployment and management of large-scale distributed networks of devices
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).	2.7 Deployment and management of large-scale distributed networks of devices
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).	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models
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	2.1 Smooth interoperability between Data Models
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	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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).	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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).	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.13 Zero touch configuration
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.2 Assurance a RESTFUL Data Exchange APIs 2.17 Harmonized Identification

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.6 Assurance Privacy and Security 2.9 Developing Standards for IoT Security Testing and Validation
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.	2.5 Resilience to Intermittent Services
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.1 Smooth interoperability between Data Models
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.1 Smooth interoperability between Data Models
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.7 Deployment and management of large-scale distributed networks of devices

Table 10: EUOS indentified IoT challenges covered/ workd out by IRTF

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
IRTF	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.	2.14 Usability of data and services provided by IoT devices and platform
IRTF	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).	2.2 Assurance a RESTFUL Data Exchange APIs
IRTF	IRTF draft-irtf-t2trg-secure-bootstrapping 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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices
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)	2.16 IoT over ICN

Table 11: EUOS indentified IoT challenges covered/ workd out by oneM2M

SDO	Specification			Relevant 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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.22 Device Management
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models
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.	2.22 Device Management
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.22 Device Management
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.	2.22 Device Management
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.	2.1 Smooth interoperability between Data Models

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.18 Semantic Interoperability
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.	2.7 Deployment and management of large-scale distributed networks of devices
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 .	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.18 Semantic Interoperability

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.14 Usability of data and services provided by IoT devices and platform
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.14 Usability of data and services provided by IoT devices and platform
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.	2.6 Assurance Privacy and Security
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.	2.22 Device Management
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.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.14 Usability of data and services provided by IoT devices and platform
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.	2.14 Usability of data and services provided by IoT devices and platform
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.	2.7 Deployment and management of large-scale distributed networks of devices

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.6 Assurance Privacy and Security
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models
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.	2.22 Device Management
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.	2.22 Device Management
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.	2.15 User level service management of IoT Network by utilizing Artificial Intelligence

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.1 Smooth interoperability between Data Models
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.	2.22 Device Management
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.	2.7 Deployment and management of large-scale distributed networks of devices
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'.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.6 Assurance Privacy and Security
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.	2.15 User level service management of IoT Network by utilizing Artificial Intelligence

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.2 Assurance a RESTFUL Data Exchange APIs
oneM2M	oneM2M WI-0109 IPE-based Device Management with Flex-Containers	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.	2.22 Device Management
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.1 Smooth interoperability between Data Models

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.7 Deployment and management of large-scale distributed networks of devices

Table 12: EUOS indentified IoT challenges covered/ workd out by OMA

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	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.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA IPSO Repo Public IPSO Repository	https://technical.openmobilealliance.org/OMNA/LwM2M/LwM-2MRegistry.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.	2.1 Smooth interoperability between Data Models 2.22 Device Management
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].	2.7 Deployment and management of large-scale distributed networks of devices
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.	2.14 Usability of data and services provided by IoT devices and platform

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.22 Device Management
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.	2.22 Device Management
OMA	OMA-TS-REST_NetAPI_Device-Capabilities-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_Device-Capabilities-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].	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.22 Device Management
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.	2.22 Device Management
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.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-TS-DM_ Protocol-V2_ 0-20160209-A OMA Device Management Protocol	https://www.openmobile-alliance.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.	2.22 Device Management
OMA	OMA-RD-EN-Cap-M-V1_ 0-20180621-A Exposing Network Capabilities to M2M Requirements	https://www.openmobile-alliance.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.	2.22 Device Management
OMA	OMA-RRELD-ENCap-M2M-V1_ 0-20180621-A Reference Release Definition for for Exposing Network Capabilities to M2M	https://www.openmobile-alliance.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.	2.22 Device Management
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.	2.22 Device Management
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.	2.22 Device Management
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.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.22 Device Management
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.	2.2 Assurance a RESTFUL Data Exchange APIs 2.22 Device Management
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].	2.22 Device Management
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.	2.22 Device Management
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).	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.22 Device Management
OMA	OMA-TS-GwMO-V1_1-20170725-A Gateway Management Object Technical Specification	https://www.openmobile-alliance.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].	2.22 Device Management
OMA	OMA-ETS-LightweightM2M_INT-V1_1-20190912-D Enabler Test Specification (Interoperability) for Lightweight M2M	https://www.openmobile-alliance.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-LightweightM-2MV1_ 1-20180710-A and OMA-TS-LightweightM2M_ Transport-V1_ 1-20180710-A.	2.22 Device Management
OMA	OMA-EVP-LightweightM2M-V1_0-20140819-C Enabler Validation Plan for Lightweight M2M	https://www.openmobile-alliance.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.	2.22 Device Management
OMA	OMA-ERELD-LightweightM2M-V1_2-20201110-A Enabler Release Definition for LightweightM2M	https://www.openmobile-alliance.org/release/LightweightM2M/V1_2-20201110-A/ OMA-ERELD-LightweightM2M-V1_2-20201110-A.pdf	The scope of this document is limited to the Enabler Release Definition of LightweightM2M v1.2 according to OMA Release process and the Enabler Release specification baseline listed below.	2.22 Device Management
OMA	OMA-RD-LightweightM2M-V1_2-20201110-A OMA Lightweight Machine to Machine Requirements	https://www.openmobile-alliance.org/release/LightweightM2M/ V1_2-20201110-A/ OMA-RD-Lightweight M2M-V1_2-20201110-A.pdf	This document represents Lightweight M2M version 1.2 consolidated requirements.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA-TS-LightweightM2M_Core-V1_2-20201110-A Lightweight Machine to Machine Technical Specification: Core	https://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-TS-LightweightM2M_Core-V1_2-20201110-A.pdf	This document, the LwM2M CORE technical specification, describes the LwM2M messaging layer. The LwM2M TRANSPORT specification [LwM2M-TRANSPORT], a companion specification, details the mapping of the messaging layer to selected transports. The separation between transport and messaging layer improves readability and simplifies extending LwM2M to further transports. The LwM2M messaging layer uses a RESTful design with several interfaces and a simple data model.	2.22 Device Management
OMA	OMA-TS-LightweightM2M_Transport-V1_2-20201110-A Lightweight 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.	2.22 Device Management
OMA	OMA-ERELD-LWM2M_BinaryAppDataCont-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.	2.22 Device Management
OMA	OMA-TS-LWM2M_BinaryAppDataContainer-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.	2.22 Device Management
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.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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.	2.22 Device Management
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	2.22 Device Management
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.	2.22 Device Management
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.	2.22 Device Management
OMA	OMA-RRELD-M2Minterface-V1_ 0-20150324-A Reference Release Definition for M2Minterface	https://www.openmobilealliance.org/release/M2Minterface/V1_0-2 0150324-A/OMA-RRELD-M2M interface-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.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA ObjL-wM2M_ 5GNR_ Conn LIGHT-WEIGHTM2M 5GNR CONNEC-TIVITY	https://www.openmobilealli-ance.org/release/ObjLwM2M_ 5GNR_ Conn/V1_ 0-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M 5GNR Connectivity v1.0.	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement
OMA	OMA Ob-jLwM2M_ ACL LIGHT-WEIGHTM2M ACCESS CON-TROL	https://www.openmobile-alliance.org/release/ObjL-wM2M_ ACL/V1_ 1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Access Control v1.1	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement
OMA	OMA ObjL-wM2M_ APN_ Conn LIGHT-WEIGHTM2M APN CONNEC-TION PROFILE	https://www.openmobilealli-ance.org/release/ObjLwM2M_ APN_ Conn/V1_ 1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M APN Connection Profile v1.1.	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement
OMA	OMA ObjL-wM2M_ Bearer_ Conn LIGHT-WEIGHTM2M BEARER SELEC-TION	https://www.openmobilealli-ance.org/release/ObjLwM2M_ Bearer_ Conn/V1_ 1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Bearer Selection v1.1.	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement
OMA	OMA ObjL-wM2M_ Cell_ Conn LIGHT-WEIGHTM2M CELLULAR CON-NECTIVITY	https://www.openmobilealli-ance.org/release/ObjLwM2M_ Cell_ Conn/V1_ 1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Cellular Connectivity v1.1.	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement
OMA	OMA ObjL-wM2M_ Conn_ Mon Light-weightM2M Connectivity Monitoring	https://www.openmobilealli-ance.org/release/ObjLwM2M_ Conn_ Mon/V1_ 3-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Connectivity Monitoring v1.3.	2.1 Smooth interoperability between Data Models 2.22 Device Man-agement

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA ObjL-wM2M_ Conn_ Stat Light-weightM2M Connectivity Statistics	https://www.openmobilealliance.org/release/ObjLwM2M_Conn_Stat/V1_0_5-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Connectivity Statistics v1.0.5.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ COSE LightweightM2M COSE	https://www.openmobilealliance.org/release/ObjLwM2M_COSE/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M COSE v1.0.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Device LightweightM2M Device	https://www.openmobilealliance.org/release/ObjLwM2M_Device/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Device v1.2.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Firm-ware Light-weightM2M Firmware Update	https://www.openmobilealliance.org/release/ObjLwM2M_Firmware/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Firmware Update v1.1.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Gateway LightweightM2M Gateway	https://www.openmobilealliance.org/release/ObjLwM2M_Gateway/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Gateway v1.0.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Location LightweightM2M Location	https://www.openmobilealliance.org/release/ObjLwM2M_Location/V1_0_3-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Location v1.0.3.	2.1 Smooth interoperability between Data Models 2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
OMA	OMA ObjL-wM2M_ MQTT_ Server Light-weightM2M MQTT Server	https://www.openmobilealliance.org/release/ObjLwM2M_MQTT_Server/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M MQTT Server v1.0.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ OSCORE LightweightM2M OSCORE	https://www.openmobilealliance.org/release/ObjLwM2M_OSCORE/V2_0-20211123-A/	DOCUMENT LISTING FOR SUP Light-weightM2M OSCORE v2.0.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Routing LightweightM2M Routing	https://www.openmobilealliance.org/release/ObjLwM2M_Routing/V1_0-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Routing v1.0.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Security LightweightM2M Security	https://www.openmobilealliance.org/release/ObjLwM2M_Security/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Security v1.2.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ Server LightweightM2M Server	https://www.openmobilealliance.org/release/ObjLwM2M_Server/V1_2-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M Server v1.2.	2.1 Smooth interoperability between Data Models 2.22 Device Management
OMA	OMA ObjL-wM2M_ WLAN_ Conn Light-weightM2M WLAN Connec-tivity	https://www.openmobilealliance.org/release/ObjLwM2M_WLAN_Conn/V1_1-20201110-A/	DOCUMENT LISTING FOR SUP Light-weightM2M WLAN Connectivity v1.1.	2.22 Device Management

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
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].	2.2 Assurance a RESTFUL Data Exchange APIs
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.	2.2 Assurance a RESTFUL Data Exchange APIs 2.22 Device Management
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.	2.2 Assurance a RESTFUL Data Exchange APIs 2.22 Device Management
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.	2.2 Assurance a RESTFUL Data Exchange APIs 2.22 Device Management

Table 13: EUOS indentified IoT challenges covered/ workd out by Open Source

SDO	Specification			Relevant EUOS identified IoT challenges
	Title	URL	Abstract	Labels & Sections
Contiki	Contiki 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.	2.23 Simulation and Emulation Environments
FIWARE Foundation	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.	2.23 Simulation and Emulation Environments
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.	2.23 Simulation and Emulation Environments
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.	2.23 Simulation and Emulation Environments

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